

# Periodic Safety Review - Final Document Review Traveler



Bruce Power Document #: NK29-SFR-09701-00001	Revision: R000	Information Classification Internal Use Only	Usage Classification Information
Bruce Power Document Title: Safety Factor 1 – Plant Design			
Bruce Power Contract/Purchase Order: 00193829	Bruce Power Project #: 39075		
Supplier's Name: CANDESCO		Supplier Document #: K-421231-00201	Revision: R00
Supplier Document Title: Safety Factor 1 – Plant Design			

<b>Accepted for use at Bruce Power by:</b>	<b>Signature:</b>	<b>Date</b>
Name: Gary Newman Title: Chief Engineer & Sr. Vice President, Engineering		30 SEP 2016.

Acceptance of this document does not relieve the  
Supplier of responsibility for any errors or omissions

# Periodic Safety Review - Final Document Review Traveler

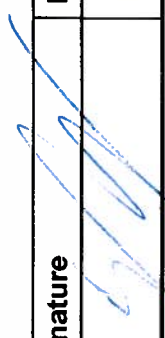
Sheet # 2 of 5

Bruce Power Document #:	NK29-SFR-09701-00001	Rev #: R000	Information Classification: Internal Use Only	Usage Classification: Information
Bruce Power Document Title:	Safety Factor 1 – Plant Design	Suppliers Name:	CANDESCO	
Bruce Power Contract/ Purchase Order:	00193829	Supplier Document Title:	Safety Factor 1 – Plant Design	
Bruce Power Project #:	39075	Supplier Document:	K-421231-00201	Rev #: R00

## Reviewed By:

Name	Title	Department	Signature	Date
Fred Rance	Sr. Technical Specialist	Nuclear Safety Analysis and Support	electronic acceptance	18Aug2016
Neman Ali	Sr. Technical Engineer	Nuclear Safety Analysis and Support	electronic acceptance	23Aug2016
Ken Chuong	Sr. Technical Specialist	Nuclear Safety Analysis and Support	electronic acceptance	23Aug2016
Richard Scrannage	Technical Engineer	Nuclear Safety Analysis and Support	electronic acceptance	24Aug2016
Jason Goldberg (RegC AR 28563014.14)	Department Manager	Nuclear Safety Analysis and Support		
Andrew Maksymyk (RegC AR 28563014.13)	Department Manager	Reactor Safety Support		

## Recommended for Use By:

Name	Title	Department	Signature	Date
Peter Purdy (RegC AR 28563014)	Division Manager	Reactor Safety Engineering		Apr-29/16

NOTE: Per meeting held with VP, NQA on September 28<sup>th</sup>, 2016 concerns with working of some of the macro gaps will be addressed with the addition of context-setting text in the GAE and IP documents. *Apr-29/16*

## Periodic Safety Review - Final Document Review Traveler

Sheet # 2 of 5

Bruce Power Document #:	NK29-SFR-09701-00001	Rev #: R000	Information Classification: Internal Use Only	Usage Classification: Information
Bruce Power Document Title:	Safety Factor 1 - Plant Design	Suppliers Name:	CANDESCO	
Bruce Power Contract/ Purchase Order:	00193829	Supplier Document Title:	Safety Factor 1 - Plant Design	
Bruce Power Project #:	39075	Supplier Document:	K-421231-00201	Rev #: R00

Reviewed By:				
Name	Title	Department	Signature	Date
Fred Rance	Sr. Technical Specialist	Nuclear Safety Analysis and Support	electronic acceptance	18Aug2016
Neman Ali	Sr. Technical Engineer	Nuclear Safety Analysis and Support	electronic acceptance	23Aug2016
Ken Chuong	Sr. Technical Specialist	Nuclear Safety Analysis and Support	electronic acceptance	23Aug2016
Richard Scranage	Technical Engineer	Nuclear Safety Analysis and Support	electronic acceptance	24Aug2016
Jason Goldberg (RegC AR 28563014.14)	Department Manager	Nuclear Safety Analysis and Support		
Andrew Maksymyk (RegC AR 28563014.13)	Department Manager	Reactor Safety Support	<i>A. Maksymyk</i>	28 Sep 2016

Recommended for Use By:			
Name	Title	Department	Date
Peter Purdy (RegC AR 28563014)	Division Manager	Reactor Safety Engineering	

## Periodic Safety Review - Final Document Review Traveler

Sheet # 2 of 5

Bruce Power Document #:	NK29-SFR-09701-00001	Rev #: R000	Information Classification: Internal Use Only	Usage Classification: Information
Bruce Power Document Title:	Safety Factor 1 – Plant Design	Suppliers Name:	CANDESCO	
Bruce Power Contract/ Purchase Order:	00193829	Supplier Document Title:	Safety Factor 1 – Plant Design	
Bruce Power Project #:	39075	Supplier Document:	K-421231-00201	Rev #: R00

## Reviewed By:

Name	Title	Department	Signature	Date
Fred Rance	Sr. Technical Specialist	Nuclear Safety Analysis and Support	electronic acceptance	18Aug2016
Neman Ali	Sr. Technical Engineer	Nuclear Safety Analysis and Support	electronic acceptance	23Aug2016
Ken Chuong	Sr. Technical Specialist	Nuclear Safety Analysis and Support	electronic acceptance	23Aug2016
Richard Scrannage	Technical Engineer	Nuclear Safety Analysis and Support	electronic acceptance	24Aug2016
Jason Goldberg (RegC AR 28563014.14)	Department Manager	Nuclear Safety Analysis and Support	<i>AB</i>	24 Aug 2016
Andrew Maksymyk (RegC AR 28563014.13)	Department Manager	Reactor Safety Support		


## Recommended for Use By:

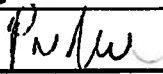
Name	Title	Department	Signature	Date
Peter Purdy (RegC AR 28563014)	Division Manager	Reactor Safety Engineering		

# Periodic Safety Review - Final Document Review Traveler

 Sheet # 3 of 5

Bruce Power Document #	NK29-SFR-09701-00001	Rev # R000	Information Classification: Internal Use Only	Usage Classification: Information
Bruce Power Document Title	Safety Factor 1 – Plant Design	Suppliers Name:	CANDESCO	
Bruce Power Contract/ Purchase Order:	00193829	Supplier Document Title:	Safety Factor 1 – Plant Design	
Bruce Power Project #	39075	Supplier Document:	K-421231-00201	Rev #: R00

Reviewed By:				
Name	Title	Department	Signature	Date
Martin Baumann	Shift Supervisor In Training	Bruce B Operations	electronic acceptance	15Jul2016
Colin Moranno (RegC AR 28562999.09)	Division Manager	Bruce B Operations		23SEP2016


Recommended for Use By:				
Name	Title	Department	Signature	Date
Paul Clark (RegC AR 28562999)	Plant Manager	Bruce B Operations		23 Sep 16

## Periodic Safety Review - Final Document Review Traveler

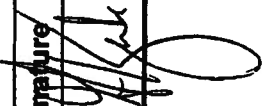
Sheet # 4 of 5

Bruce Power Document #:	NK29-SFR-09701-00001	Rev #: R000	Information Classification: Internal Use Only	Usage Classification: Information
Bruce Power Document Title:	Safety Factor 1 – Plant Design	Suppliers Name:	CANDESCO	
Bruce Power Contract/ Purchase Order:	00193829	Supplier Document Title:	Safety Factor 1 – Plant Design	
Bruce Power Project #:	39075	Supplier Document:	K-421231-00201	Rev #: R000

## Reviewed By:

Name	Title	Department	Signature	Date
Rob Dunn	Section Manager	Reactor Design	electronic acceptance	30Aug2016
Jim Slawson (RegC AR 28563002.08)	Department Manager	Mechanical & Civil		21 Sep 2016

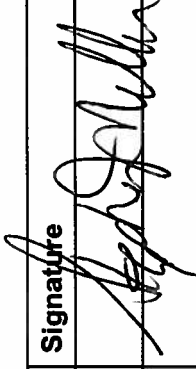
## Recommended for Use By:

Name	Title	Department	Signature	Date
Gord Kozak (RegC AR 28563002)	Division Manager	Engineering Support		29 Sep 2016

# Periodic Safety Review - Final Document Review Traveler

Sheet # 5 of 5

Bruce Power Document #:	NK29-SFR-09701-00001	Rev #: R000	Information Classification: Internal Use Only	Usage Classification: Information
Bruce Power Document Title:	Safety Factor 1 – Plant Design	Suppliers Name:	CANDESCO	
Bruce Power Contract/ Purchase Order:	00193829	Supplier Document Title:	Safety Factor 1 – Plant Design	
Bruce Power Project #:	39075	Supplier Document:	K-421231-00201	Rev #: R00

Reviewed By:				
Name	Title	Department	Signature	Date
Stephen Miller (RegC AR 28563003.07)	Department Manager	Equipment Reliability Integration		21 SEP 2016

Recommended for Use By:			
Name	Title	Department	Date
Kevin Pickles (RegC AR 28563003)	Division Manager	Station Engineering	22 SEP 2016

# Periodic Safety Review - Final Document Review Traveler

Sheet # \_\_\_\_\_ of \_\_\_\_\_

Bruce Power Document #:		Rev #:	Information Classification: Internal Use Only	Usage Classification: Information
Bruce Power Document Title:		Suppliers Name:		
Bruce Power Contract/ Purchase Order:		Supplier Document Title:		
Bruce Power Project #:		Supplier Document:		Rev #:

<b>Reviewed By:</b>				
<b>Name</b>	<b>Title</b>	<b>Department</b>	<b>Signature</b>	<b>Date</b>

<b>Recommended for Use by:</b>				
<b>Name</b>	<b>Title</b>	<b>Department</b>	<b>Signature</b>	<b>Date</b>



Sheet # \_\_\_\_\_ of \_\_\_\_\_

Bruce Power Document #:		Rev #:	Information Classification: Internal Use Only	Usage Classification: Information
Bruce Power Document Title:		Suppliers Name:		
Bruce Power Contract/ Purchase Order:		Supplier Document Title:		
Bruce Power Project #:		Supplier Document:		Rev #:

Reviewed By:				
Name	Title	Department	Signature	Date

Recommended for Use By:			
Name	Title	Department	Date




**NK29-SFR-09701-00001**

**Title: Safety Factor 1 - Plant Design**


**File: K-421231-00201-R00**



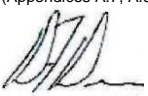
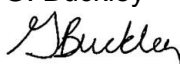
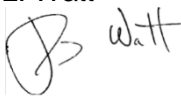
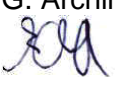

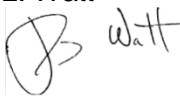
**A Report Submitted to Bruce Power**


**September 20, 2016**

 <div>canDESCO</div> <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

<b>Issue</b>  R00D0	<b>Reason for Issue:</b>  For harmonization				
	Author: P. Ardenska C. Cuddy D. Duncan (Appendices A.7, A.8, and A.9)	Verifier:	Reviewer:	Approver:	Date:  June 7, 2016
<b>Issue</b>  R00D1	<b>Reason for Issue:</b>  For internal review				
	Author: P. Ardenska C. Cuddy D. Duncan (Appendices A.7, A.8, and A.9)	Verifier:	Reviewer: L. Watt G. Archinoff D. Duncan (except for Appendices A.7, A.8, and A.9)	Approver:	Date:  June 9, 2016
<b>Issue</b>  R00D2	<b>Reason for Issue:</b>  For Bruce Power review				
	Author: P. Ardenska C. Cuddy D. Duncan (Appendices A.7, A.8, and A.9)	Verifier: G. Buckley	Reviewer: L. Watt G. Archinoff D. Duncan (except for Appendices A.7, A.8, and A.9)	Approver:	Date:  July 13, 2016
<b>Issue</b>  R00D3	<b>Reason for Issue:</b>  Addresses Bruce Power review comments and internal verification comments.				
	Author: P. Ardenska C. Cuddy D. Duncan (Appendices A.7, A.8, and A.9)	Verifier: G. Buckley	Reviewer: L. Watt G. Archinoff D. Duncan (except for Appendices A.7, A.8, and A.9)	Approver:	Date:  Sept 1, 2016


 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Issue  R00	Reason for Issue:				
	For use				
	Author: P. Ardenska   C. Cuddy   D. Duncan (Appendices A.7, A.8, and A.9) 	Verifier: G. Buckley 	Reviewer: L. Watt   G. Archinoff   D. Duncan (except for Appendices A.7, A.8, and A.9) 	Approver: L. Watt 	Date: Sept 20, 2016
Document Classification: Report		Security Classification: Client Proprietary			


 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## Table of Contents


<b>Acronyms and Abbreviations .....</b>	<b>vii</b>
<b>1. Objective and Description .....</b>	<b>1</b>
1.1. Objective .....	1
1.2. Description .....	2
<b>2. Methodology of Review .....</b>	<b>3</b>
<b>3. Applicable Codes and Standards .....</b>	<b>5</b>
3.1. Acts and Regulations .....	5
3.2. Power Reactor Operating Licence .....	5
3.3. Regulatory Documents .....	10
3.4. CSA Standards .....	12
3.5. International Standards .....	17
3.6. Other Applicable Codes and Standards .....	19
<b>4. Overview of Bruce B Station Programs and Processes .....</b>	<b>21</b>
4.1. Pressure Boundary Quality Assurance Program .....	24
4.1.1. Relevant Statutory, Regulatory, and Licensing Requirements Addressed by the Program .....	26
4.1.2. Implementing Procedures .....	27
4.2. Plant Design Basis Management .....	27
4.2.1. Relevant Statutory, Regulatory, and Licensing Requirements Addressed by the Program .....	27
4.2.2. Implementing Procedures .....	28
4.3. Engineering Change Control Program .....	29
4.3.1. Relevant Statutory, Regulatory, and Licensing Requirements Addressed by the Program .....	30
4.3.2. Implementing Procedures .....	31
4.4. Configuration Management .....	32
4.4.1. Relevant Statutory, Regulatory and Licensing Requirements Addressed by the Program .....	33
4.4.2. Implementing Procedures .....	33
<b>5. Results of the Review .....</b>	<b>34</b>
5.1. List of SSCs Important to Safety .....	35
5.2. Verification that Plant Design Supports Plant Safety and Performance .....	36
5.3. Identification of Differences Between Standards Met by NPPs Design and Modern Codes and Standards .....	38
5.3.1. Review Against Changes to CSA N287.1-14 General Requirements for Concrete Containment Structures for Nuclear Power Plants .....	39
5.3.2. Review Against Changes to CSA N287.3-14 Design Requirements for Concrete Containment Structures for Nuclear Power Plants .....	39
5.3.3. Review Against Changes to CSA N289.1-08 (R2013) General Requirements for Seismic Design and Qualification of CANDU Nuclear Power Plants .....	40
5.3.4. Review Against Changes to CSA N289.2-10 Ground Motion Determination for Seismic Qualification of Nuclear Power Plants .....	41
5.3.5. Review Against Changes to CSA N289.3-10 Design Procedures for Seismic Qualification of Nuclear Power Plants .....	41

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

5.3.6.	Review Against Changes to CSA N289.4-12 Testing Procedures for Seismic Qualification of Nuclear Power Plant SSCs .....	42
5.3.7.	Review Against Changes to CSA N289.5-12 Seismic Instrumentation Requirements for Nuclear Power Plants and Nuclear Facilities .....	43
5.3.8.	Review Against CSA N290.0-11 Requirements for Emergency Core Cooling Systems of Nuclear Power Plants .....	44
5.3.9.	Review Against Changes to CSA N290.1-13 Requirements for the Shutdown Systems of Nuclear Power Plants .....	44
5.3.10.	Review Against CSA N290.2-11 Requirements for Emergency Core Cooling Systems of Nuclear Power Plants .....	44
5.3.11.	Review Against CSA N290.3-11 Requirements for Containment Systems of Nuclear Power Plants .....	44
5.3.12.	Review Against CSA N290.11-13 Requirements to Reactor Heat Removal Capability During Outage of Nuclear Power Plants .....	44
5.3.13.	Review Against CSA N291-15 Requirements for Safety-Related Structures for Nuclear Power Plants.....	45
5.3.14.	Review Against CNSC G-149 Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors.....	45
5.3.15.	Review Against CNSC REGDOC-2.5.2.....	45
5.3.16.	Review Against ANSI/NIRMA CM-1.0-2007, Guidelines for Configuration Management of Nuclear Facilities .....	45
5.3.17.	Review Against ASME BPVC Section III, Section VIII and B31.1 .....	45
5.3.18.	Review Against NFPA-805 (2015) Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plant .....	46
5.4.	Adequacy of Design Basis Documentation .....	46
5.5.	Compliance with Plant Design Specifications .....	48
5.6.	Safety Analysis Report or Licensing Basis .....	50
5.7.	Plant SSCs Important to Safety .....	52
5.8.	Spent Fuel Storage Strategy .....	55
<b>6.</b>	<b>Interfaces with Other Safety Factors .....</b>	<b>57</b>
<b>7.</b>	<b>Program Assessments and Adequacy of Implementation.....</b>	<b>58</b>
7.1.	Self-Assessments .....	59
7.1.1.	SA-COM-2015-03 Configuration Management Engineering Governance Review ..	61
7.1.2.	SA-COM-2015-05 N286.7 Design Engineering Implementation .....	62
7.1.3.	SA-COM-2015-06 Pressure Boundary Assessment .....	63
7.1.4.	SA-ERI-2015-17 Station Engineering Setting and Reinforcing Standards .....	63
7.2.	Internal and External Audits and Reviews .....	64
7.2.1.	AU-2015-00020 Fire Protection Program .....	65
7.2.2.	AU-2015-00018 Temporary Change Control .....	65
7.2.3.	AU-2015-00006 Pressure Boundary Quality Assurance Program Section 18.....	67
7.2.4.	AU-2015-00007 Pressure Boundary Quality Assurance Program (excluding Section 18 Audit).....	67
7.2.5.	AU-2014-00002 Pressure Boundary Quality Assurance Program (excluding Section 18 Audit).....	68
7.2.6.	AU-2013-00015 PassPort Equipment Data Management.....	69
7.2.7.	AU-2012-00015 Critical Drawing Management.....	70
7.3.	Regulatory Evaluations and Reviews .....	71

 <div style="font-size: small;">Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


7.3.1.	Bruce B: CNSC Type II Compliance Inspection Report: BRPD-B-2016-002, Environmental Qualification Program, New Action Item 2016-07-7682.....	72
7.3.2.	CNSC Type II Compliance Inspection Report: BRPD-AB-2015-013 Bruce A and B Generating Stations Quarterly Field Inspection Report for Q1 2015-16 [208], Q2 2015-16 [209] and Q3 2015-16 [210].....	73
7.3.3.	Action Item 2015-07-6855: CNSC Type II Compliance Inspection Report : BRPD-AB-2015-004 Fukushima Verifications [211].....	73
7.3.4.	CNSC Type II Compliance Inspection: Implementation of the Engineering Change Control Process [212].....	74
7.3.5.	Bruce B CNSC Compliance Inspection Report : BRPD-AB-2012-011- Pressure Boundary Program Compliance at Bruce Power [214].....	74
7.4.	Performance Indicators .....	75
8.	<b>Summary and Conclusions .....</b>	<b>75</b>
9.	<b>References .....</b>	<b>81</b>
<b>Appendix A – High-Level Assessments Against Relevant Codes and Standards .....</b>		<b>A-1</b>
A.1.	<b>CNSC G-149, Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors .....</b>	<b>A-1</b>
A.2.	<b>Changes to CSA N287.1-14, General Requirements for Concrete Containment Structures for Nuclear Power Plants .....</b>	<b>A-3</b>
A.3.	<b>CSA N287.3-14, Design Requirements for Concrete Containment Structures for Nuclear Power Plants .....</b>	<b>A-6</b>
A.4.	<b>CSA N291-15, Requirements for Safety-Related Structures for Nuclear Power Plants A-8</b>	
A.5.	<b>NFPA-805 (2015), Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plant .....</b>	<b>A-10</b>
A.6.	<b>ANSI/NIRMA CM 1.0-2007, Guidelines for Configuration Management of Nuclear Facilities .....</b>	<b>A-13</b>
A.7.	<b>ASME BPVC Section III, Rules for Construction of Nuclear Power Plant Components A-27</b>	
A.8.	<b>ASME BPVC Section VIII, Design and Fabrication of Pressure Vessels .....</b>	<b>A-32</b>
A.9.	<b>ASME B31.1, Code for Power Piping .....</b>	<b>A-35</b>
A.10.	<b>CSA N290.0-11, General Requirements for Safety Systems of Nuclear Power Plants A-37</b>	
A.11.	<b>CSA N290.2-11, Requirements for emergency core cooling systems of nuclear plants .....</b>	<b>A-48</b>
A.12.	<b>CSA N290.3-11, Requirements for the containment system of nuclear plants.....</b>	<b>A-56</b>
A.13.	<b>CSA N290.11-13, Requirements for reactor heat removal capability during outage of nuclear power plants .....</b>	<b>A-64</b>
<b>Appendix B – Clause-by-Clause Assessments Against Relevant Codes and Standards B-1</b>		
B.1.	<b>CSA N290.1-13, Requirements for the Shutdown Systems of Nuclear Power PlantsB-2</b>	
B.2.	<b>CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants.....</b>	<b>B-42</b>

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## List of Tables


Table 1: Codes, Standards, and Regulatory Documents Referenced in Bruce A and B PROL and LCH.....	5
Table 2: Regulatory Documents.....	10
Table 3: CSA Standards .....	12
Table 4: International Standards .....	18
Table 5: Related Codes and Standards .....	19
Table 6: Bruce Power Programs Related to Plant Design .....	22
Table 7: Internal Self-Assessments Relevant to Plant Design .....	59
Table 8: Key Issues .....	76
Table B1: CSA N290.1-13, Requirements for the Shutdown Systems of Nuclear Power Plants B-2	
Table B2: CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plant .....	B-42




 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## Acronyms and Abbreviations


<b>AECB</b>	Atomic Energy Control Board
<b>AHJ</b>	Authority Having Jurisdiction
<b>AIA</b>	Authorized Inspection Agency
<b>ANSI</b>	American National Standards Institute
<b>AOO</b>	Anticipated Operational Occurrence
<b>AOR</b>	Analysis of Record
<b>AR</b>	Action Request
<b>ASDV</b>	Atmospheric Steam Discharge Valves
<b>ASME</b>	American Society of Mechanical Engineers
<b>BDBAs</b>	Beyond Design Basis Accidents
<b>BEP</b>	Boiler External Piping
<b>BP</b>	Bruce Power
<b>BPMS</b>	Bruce Power Management System
<b>BPVC</b>	Boiler and Pressure Vessel Code
<b>CANDU</b>	Canada Deuterium Uranium
<b>CAFF</b>	Channel Cooling in the Absence of Forced Flow
<b>CCI</b>	Corium/Concrete Interaction
<b>CFAM</b>	Corporate Functional Area Manager
<b>CFVS</b>	Containment Filtered Venting System
<b>CIC</b>	Configuration Information Changes
<b>CM</b>	Configuration Management
<b>CNSC</b>	Canadian Nuclear Safety Commission
<b>COG</b>	CANDU Owners Group
<b>CSA</b>	Canadian Standards Association
<b>CSDV</b>	Condenser Steam Discharge Valves
<b>DBA</b>	Design Basis Accident
<b>DBE</b>	Design Basis Earthquake
<b>DCN</b>	Design Change Notice
<b>DCP</b>	Design Change Package
<b>DD</b>	Design Description

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


<b>DEC</b>	Design Extension Condition
<b>DRL</b>	Derived Release Limits
<b>EA</b>	Environmental Assessment
<b>EC</b>	Engineering Change
<b>ECC</b>	Engineering Change Control
<b>ECI</b>	Emergency Coolant Injection
<b>ECIS</b>	Emergency Coolant Injection Supply
<b>EFADS</b>	Emergency Filtered Air Discharge System
<b>EFPD</b>	Effective Full Power Days
<b>EQ</b>	Environmental Qualification
<b>EQIS</b>	Environmental Qualification Information System
<b>EQ SRCL</b>	Environmental Qualification Safety Related Component List
<b>ERP</b>	Equipment Reliability Program
<b>ESS</b>	Emergency Storage System
<b>FAI</b>	Fukushima Action Items
<b>FASA</b>	Focus Area Self-Assessment
<b>FCI</b>	Facility Configuration Information
<b>GIO</b>	Global Improvement Opportunity
<b>GSS</b>	Guaranteed Shutdown State
<b>HTS</b>	Heat Transport System
<b>HX</b>	Heat Exchangers
<b>IAEA</b>	International Atomic Energy Agency
<b>IFB</b>	Irradiated Fuel Bay
<b>ISR</b>	Integrated Safety Review
<b>IST</b>	Industry Standard Toolset
<b>ITP</b>	Inspection and Test Plan
<b>IUC</b>	Instrument Uncertainty Calculation
<b>LCH</b>	Licence Conditions Handbook
<b>LCMP</b>	Life Cycle Management Plan
<b>LLOCA</b>	Large Loss-of-Coolant Accident
<b>LOCA</b>	Loss-of-Coolant Accident
<b>LTEP</b>	Long Term Energy Plan

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


<b>LVRF</b>	Low Void Reactivity Fuel
<b>M&amp;TE</b>	Measure & Test Equipment
<b>MCR</b>	Major Component Replacement
<b>MCS</b>	Maintenance Cooling System
<b>MEL</b>	Master Equipment List
<b>MP</b>	Maintenance Program
<b>MSM</b>	Management System Manual
<b>NBCC</b>	National Building Code of Canada
<b>NERP</b>	Nuclear Emergency Response Plan
<b>NFCC</b>	National Fire Code of Canada
<b>NIRMA</b>	Nuclear Information and Records Management Association
<b>NOP</b>	Neutron Overpower
<b>NORA</b>	Nuclear Oversight and Regulatory Affairs
<b>NPP</b>	Nuclear Power Plant
<b>NSA</b>	Nuclear Safety Assessment
<b>NSAS</b>	Nuclear Safety Analysis and Support
<b>NSCA</b>	Nuclear Safety and Control Act
<b>NUPIC</b>	Nuclear Procurement Issues Committee
<b>OFI</b>	Opportunities for Improvements
<b>OLC</b>	Operational Limit and Conditions
<b>OP&amp;P</b>	Operating Policies and Principles
<b>OPEX</b>	Operating Experience
<b>OPG</b>	Ontario Power Generation
<b>OSR</b>	Operational Safety Requirements
<b>PARs</b>	Passive Autocatalytic Recombiners
<b>PB</b>	Pressure Boundary
<b>PB QA</b>	Pressure Boundary Quality Assurance
<b>PBQAP</b>	Pressure Boundary Quality Assurance Program
<b>PDE</b>	Plant Design Engineering
<b>PE</b>	Procurement Engineering
<b>PHT</b>	Primary Heat Transport
<b>PO&amp;C</b>	Performance Objectives and Criteria

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

<b>PRA</b>	Probabilistic Risk Assessment
<b>PROL</b>	Power Reactor Operating Licence
<b>PSA</b>	Probabilistic Safety Assessment
<b>PSR</b>	Periodic Safety Review
<b>QA</b>	Quality Assurance
<b>RLE</b>	Review Level Earthquake
<b>RS</b>	Reactor Safety
<b>SAM</b>	Severe Accident Management
<b>SAMG</b>	Severe Accident Management Guidelines
<b>SBR</b>	Safety Basis Report
<b>SCA</b>	Safety and Control Area
<b>SCR</b>	Station Condition Record
<b>SDCS</b>	Shutdown Cooling (System)
<b>SDE</b>	Site Design Earthquake
<b>SDM</b>	System Design Manuals
<b>SDS</b>	Shutdown System
<b>SFR</b>	Safety Factor Report
<b>SIS</b>	Systems Important to Safety
<b>SMA</b>	Seismic Margin Assessment
<b>SOE</b>	Safe Operating Envelope
<b>SPDS</b>	Safety Parameter Display System
<b>SPOC</b>	Single Point of Contact
<b>SQ</b>	Seismic Qualification
<b>SR</b>	Safety Report
<b>SRI</b>	Safety Report Improvement
<b>SRLCs</b>	Seismic Review Level Conditions
<b>SRSL</b>	Safety Related System List
<b>SSCs</b>	Structures, Systems, and Components
<b>SSCTs</b>	Structures, Systems, Components, and Significant Tools
<b>TBD</b>	Technical Basis Document
<b>TCC</b>	Temporary Configuration Change
<b>TMOD</b>	Temporary Modification

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

<b>TOE</b>	Technical Operability Evaluation
<b>TSSA</b>	Technical Standards and Safety Authority
<b>VVRS</b>	Vault Vapour Recovery System
<b>WANO</b>	World Association of Nuclear Operators

 <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## 1. Objective and Description

Bruce Power (BP), as an essential part of its operating strategy, is planning to continue operation of Bruce B as part of its contribution to the Long Term Energy Plan (LTEP) (<http://www.energy.gov.on.ca/en/ltep/>). Bruce Power has developed integrated plant life management plans in support of operation to 247,000 Equivalent Full Power Hours in accordance with the Bruce Power Reactor Operating Licence (PROL) [1] and Licence Conditions Handbook (LCH) [2].

A more intensive Asset Management program is under development, which includes a Major Component Replacement (MCR) approach to replacing pressure tubes, feeders and steam generators, so that the units are maintained in a fit for service state over their lifetime. However, due to the unusually long outage and de-fuelled state during pressure tube replacement, there is an opportunity to conduct other work, and some component replacements that could not be done reasonably in a regular maintenance outage will be scheduled concurrently with MCR. In accordance with Licence Condition 15.2 of the PROL [1], Bruce Power is required to inform the Canadian Nuclear Safety Commission (CNSC) of any plan to refurbish a reactor or replace a major component at the nuclear facilities, and Bruce Power shall:

- (i) Prepare and conduct a periodic safety review;
- (ii) Implement and maintain a return-to-service plan; and
- (iii) Provide periodic updates on progress and proposed changes.


The fifteen reports prepared as part of the Periodic Safety Review (PSR), including this Safety Factor Report (SFR), are intended to satisfy Licence Condition 15.2 (i) as a comprehensive evaluation of the design, condition and operation of the nuclear power plant (NPP). In accordance with Regulatory Document REGDOC-2.3.3 [3], a PSR is an effective way to obtain an overall view of actual plant safety and the quality of safety documentation and determine reasonable and practicable improvements to ensure safety until the next PSR.

Bruce Power has well-established PSR requirements and processes for the conduct of a PSR for the purpose of life-cycle management, which are documented in the procedure Periodic Safety Reviews [4]. This procedure, in combination with the Bruce B Periodic Safety Review Basis Document [5], governs the conduct of the PSR and facilitates its regulatory review to ensure that Bruce Power and the CNSC have the same expectations for scope, methodology and outcome of the PSR.

This PSR supersedes the Bruce B portion of the interim PSR that was conducted in support of the ongoing operation of the Bruce A and Bruce B units until 2019 [6]. Per REGDOC-2.3.3 [3], subsequent PSRs will focus on changes in requirements, facility conditions, operating experience and new information rather than repeating activities of previous reviews.

### 1.1. Objective

The overall objectives of the Bruce B PSR are to conduct a review of Bruce B against modern codes and standards and international safety expectations, and to provide input to a practicable

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


set of improvements to be conducted during the MCR in Units 5 to 8, and during asset management activities to support ongoing operation of all four units, as well as U0B, that will enhance safety to support long term operation. It will cover a 10-year period, since there is an expectation that a PSR will be performed on approximately a 10-year cycle, given that all units are expected to be operated well into the future.

The specific objective of the review of this Safety Factor is to determine the adequacy of the design of the nuclear power plant and its documentation by assessment against modern national and international standards and practices.

## 1.2. Description

The review is conducted in accordance with the Bruce B PSR Basis Document [5], which states that the review covers Structures, Systems, and Components (SSCs) important to safety unless modified otherwise. The scope of the tasks will depend on the extent of changes in standards and/or the licensing basis since the previous PSR(s). The review of plant design (including site characteristics) includes the following tasks:

1. Review of the list of SSCs important to safety for completeness and adequacy.
2. Review to verify that design and other characteristics are appropriate to meet the requirements for plant safety and performance for all plant conditions and the applicable period of operation, including:
  - The prevention and mitigation of events (faults and hazards) that could jeopardize safety;
  - The application of defence in depth and engineered barriers for preventing the dispersion of radioactive material (integrity of fuel, cooling circuit and containment building);
  - Safety requirements (for example, on the dependability, robustness and capability of SSCs important to safety); and
  - Design codes and standards.
3. Identification of differences between standards met by the nuclear power plant's design (for example, the standards and criteria in force when it was built) and modern nuclear safety and design standards;
4. Review of the adequacy of the design basis documentation;
5. Review for compliance with plant design specifications;
6. Review of the safety analysis report or licensing basis documents following plant modifications and in light of their cumulative effects and updates to the site characterization;
7. Review of plant SSCs important to safety to ensure that they have appropriate design characteristics and are arranged and segregated in such a way as to meet modern requirements for plant safety and performance, including the prevention and mitigation of events that could jeopardize safety; and

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

8. Review of the strategy for the spent fuel storage and conduct of an engineering assessment of the condition of the storage facilities, the records management and the inspection regimes being used.

As required by the PSR Basis Document, preparation of this Safety Factor Report included an assessment of the review tasks to determine if modifications were appropriate. Any changes to the review tasks described in this section are documented and justified in Section 5.

## 2. Methodology of Review

As discussed in the Bruce B PSR Basis Document [5], the methodology for a PSR should include making use of safety reviews that have already been performed for other reasons. Accordingly, the Bruce B PSR makes use of previous reviews that were conducted for the following purposes:

- Return to service of Bruce Units 3 and 4 (circa 2001) [7];
- Life extension of Bruce Units 1 and 2 (circa 2006) [8] [9] [10];
- Proposed refurbishments of Bruce Units 3 and 4 (circa 2008) [11] [12] [13] [14] [15];
- Safety Basis Report (SBR) and PSR for Bruce Units 1 to 8 (2013) [6]; and
- Bruce A Integrated Safety Review (ISR) to enhance safety and support long term operation (2015) [16] [17].

These reviews covered many, if not all, of the same Safety Factors that are reviewed in the current PSR. A full chronology of Bruce Power safety reviews up to 2013 is provided in Appendix F of [18].

The Bruce B PSR Safety Factor review process comprises the following steps:

1. **Interpret and confirm review tasks:** As a first step in the Safety Factor review, the Safety Factor Report author(s) confirm the review tasks identified in the PSR Basis Document [5] and repeated in Section 1.2 to ensure a common understanding of the intent and scope of each task. In some cases, this may lead to elaboration of the review tasks to ensure that the focus is precise and specific. Any changes to the review tasks are identified in Section 5 of the Safety Factor Report (SFR) and a rationale provided.
2. **Confirm the codes and standards to be considered for assessment:** The Safety Factor Report author(s) validates the list of codes and standards presented in the PSR Basis Document against the defined review tasks to ensure that the assessment of each standard will yield sufficient information to complete the review tasks. Additional codes and standards are added if deemed necessary. If no standard can be found that covers the review task, the assessor may have to identify criteria on which the assessment of the review task will be based. The final list of codes and standards considered for this Safety Factor is provided in Section 3.
3. **Determine the type and scope of assessment to be performed:** This step involves the assessor confirming that the assessment type identified in Appendix C of the Bruce B PSR Basis Document [5] for each of the codes, standards and guidance documents selected for




 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

this factor is appropriate based on the guidance provided. The PSR Basis Document provides an initial assignment for the assessment type, selecting one of the following review types:

- Programmatic Clause-by-Clause Assessments;
- Plant Clause-by-Clause Assessments;
- High-Level Programmatic Assessments;
- High-Level Plant Assessments;
- Code-to-Code Assessments; or
- Confirm Validity of Previous Assessment.

The final assessment types are identified in Section 3, along with the rationale for any changes relative to the assignment types listed in the PSR Basis Document.

4. **Perform gap assessment against codes and standards:** This step comprises the actual assessment of the Bruce Power programs and the Bruce B plant against the identified codes and standards. In general, this involves determining from available design or programmatic documentation whether the plant or program meet the provisions of the specific clause of the standard or of some other criterion, such as a summary of related clauses. Each individual deviation from the provisions of codes and standards is referred to as a Safety Factor “micro-gap”. The assessments, performed in Appendix A and Appendix B, include the assessor’s arguments conveying reasons why the clause is considered to be met or not met, while citing appropriate references that support this contention.
5. **Assess alignment with the provisions of the review tasks:** The results of the assessment against codes and standards are interpreted in the context of the review tasks of the Safety Factor. To this end, each assessment, whether clause-by-clause, high-level or code-to-code, is assigned to one or more of the review tasks (Section 5). Assessment against the provision of the review task involves formulating a summary assessment of the degree to which the plant or program meets the objective and provisions of the particular review task. This assessment may involve consolidation and interpretation of the various compliance assessments to arrive at a single compliance indicator for the objective of the review task as a whole. The results of this step are documented in Section 5 of each SFR.
6. **Perform program assessments:** The most pertinent self-assessments, audits and regulatory evaluations are assessed, and performance indicators relevant to the Safety Factor identified. The former illustrates that Bruce Power has a comprehensive process of reviewing compliance with Bruce Power processes, identifying gaps, committing to corrective actions, and following up to confirm completion and effectiveness of these actions. The latter demonstrates that there is a metric by which Bruce Power assesses the effectiveness of the programs relevant to the Safety Factor in Section 7. Taken as a whole, these demonstrate that the processes associated with this Safety Factor are implemented effectively (individual findings notwithstanding). Thus, program effectiveness, if not demonstrated explicitly in the review task assessments in Step 5, can be inferred if Step 5 shows that Bruce Power processes meet the Safety Factor requirements and if this step shows there are ongoing processes to ensure compliance with Bruce Power processes.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

7. **Identification of findings:** This step involves the consolidation of the findings of the assessment against codes and standards and the results of executing the review tasks into a number of definitive statements regarding positive and negative findings of the assessment of the Safety Factor. Positive findings or strengths are only identified if there is clear evidence that the Bruce B plant or programs exceed compliance with the provision of codes and standards or review task objectives. Each individual negative finding or deviation is designated as a Safety Factor micro-gap for tracking purposes. Identical or similar micro-gaps are consolidated into comprehensive statements that describe the deviation known as Safety Factor macro-gaps, which are listed in Section 8 of the Safety Factor Reports, as applicable.

### 3. Applicable Codes and Standards

This section lists the applicable regulatory requirements, codes and standards considered in the review of this Safety Factor. Table C-1 of the Bruce B PSR Basis Document [5] identifies the codes, standards and guides that are relevant to this PSR. Modern revisions of some codes and standards listed in Table C-1 of the PSR Basis Document [5] have been identified in the licence renewal application and supplementary submissions for the current PROL [19] [20] [21]. Codes, standards and guides issued after the freeze date of December 31, 2015 were not considered in the review [5].

#### 3.1. Acts and Regulations


The Nuclear Safety and Control Act (NSCA) [22] establishes the Canadian Nuclear Safety Commission and its authority to regulate nuclear activities in Canada. Bruce Power has a process to ensure compliance with the NSCA [22] and its Regulations. Therefore, the NSCA and Regulations were not considered further in this review.

#### 3.2. Power Reactor Operating Licence

The list of codes and standards related to plant design that are referenced in the PROL [1] and LCH [2], and noted in Table C-1 of the Bruce B PSR Basis Document [5], are identified in Table 1. The edition dates referenced in the third column of the table are the modern versions used for comparison.

**Table 1: Codes, Standards, and Regulatory Documents Referenced in Bruce A and B PROL and LCH**


Document Number	Document Title	Modern Version used for PSR Comparison	Type of Review
CNSC REGDOC-2.3.3	Periodic Safety Reviews	[3]	NA

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Document Number	Document Title	Modern Version used for PSR Comparison	Type of Review
CNSC REGDOC-2.4.2 (2014)	Probabilistic Safety Assessment For Nuclear Power Plants	[23]	2SF
CNSC RD-327	Nuclear Criticality Safety	[24]	NA
CNSC G-278	Human Factors Verification and Validation	[25]	NA
CSA N285.0-08	General Requirements For Pressure-Retaining Systems And Components In CANDU Nuclear Power Plants	CSA N285.0-12 [26]	NA
CSA N286-05 [27]	Management System Requirements for Nuclear Facilities	CSA N286-12 [28]	NA
CSA N286.7-99	Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants	CSA N286.7-99 (R2012) [29]	NA
CSA N288.4-10 (R2015)	Environmental Monitoring Programs at Class I Nuclear Facilities	[30]	2SF
CSA N290.13-05 (R2010)	Environmental Qualification Of Equipment For CANDU Nuclear Power Plants	[31]	NA
CSA N290.15-10 (R2015)	Requirements for the Safe Operating Envelope of Nuclear Power Plants	[32]	NA
CSA N293-07	Fire Protection For CANDU Nuclear Power Plants	CSA N293-12 [33]	2SF
Assessment type: <b>NA:</b> Not Assessed; <b>CBC:</b> Clause-by-Clause; <b>PCBC:</b> Partial Clause-by-Clause; <b>CTC:</b> Code-to-Code; <b>HL:</b> High Level; <b>2SF:</b> Assessment performed in another SFR; <b>CV:</b> Confirm Validity of Previous Assessments			

**CNSC REGDOC-2.3.3:** This PSR is being conducted in accordance with CNSC REGDOC-2.3.3 per Licence Condition 15.2 (i) [1], and associated compliance verification criteria [2]. Therefore, REGDOC-2.3.3 is not reviewed further in this document.

**CNSC REGDOC-2.4.2:** CNSC REGDOC-2.4.2 [23] sets out the requirements of the CNSC with respect to the probabilistic safety assessment. This document is the second version of Probabilistic Safety Assessment (PSA) for Nuclear Power Plants. It supersedes the previous

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

version of the same title that was identified as S-294. CNSC REGDOC-2.4.2 includes amendments to reflect lessons learned from the Fukushima nuclear event of March 2011, and to address findings from the CNSC Fukushima Task Force Report, as applicable to S-294. In comparison with S-294, CNSC REGDOC-2.4.2 contains additional guidance clauses that elaborate further on the requirements and/or provide direction on how to meet the requirements. Table C-1 of the PSR Basis Document [5] calls for a clause-by-clause assessment of REGDOC-2.4.2 to be performed and documented in Safety Factor 6. Results of the clause-by-clause assessment performed in Safety Factor 6 are used to support the review tasks listed in Section 5.

**CNSC RD-327:** CNSC RD-327 [24] provides requirements for prevention of criticality accidents in the handling, storage, processing, and transportation of fissionable materials and the long-term management of nuclear waste. Analysis has been performed to address any potential for criticality for Low Void Reactivity Fuel (LVRF) stored at Bruce B [21]. Bruce Power is currently fully aligning current practices documenting compliance with RD-327 within applicable governance for Bruce B [21]. An update was provided on October 28, 2015, which identifies that an internal gap assessment has been completed and requested an extension of compliance from October 31, 2015 to May 31, 2016 [34]. Table C-1 of the PSR Basis Document [5] does not call for this code to be assessed (i.e., assessment type is 'Not Assessed'). This is also discussed in Section 5.8.

**CNSC G-278:** CNSC G-278 [25] describes the effective human factors verification and validation planning. This guidance is listed under the compliance verification criteria for Licence Conditions 2.2, and 5.1 and therefore is not assessed further for the purposes of this PSR.

**CSA N285.0-12:** Canadian Standards Association (CSA) N285.0-12 [26] provides general requirements for pressure-retaining systems and components. Table C-1 of the PSR Basis Document [5] does not call for this code to be assessed (i.e., assessment type is 'Not Assessed').

**CSA N286-12:** CSA N286-05 [27] is noted in the PROL (Licence Condition 1.1 [1]). Per the LCH [2], an implementation strategy for the 2012 version is in progress to be submitted to the CNSC by the end of January 2016. CNSC staff have stated that in their view the CSA N286-12 version of CSA N286 “does not represent a fundamental change to the current Bruce Power Management System” and have acknowledged that “the new requirements in CSA N286-12 are already addressed in Bruce Power's program and procedure documentation” [35].

Bruce Power had agreed to perform a gap analysis and to prepare a detailed transition plan, and to subsequently implement the necessary changes in moving from the CSA N286-05 version of the code to the CSA N286-12 version, during the current licensing period [36]. This timeframe will facilitate the implementation of N286 changes to the management system, and enable the gap analysis results from the large number of new or revised Regulatory Documents or Standards committed in the 2015 operating licence renewal. Bruce Power has also proposed that in the interim, CSA N286-05 be retained in the PROL to enable it to plan the transition to CSA N286-12, and committed to develop the transition plan and communicate the plan to the CNSC by January 30, 2016 [37]. Bruce Power further stated CSA N286-12 does not establish any significant or immediate new safety requirements that would merit a more accelerated implementation. The gap analysis and the resulting transition plan were submitted to the CNSC [38]. Per [38], the major milestones of the transition plan to N286-12 are as follows:

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- 22 January 2016: Discuss all the regulatory actions and the transition plan at the Corporate Functional Area Manager (CFAM) meeting
- 31 December 2016: Revision of CFAM Program Document(s) [with LCH notification requirements to the CNSC] to comply with CSA N286-12 requirements completed.
- 31 March 2017: Revision of CFAM Program Document(s) [that do not have LCH notification requirements to the CNSC] to comply with CSA N286-12 requirements completed
- 31 December 2017: Confirmation that that all impacted documents in the program suite comply with the requirements of CSA N286-12
- 15 September 2018: Verification via a FASA that previously identified transition Gaps to meeting the requirements of CSA N286-12 have been addressed and effectively implemented
- 14 December 2018: issue notification to the CNSC regarding state of CSA N286-12 readiness, and, implementation date

This Safety Factor therefore has not performed a code-to-code assessment between CSA N286-05 and CSA N286-12 and will not be performing a clause-by-clause assessment of CSA N286-05, since it is in the current licence and there is a transition plan in effect.

**CSA N286.7-99:** CSA N286.7-99 [29] provides quality assurance requirements for the design, development, maintenance, modification, and use of computer programs that are used in nuclear power plant applications. The use of computer software for design makes this standard relevant in that it provides quality assurance requirements in conjunction with CNSC G-149 [39], which is discussed in Section 3.3. Relevant aspects of the plant design and associated safety analysis (refer to Safety Factor 5) predate CSA N286.7-99 and were performed using legacy tools that do not fully meet CSA N286.7-99 requirements. Currently, Bruce Power's Plant Design Basis Management Program BP-PROG-10.01 is intended to satisfy relevant statutory, regulatory and licensing requirements including CSA N286.7-99. Compliance with N286.7-99 is a condition of the PROL, so this standard is subject to ongoing compliance assessment. Per licence condition 4.2 [2] design and analysis computer codes and software used to support the safe operation are in accordance with CSA N286.7-99. Engineering analysis software covers the domain of highly specialized, high performance systems or software, used by a group of specialists for analysis and analytical simulation in support of the business, as defined in BP-PROC-00326 [40]. Systems in this domain are normally qualified in a manner to satisfy CSA N286.7, regulators or professional licensing. As noted in the Engineering Analysis Software procedure DIV-ENG-00006 [41], if the software is to be used for design analysis of nuclear safety related systems, CSA N286.7 must be specified as a quality requirement. Therefore, Table C-1 of the PSR Basis Document [5] does not call for this code to be assessed (i.e., assessment type is 'Not Assessed').

**CSA N288.4-10:** CSA N288.4-10 [30] addresses monitoring of radioactive and non-radioactive contaminants, physical stressors, potential biological effects, and pathways for both human and non-human biota. A high level review of the 2010 edition of CSA N288.4 has been conducted and documented in Safety Factor 14. In the licence renewal application [19], Bruce Power provided implementation and transition measures, and committed to full implementation of N288.4-10 by December 2018. These commitments were subsequently included in the LCH [2]




 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

and are discussed further in Safety Factor 14. For this reason, the review type has been changed from Table C-1 of the PSR Basis Document [5] that calls for a high-level assessment in Safety Factor 1 to refer to the assessment documented in Safety Factor 14.

**CSA N290.13-05:** CSA N290.13 [31] specifies the requirements for an environmental qualification program for Canada Deuterium Uranium (CANDU) NPPs. The modern version of this standard is the same as that referenced in the PROL. Therefore, Table C-1 of the PSR Basis Document [5] does not call for this code to be assessed (i.e., assessment type is 'Not Assessed').

**CSA N290.15-10:** CSA N290.15-10 [32] is the first edition of this standard. It provides requirements for the definition, implementation, and maintenance of the safe operating envelope at nuclear power plants. Guidance material for existing CANDU nuclear power plants has been provided in an annex to supplement the requirements. This standard addresses one of the main objectives of deterministic safety analysis, which is to derive or confirm operational limits and conditions that are consistent with the design and safety requirements for the nuclear power plant. As noted in the LCH, Bruce Power is moving towards the implementation of a Safe Operating Envelope (SOE) program, which will provide the comprehensive identification of all operating limits and conditions in compliance with the requirements of CSA N290.15 [32]. The initial SOE objectives were to comply with COG-02-901 [42], which predates CSA N290.15; however, the requirements of CSA N290.15 were considered in the development of Bruce Power's SOE program. Bruce Power has performed a number of assessments and has initiated actions to confirm compliance to the requirements of CSA N290.15-10, both at the program level and at the detailed level. At the program level, a clause by clause assessment of Bruce Power compliance to this standard has been performed and documented in [43]. The review demonstrated that the minimum requirements for compliance to the standard have been met and no additional documentation changes are required. Additional work is required to ensure alignment with general governance programs, in particular with BP-PROG-01.02 Bruce Power Management System Management and BP-PROG-03.01, Document Management. At the detailed level, a number of initiatives have been put in place to alleviate any concerns regarding the comprehensive identification and implementation of all required safety analysis requirements as part of the SOE program [44]. The combination of actions to verify the initial Operational Safety Requirements (OSR) bases and implementation, to improve the interface with associated procedures and to review the compliance to each OSR provides sufficient assurance that the SOE program is comprehensively addressing all the requirements of CSA N290.15-10 and accordingly no further assessment against CSA requirements are performed in this PSR. Table C-1 of the PSR Basis Document [5] does not call for this code to be assessed (i.e., assessment type is 'Not Assessed').

**CSA N293-12:** CSA N293-12 [33] provides the minimum fire protection requirements for the design, construction, commissioning, operation, and decommissioning of NPPs. A recent review of the Bruce Power Fire Protection Program against CSA N293-07 has been performed [45] to satisfy a commitment to the CNSC to provide an assessment of the Fire Protection Program at Bruce A/B, including the alignment with Fire Protection Codes and Standards [18]. Table C-1 of the PSR Basis Document [5] calls for the review of Safety Factor 7 to include a code-to-code assessment of the differences between CSA N293-12 [33] and CSA N293-07 (R2011). Safety Factor 7 presents this code-to-code assessment, along with an incremental clause-by-clause assessment for those clauses in CSA N293-12 that do not have a

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

corresponding equivalent in CSA N293-07. These results are used in the assessment of this Safety Factor.


### 3.3. Regulatory Documents

In addition to those listed in the PROL [1] and the LCH [2], the Regulatory Documents identified in Table C-1 of the PSR Basis Document [5] considered for application to review tasks of this Safety Factor are included in Table 2.

**Table 2: Regulatory Documents**

Document Number	Document Title	Reference	Type of Review
CNSC R-10 (1977)	The Use of Two Shutdown Systems in Reactors	[46]	NA
CNSC R-77 (1987)	Overpressure Protection Requirements for Primary Heat	[47]	NA
CNSC G-149 (2000)	Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors	[39]	HL
CNSC G-276	Human Factors Engineering Program Plans	[48]	2SF
CNSC RD-346	Site Evaluation for New Nuclear Power Plants	[49]	NA
CNSC REGDOC-2.5.2 (2014)	Design of Reactor Facilities: Nuclear Power Plants	[50]	CBC
Assessment type: <b>NA:</b> Not Assessed; <b>CBC:</b> Clause-by-Clause; <b>PCBC:</b> Partial Clause-by-Clause; <b>CTC:</b> Code-to-Code; <b>HL:</b> High Level; <b>2SF:</b> Assessment performed in another SFR; <b>CV:</b> Confirm Validity of Previous Assessments			

**CNSC R-10:** CNSC R-10 [46] provides requirements for the shutdown systems in reactors. Part II, Section 3 of this regulatory document identifies the design requirements for the use of two shutdown systems for reactors and thus is relevant to design. The CNSC has reviewed and reorganized its regulatory framework program in order to develop a more robust, manageable and up-to-date regulatory requirements framework. A key objective of the review was ensuring that CNSC regulatory requirements are well defined and supported by additional guidance, as necessary. CNSC staff has been working with the CSA Group to develop amendments to CSA N290.1, Requirements for the Shutdown Systems of CANDU Nuclear Plants, to incorporate all necessary existing requirements currently available in R-10. With the publication of this standard, CNSC R-10 is no longer reflecting the current regulatory environment and as such during FY 2012-13 [51] it was identified that it is not necessary to maintain CNSC R-10 and it

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

can be withdrawn and archived. Therefore, Table C-1 of the PSR Basis Document [5] does not call for this code to be assessed (i.e., assessment type is 'Not Assessed').

**CNSC R-77:** CNSC R-77 [47] provides overpressure protection requirements for primary heat transport systems in CANDU power reactors fitted with two shutdown systems, and is relevant to plant design. A clause-by-clause review of R-77 was conducted in Enclosure 3 of [9] as part of the Bruce 1 and 2 ISR. Bruce A was found to be fully compliant with the requirements based on the results in the Safety Report for accidents which lead to pressurization of the heat transport system, i.e., Electrical System failures; Feedwater and Steam Supply System Failures; Loss of Reactivity or Power Control; and Loss of Pressure Control (high). In [52], it is demonstrated that for all safety analysis accidents leading to pressurization of the heat transport system:

- The conclusions derived in Enclosure 3 of [9] regarding compliance of Bruce A safety analysis to R-77 Heat Transport System (HTS) overpressure requirements remain valid for the current (2012) version of the Bruce A Safety Report;
- The Bruce B overpressurization results in the current (2011) version of the Bruce B Safety Report [53] show that Bruce B is also compliant with R-77 HTS overpressure requirements.

Table C-1 of the PSR Basis Document [5] does not call for this code to be assessed (i.e., assessment type is 'Not Assessed').


**CNSC G-149:** CNSC G-149 [39] provides guidance on the development, maintenance and use of computer programs used for the design of a NPP. A high level review of CNSC G-149 has been performed as part of this PSR and documented in Safety Factor 5. A summary of the assessment findings is presented in Appendix A (A.1).

**CNSC G-276:** CNSC G-276 [48] describes the elements of the effective human factors engineering program planning documentation. A high level review of CNSC G-276 has been performed as part of this PSR and documented in Safety Factor 12. For this reason, the review type has been changed from Table C-1 of the PSR Basis Document [5] that calls for a high-level assessment in Safety Factor 1 to refer to the assessment of G-276 documented in Safety Factor 12.

**CNSC RD-346:** CNSC RD-346 [49] covers evaluation of sites for new NPPs (or plants) before application is made for a Licence to Prepare Site, and before an environmental assessment (EA) determination is initiated. It represents the CNSC staff's adoption, or where applicable, adaptation of the principles set forth by the International Atomic Energy Agency (IAEA) in NS-R-3, Site Evaluation for Nuclear Installations [54]. The latest assessment was performed in the 2008 Bruce 3 and 4 ISR Safety Factor 7 per NK21-CORR-00531-06076 [14], which concluded "[t]he IAEA guides under NS-R-3 relate to siting which has been addressed as part of the Environmental Assessment which has already been accepted by the CNSC". The same logic applies to CNSC RD-346, and therefore, Table C-1 of the PSR Basis Document [5] does not call for this code to be assessed (i.e., assessment type is 'Not Assessed').

**CNSC REGDOC-2.5.2:** CNSC REGDOC-2.5.2 [50] sets out requirements and guidance for new licence applications for water-cooled NPPs. It establishes a set of comprehensive design requirements and guidance that are risk-informed and align with accepted international codes and practices. This document provides criteria pertaining to the safe design of new water-



	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


cooled NPPs. The Design of Reactor Facilities: Nuclear Power Plants supersedes RD-337, which was published in 2008. In addition, it implements recommendations from the CNSC Fukushima Task Force Report. Table C-1 of the PSR Basis Document [5] calls for a clause-by-clause assessment of CNSC REGDOC-2.5.2, which is documented in Appendix B (B.2).

### 3.4. CSA Standards


In addition to those identified in the Bruce Power PROL [1] and LCH [2], the CSA standards identified in Table C-1 of the PSR Basis Document [5] considered for application to review tasks of this Safety Factor are included in Table 3.

**Table 3: CSA Standards**

Document Number	Document Title	Reference	Type of Review
CSA B51-14 (2014)	Boiler, Pressure Vessel, and Pressure Piping Code	[55]	NA
CSA N287.1-14	General Requirements for Concrete Containment Structures for Nuclear Power Plants	[56]	HL
CSA N287.2-08 (R2013)	Material Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants	[57]	CV
CSA N287.3-14	Design Requirements for Concrete Containment Structures for Nuclear Power Plants	[58]	CTC/HL
CSA N287.4-09	Construction, Fabrication, and Installation Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants	[59]	CV
CSA N287.5-11	Examination and Testing Requirements for Concrete Containment Structures for Nuclear Power Plants	[60]	CV
CSA N287.6-11	Pre-Operational Proof and Leakage Rate Testing Requirements for Concrete Containment Structures for Nuclear Power Plants.	[61]	NA

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Document Number	Document Title	Reference	Type of Review
CSA N289.1-08	General Requirements for Seismic Design and Qualification of CANDU Nuclear Power Plants	[62]	HL
CSA N289.2-10	Ground Motion Determination for Seismic Qualification of Nuclear Power Plants	[63]	HL
CSA N289.3-10	Design Procedures for Seismic Qualification of Nuclear Power Plants	[64]	HL
CSA N289.4-12	Testing Procedures for Seismic Qualification of Nuclear Power Plant Structure, Systems and Components	[65]	HL
CSA N289.5-12	Seismic Instrumentation Requirements for Nuclear Power Plants and nuclear facilities	[66]	HL
CSA N290.0-11 (2011)	General Requirements for safety systems of nuclear power plants	[67]	HL
CSA N290.1-13	Requirements for the Shutdown Systems of Nuclear Power Plants	[68]	CBC
CSA N290.2-11 (2011)	Requirements for emergency core cooling systems of nuclear power plants	[69]	HL
CSA N290.3-11 (2011)	Requirements for the containment system of nuclear power plants	[70]	HL
CSA N290.4-11	Requirements for Reactor Control Systems of Nuclear Power Plants	[71]	CV
CSA N290.5 (2006; Reaffirmed 2011)	Requirements for Electrical Power and Instrument Air Systems of CANDU Nuclear Power Plants	[72]	CV
CSA N290.6-09 (R2014)	Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of an Accident	[73]	CV

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Document Number	Document Title	Reference	Type of Review
CSA N290.11-13	Requirements for reactor heat removal capability during outage of nuclear power plants	[74]	HL
CSA N290.12-14	Human Factors in Design for Nuclear Power Plants	[75]	2SF
CSA N291-15	Requirements for Safety-Related Structures for Nuclear Power Plants	[76]	HL


Assessment type:

**NA:** Not Assessed; **CBC:** Clause-by-Clause; **PCBC:** Partial Clause-by-Clause; **CTC:** Code-to-Code;  
**HL:** High Level; **2SF:** Assessment performed in another SFR; **CV:** Confirm Validity of Previous Assessments

**CSA B51-14:** CSA B51-14 [55] provides requirements for boilers, pressure vessels, pressure piping and fittings. Table C-1 of the PSR Basis Document [5] indicates that assessment of CSA B51-14 should confirm validity however, the review type was changed to not assessed. CSA B51 is incorporated in the regulatory structure because this standard is called directly by CSA N285.0, which is in the Bruce PROL and subject to a transition plan. Therefore, no further review of CSA B51 is needed in support of this Safety Factor Report.

**CSA N287.1-14:** CSA N287.1-14 [56] provides general requirements for the design, fabrication, construction, installation, examination, and commissioning, as well as the in-service examination, testing, and evaluation of reinforced (prestressed and non-prestressed) concrete containment structures for nuclear power plants designated as class containment. Table C-1 of the PSR Basis Document [5] calls for a code-to-code assessment followed by a high-level assessment of the differences; however a high level review of the entire current version of this standard was completed. The results of this review are presented in Appendix A (A.2). A code-to-code followed by a clause-by-clause assessment has been performed in Safety Factor 4.

**CSA N287.2-08, CSA N287.4-09, CSA N287.5-11:** CSA N287.2-08 [57], CSA N287.4-09 [59], CSA N287.5-11 [60] address requirements for the materials, construction, fabrication, installation, examination and testing of concrete containment structures. As noted in the 2013 assessment [6], in applying these standards, the relevant systems important to safety are the parts of the Bruce B containment envelope that include the four Reactor Vaults, Central Fuelling Area, Fuelling Duct, East Service Area, Pressure Relief Ducts, Pressure Relief Valve Manifold and Vacuum Building. Also forming part of the containment boundary are containment appurtenances, which include airlocks/transfer chambers, dampers and penetration seals. The containment system was designed, constructed, and installed as part of initial construction of the station. The adequacy of the containment structure design to meet release requirements during postulated Design Basis Accidents is established by analysis documented in Part 3 of the Safety Report (Appendix 5.6 Containment Response and Dose Assessment) [53]. In addition, as part of Fukushima safety improvements, Bruce Power has completed the analysis and

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

assessment activities to evaluate options for ensuring containment integrity and filtered venting in the event of a multi-unit severe accident. The final report documented in [77] concluded that existing design capability and emergency mitigation measures aimed at preventing severe core damage represent a viable alternative to the installation of a filter vent system dedicated to management of containment pressure during severe accidents. Therefore the existing design means to protect containment integrity and uncontrolled releases are adequate [78]. In order to provide the option for a future portable system, a Containment Filtered Venting System (CFVS) connection point was installed in Bruce B during the Vacuum Building outage in 2015 [78]. Bruce Power is performing supplementary evaluations of further improvements by the end of 2016 and is tracking the project progress under AI 2015-07-3683. No new construction or other permanent modifications have been made to the containment structures to necessitate compliance of the original containment construction to the new standards. Table C-1 of the PSR Basis Document [5] calls for a confirmation of validity of previous assessments. For the reasons stated above, a review against CSA N287.2-08, CSA N287.4-09, CSA N287.5-11 was not repeated for the purposes of the review tasks in this Safety Factor Report.

**CSA N287.3-14:** CSA N287.3-14 [58] specifies requirements for the design of concrete containment structures of a containment system and addresses their beyond design basis assessment. Table C-1 of the PSR Basis Document [5] calls for a high-level assessment, to support this high-level assessment a code-to-code comparison of the 1978 version against the 2014 version of this standard was performed to identify the significant differences. The results of a high level review are presented in Appendix A (A.3).

**CSA N287.6-11:** CSA N287.6-11 [61] specifies requirements for pre-operational proof and leakage rate testing of concrete containment structures of a containment system that are designated as class containment components. Concrete containment structures after completion but before criticality, shall be tested in accordance with the requirements of this standard. As noted in clause 8.1, for existing plants, there is a requirement to perform proof and leakage-rate tests for containment structures in accordance with CSA N287.7-08. This testing was last documented in the Bruce B 2015 Containment and Vacuum building Pressure test final results [79]. Table C-1 of the PSR Basis Document [5] does not call for this code to be assessed (i.e., assessment type is 'Not Assessed').

**CSA N289.1-08:** CSA N289.1-08 [62] defines a seismic success path as the “minimum set of SSCs that can perform the required nuclear safety functions following an earthquake.” The seismic qualification of Bruce B is addressed in Safety Factor 3. The adequacy of the plant design to accommodate seismic events is also addressed by the seismic Probabilistic Safety Assessment (PSA) in Safety Factor Report 6. An update in September 2014 added new requirements, such as the periodic evaluation of a beyond design basis earthquake (Clause 5.3.11) and consideration of the effects of aging (Clause 5.4.3). The September 2014 update also clarified a number of other requirements regarding the application of the seismic margin assessment methodology, and updated the reference publications (including the N289 series). The results of a high level review of the current version of this standard are presented in Section 5.3.3.

**CSA N289.2-10:** CSA N289.2-10 [63] describes the investigations required to obtain the seismological and geological information necessary to determine, for a proposed or existing NPP site, the seismic ground motion that will be used in seismic qualification of safety-related plant structures and systems, and the potential for seismically induced phenomena that can

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

have a direct or indirect effect on plant safety or operation. The results of a high level review are presented in Section 5.3.4.

**CSA N289.3-10:** CSA N289.3-10 [64] applies to SSCs in NPPs that require seismic qualification by analytical methods and specifies the design requirements, criteria, and methods of analysis for determining the engineering representation of ground motion, ground response spectra, and floor response spectra for use in the design and seismic qualification of SSCs and for performing seismic qualification of specified SSCs by analytical methods. The results of a high level review are presented in Section 5.3.5.

**CSA N289.4-12:** CSA N289.4-12 [66] provides design requirements and methods for seismic qualification of specific components and systems by testing methods. The results of a high level review are presented in Section 5.3.6.

**CSA N289.5-12:** CSA N289.5-12 [66] describes the requirements for seismic instrumentation systems for NPPs and nuclear facilities to monitor site-specific seismic responses. A code-to-code comparison of the 1991 and 2012 editions of CSA N289.5 has been conducted. A high-level review of the differences introduced with the new code was performed as stated in Table C-1 of the PSR Basis Document [5]. The associated findings of the high-level review are addressed in Section 5.3.7.

**CSA N290.0-11:** CSA N290.0-11 [67] is the first edition of this standard and is one of the series of standards on reactor control systems, safety systems, and instrumentation for nuclear power plants. The standard covers the design, qualification, installation, operation, maintenance, inspection, and documentation of the safety systems for a water-cooled nuclear power plant. This standard defines the general requirements for the safety systems and is a companion document of CSA N290.2 and N290.3, which outline specific requirements. The results of a high-level review of this standard are presented in Appendix A (A.10).

**CSA N290.1-13:** CSA N290.1-13 [68] applies to the design, procurement, installation, commissioning, operation, testing, and maintenance requirements of reactor shutdown systems (SDSs) for existing and new water-cooled NPPs. The results of a clause-by-clause assessment are presented in Appendix B (B.1).

**CSA N290.2-11:** CSA N290.2-11 [69] is the first edition of this standard. The standard defines the requirements for the design, qualification, installation, operation, maintenance, inspection, and documentation of the emergency core cooling system for a water-cooled nuclear power plant. The standard also applies to all support systems required to ensure that the emergency core cooling system is able to maintain adequate heat transfer for as long as necessary to maintain the release of radioactive material within reference dose limits by limiting fuel failure. The results of a high-level review are presented in Appendix A (A.11).

**CSA N290.3-11:** CSA N290.3-11 [70] is the first edition of this standard and applies to the containment system of existing and new water-cooled nuclear power plants. The standard presents the general requirements for the containment system, and establishes the nuclear safety design, procurement, installation, and testing requirements to control and minimize radioactive releases. The results of a high-level review are presented in Appendix A (A.12).

**CSA N290.4-11:** CSA N290.4-11 [71] specifies the provisions for safe and effective control of reactor power. A code-to-code comparison of the 1982 and 2011 edition had been conducted in the 2013 Interim PSR assessment [6], which identified new or different clauses. These clauses



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

were assessed and no compliance gaps were identified against Bruce Power programs or design. No changes have been made to the programs or design that would invalidate this assessment. There have been no revisions or updates of the standard and the review remains applicable. The 2013 Interim PSR assessment of this standard [6] is, therefore, confirmed valid for the purposes of the review tasks for this Safety Factor.

**CSA N290.5-06:** CSA N290.5-06 (R2011) [72] covers the design, procurement, qualification, construction, installation, inspection, and documentation of CANDU NPP electrical power and instrument air systems. This version of the standard was assessed clause-by-clause in the 2013 Interim PSR [6], where one gap in the Units 3&4 design was identified against clause 6.2.3. The 2013 assessment is confirmed valid for the purposes of the review tasks in this Safety Factor Report.

**CSA N290.6-09:** CSA N290.6-09 [73] provides requirements for the design, testing, installation, and qualification of equipment for the display of NPP safety functions in the event of an accident. A code-to-code comparison of the 1982 and 2009 edition had been conducted in the 2013 Interim PSR [6], where no gaps were identified. There have been no revisions or updates of the standard and the review remains applicable. The 2013 assessment is confirmed valid for the purposes of the review tasks in this Safety Factor Report.

**CSA N290.11-13:** CSA N290.11-13 [74] is the first edition of this standard. The standard establishes the requirements for the design, qualification, installation, commissioning, operation, maintenance, testing, inspection, and documentation for systems providing heat removal from the reactor core to the ultimate heat sink(s) for water-cooled nuclear power plants during outages. This standard is limited to fuel cooling within the reactor core and does not cover spent fuel pool cooling, off-reactor fuelling operations, or the completely defueled core state. The results of a high level review of this standard are presented in Appendix A (A.13).

**CSA N290.12-14:** CSA N290.12-14 [75] Human factors in design applies to nuclear safety, protection of the environment, health and safety of persons, security and productivity. This standard covers human factors in design for existing and new nuclear power plants. Table C-1 of the PSR Basis Document [5] calls for a clause-by-clause assessment to be performed in Safety Factor 12. The results of the clause-by-clause review demonstrate that overall, Bruce Power meets the intent of the standard with some exceptions as documented in Safety Factor Report 12.

**CSA N291-15:** CSA N291-15 [76] provides material, design, construction, fabrication, inspection, and examination requirements for safety-related structures constructed of structural steel, reinforced concrete, and reinforced masonry. This standard is mentioned in the LCH [2] providing recommendations and guidance in support of Licence Conditions 5.1 and 6.1. The results of a high level review this standard are presented in Appendix A (A.4).

### 3.5. International Standards

The international standards listed in Table 4 are relevant to this Safety Factor and were considered for this review.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

**Table 4: International Standards**


Document Number	Document Title	Reference	Type of Review
ANSI/NIRMA CM 1.0-2007	Guidelines for Configuration Management of Nuclear Facilities	[80]	HL
ASME BPVC Section III	Rules for Construction of Nuclear Power Plant Components	[81]	HL
ASME BPVC Section VIII	Design and Fabrication of Pressure Vessels	[82]	HL
ASME B31.1	Code for Power Piping	[83]	HL
IAEA SSG-25	Periodic Safety Review For Nuclear Power Plants	[84]	NA
NFPA-805	Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants	[85]	HL
Assessment type: <b>NA:</b> Not Assessed; <b>CBC:</b> Clause-by-Clause; <b>PCBC:</b> Partial Clause-by-Clause; <b>CTC:</b> Code-to-Code; <b>HL:</b> High Level; <b>2SF:</b> Assessment performed in another SFR; <b>CV:</b> Confirm Validity of Previous Assessments			

**ANSI/NIRMA CM 1.0-2007:** ANSI/NIRMA CM 1.0-2007 [80] (American National Standards Institute/Nuclear Information and Records Management Association) establishes functional criteria for the cost-effective implementation of configuration management at a nuclear facility. Its purpose is to enable the implementation of configuration management so that equilibrium between design requirements, physical configuration and Facility Configuration Information can be achieved and maintained in order to reduce costs and risk of error. The results of a high level review are presented in Appendix A (A.6).

**ASME BPVC Section III:** American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code (BPVC) Section III [81] establishes rules of safety governing the design, fabrication and inspection of boilers and pressure vessels, including nuclear power systems. The results of a high level review are presented in Appendix A (A.7).

**ASME BPVC Section VIII:** ASME BPVC Section VIII [82] provides requirements applicable to the design, fabrication, inspection, testing, and certification of pressure vessels operating at either internal or external pressures exceeding 15 psig. The results of a high level review are presented in Appendix A (A.8).

**ASME B31.1:** ASME B31.1 [83] prescribes minimum requirements for the design, materials, fabrication, erection, test, and inspection of power and auxiliary service piping systems for

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

electric generation stations. The results of a high level review are presented in Appendix A (A.9).

**IAEA SSG-25:** IAEA SSG-25 [84] addresses the periodic safety review of nuclear power plants. Per the PSR Basis Document [5] this PSR is being conducted in accordance with REGDOC-2.3.3. As stated in REGDOC-2.3.3 [3], this regulatory document is consistent with IAEA SSG-25. The combination of IAEA SSG-25 and REGDOC-2.3.3, define the review tasks that should be considered for the Safety Factor Reports. However, no assessment is performed specifically on IAEA SSG-25.

**NFPA-805:** NFPA-805 [85] standard specifies the minimum fire protection requirements for existing light water nuclear power plants during all phases of plant operation, including shutdown, degraded conditions and decommissioning. The results of a high level review are presented in Appendix A (A.5).

### 3.6. Other Applicable Codes and Standards

Other applicable standards/practices listed in Table 5 were considered for this review.

**Table 5: Related Codes and Standards**

Document Number	Document Title	Reference	Type of Review
Darlington-DG-38-03650-1	Purpose and Application of Nuclear Safety Design Guides	[86]	NA
Darlington DG-38-03650-2A	Common Mode Incidents – Overview and Design Requirements	[87]	NA
Darlington DG-38-03650-2B	Common Mode Incidents – Seismic Design	[88]	NA
Darlington DG-38-03650-3	Limiting Consequential Damage of Postulated Pipe Ruptures	[89]	NA
Darlington DG-38-03650-4	Shutdown Systems	[90]	NA
Darlington DG-38-03650-5	Emergency Coolant Injection	[91]	NA
Darlington DG-38-03650-6	Containment	[92]	NA
Darlington DG-38-03650-7	Extensions of the Containment Envelope	[93]	NA



	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Document Number	Document Title	Reference	Type of Review
Darlington DG-38-03650-8	Environmental Qualification of Safety Related Equipment	[94]	NA
Darlington DG-38-03650-9	Safety Assessments	[95]	NA
NBCC (2015)	National Building Code of Canada	[96]	NA
NFCC (2015)	National Fire Code of Canada	[97]	NA
<p>Assessment type:</p> <p><b>NA:</b> Not Assessed; <b>CBC:</b> Clause-by-Clause; <b>PCBC:</b> Partial Clause-by-Clause; <b>CTC:</b> Code-to-Code; <b>HL:</b> High Level; <b>2SF:</b> Assessment performed in another SFR; <b>CV:</b> Confirm Validity of Previous Assessments</p>			

**Darlington Design Guides:** Clause-by-clause reviews were conducted against the Darlington Design Guides as part of the Bruce 1 and 2 ISR (Enclosure 4, NK21-CORR-00531-04059 [9]). In addition to the Bruce Power site design guides, Bruce B has a suite of engineering design guides which were used to describe the requirements of the design of units 5 to 8. The Bruce B Design Guides were prepared during a similar time period as the Darlington Design Guides which are no longer considered a modern code or standard. Therefore, Table C-1 of the PSR Basis Document [5] does not call for the Darlington Design Guides to be assessed (i.e., assessment type is 'Not Assessed').

**National Building Code of Canada:** The National Building Code (NBCC) [96] sets out technical provisions for the design and construction of new buildings. It also applies to the alteration, change of use and demolition of existing buildings. The updated seismicity map in the 2005 version of the code placed the Bruce site among the areas with lowest seismic activity in Canada and not affecting the plant's seismic design basis. The sections of the NBC related to concrete Containment Structures was reviewed as part of a Category 2 issue that flowed from the Bruce 1 and 2 ISR (see NK21-CORR-00531-05728 [98]). The assessment found that the requirements of the N287 Series of CSA Standards generally exceed the requirements of the NBC of Canada and concluded that there is no need to assess the containment structures for compliance with the requirements of the NBC 2005 - Part IV. As part of the methodology for the Fire Protection Code Compliance Review for Bruce B Units 5-8 (including Unit 0), NK29-REP-71400-00002 [99] states:

*"The majority of this code compliance evaluation compares the design of the facility to the requirements of the 1975 Edition of the National Building Code of Canada, as well as any other standards referenced by this code. Building codes, including the NBC, are rarely retroactive. Appendix A-1.1.1.1(1) of the NBC 2005 specifically states,*

*'It is not intended that the NBC be used to enforce the retrospective application of new requirements to existing buildings or existing portions of relocated buildings, unless specifically required by local regulations or bylaws...'"*

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

This rationale is applicable for the NBCC 2015, and therefore Table C-1 of the PSR Basis Document [5] does not call for this code to be assessed (i.e., assessment type is 'Not Assessed').

**National Fire Code of Canada:** The National Fire Code (NFCC) [97] contains technical requirements designed to provide an acceptable level of fire safety. It complements the NBC, and both must be considered when constructing, renovating or maintaining buildings. Unlike the Building Code, Fire Codes are commonly retroactive, therefore in accordance with the requirements of CSA N293-07 in order to meet NFCC for numerous clauses a 2005 National Fire Code clause-by-clause review was performed for Bruce B and is included in Appendix B of NK29-REP-71400-00002 [99]. The NFC, as well as fire protection related portions of the NBC were reviewed as part of the CSA N293 Gap Assessment [45] discussed above. This approach was taken because the provisions of CSA N293 are considered to be bounding those of the NFC. Therefore, Table C-1 of the PSR Basis Document [5] does not call for this code to be assessed (i.e., assessment type is 'Not Assessed').

## 4. Overview of Bruce B Station Programs and Processes


The Bruce Power Management System (BPMS) is the framework by which Bruce Power manages all aspects of its business, as documented in the Management System Manual (MSM) [100] and associated MSM Sheets [101] [102]. As stated in BP-MSM-1 [100], the BPMS ensures that Bruce Power meets the stipulations of its operating licences, other applicable codes, standards, legal and business requirements.

The BPMS Management program [103] establishes the governance, provides oversight, support and enables the maintenance of an integrated management system framework for Bruce Power.

Bruce Power uses programs to implement the MSM [100] and define regulatory and business requirements. BP-MSM-1 Sheet 0001 [101] contains the list of programs, program owners and approvers. Within each program is an associated hierarchy of documents, and primary procedures which implement the programs.


The Bruce Power programs that relate to plant design are identified in BP-MSM-1 Sheet 0001 [101] under the functional areas of Configuration Management Engineering and Equipment Reliability. The Program document, Program name, Accountable program owner, Accountable document approver and CNSC Notification requirements are defined in [101]. The related program documents are listed in Table 6<sup>1</sup>.

<sup>1</sup> Table 6 lists the key governance documents used to support the assessments of the review tasks for this Safety Factor Report. A full set of current sub-tier documents is provided within each current PROG document. In the list of references, the revision number for the governance documents is the key, unambiguous identifier; the date shown is an indicator of when the document was last updated, and is taken either from PassPort, the header field, or the "Master Created" date in the footer.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

**Table 6: Bruce Power Programs Related to Plant Design**

Level 0	Level 1	Level 2	Level 3
BP-MSM-1: Management System Manual [100]	BP-PROG-00.04: Pressure Boundary Quality Assurance Program [104]	BP-PROC-00915: Pressure Boundary Quality Assurance Program Oversight [105]	
	BP-PROG-10.01: Plant Design Basis Management [106]	BP-PROC-00335: Design Management [107]	
		BP-PROC-00363: Nuclear Safety Assessment [108]	
		DIV-ENG-00009: Design Authority [109]	
		BP-PROC-00582: Engineering Fundamentals [110]	
		BP-PROC-00502: Resolution of Differing Professional Opinions [111]	
	BP-PROG-10.02: Engineering Change Control (ECC) [112]	BP-PROC-00743: Site Services Engineering Change Control [113]	
		BP-PROC-00542: Configuration Information Change [114]	
		BP-PROC-00539: Design Change Package [115]	
		BP-PROC-00877: Modification Installation Quality Assurance [116]	

 <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Level 0	Level 1	Level 2	Level 3
		BP-PROC-00615: Commissioning Modifications and Projects [117]	
	BP-PROG-10.03: Configuration Management [118]	BP-PROC-00470: Configuration Management Program Oversight and Trending [119]	
		BP-PROC-00584: PassPort Equipment Data Management [120]	
		BP-PROC-00638: Temporary Configuration Change Management [121]	
		BP-PROC-00647: PassPort Permit Request Processing [122]	
		BP-PROC-00786: Margin Management [123]	
		BP-PROC-00898: Equipment Codes [124]	
		SEC-DO-00001: Drafting Office Work Management [125]	
	BP-PROG-11.01: Equipment Reliability [126]	BP-PROC-00778: Scoping and Identification of Critical SSCs [127]	DPT-RS-00012: Systems Important to Safety (SIS) Decision Methodology [128]
	BP-PROG-03.01, Document Management [129]	BP-PROC-00169: Safety Related System List [130]	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Each of these programs, and key supporting processes, are described in the following subsections.

#### 4.1. Pressure Boundary Quality Assurance Program


The Pressure Boundary Quality Assurance Program (PB QA Program or PBQAP) [104] ensures that all technical and QA requirements necessary to meet regulatory and licence requirements related to pressure boundary are integrated into the business processes comprising Bruce Power's Management System in order to control the quality of pressure boundary activities at the company facilities.

The PB QA Program is organized to cover nuclear pressure boundary activities and conventional pressure boundary activities. Nuclear pressure boundary activities apply to work performed in nuclear class registered systems in Bruce A and B. They also apply to work performed in conventional registered systems at Bruce Power site but outside of the station protected areas (referred to as Centre of Site). These are conducted in accordance with CSA N285.0 [26]. Conventional pressure boundary activities apply to work performed in non-nuclear class registered systems located in Bruce A and B. These are also conducted in accordance with CSA N285.0 [26]. The PB QA Program document [104], Section A, Section 1.2, states that Centre of Site activities, including the steam pipeline to the Bruce Energy Centre, are performed in accordance with CSA N285.0 [26] and CSA B51 [55].

Section 3 of the PB QA Program describes the processes that control design activities, including preparation and issue of design documents and changes thereto, design analysis, design verification and control of design interfaces. The Chief Engineer and Senior VP Engineering is the Bruce Power Design Authority and has overall responsibility for design and design control activities. As the Program Owner, the Manager, Engineering Support Division is responsible for ensuring that the corporate Plant Design Basis Management Program [106] and Engineering Change Control Program [112], together with associated implementing procedures, comply with the requirements of the PB QA Program Section 3.

The elements of PBQA design control included in Reference [104] are:

- Design process, including:
  - Requirements for the design process
  - Design specification
  - Design input
  - Design output, and
  - Design analyses.
- Design verification, including:
  - Requirements for design verification
  - Design reviews

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- Alternate calculations, and
- Qualification tests.
- Requirements for classification and design registration;
- Requirements for change control;
- Requirements for design interface control; and
- Requirements for design documentation and records.

In accordance with Compliance Verification Criteria specified in the LCH, Section 5.2, Bruce Power is adopting of CSA N285.0-12 including Update No. 1 (2013) and update No. 2 (2014). Bruce Power reviewed the changes from the 2008 edition of N285.0 to the 2012 edition (with Updates No. 1 and No. 2) to identify the impacts on its PBQAP manual and lower tier governance used to implement program requirements.

Due to the adoption of certain aspects of the 2012 edition of N285.0 within the previous licensing period via the LCH and within Bruce Power's Pressure Relief Valve Testing and Repair Program, Bruce Power is compliant to the requirements of N285.0 (2012 including Updates No. 1 and No. 2) and there are no additional transition measures required in this area.

Bruce Power was targeting implementation of the updated PBQAP manual, compliant to N285.0 (2012 with Updates No. 1 and No. 2) upon receipt of the renewed PROL and LCH. Thereafter, and in accordance with the change control provisions within the Technical Standards and Safety Authority (TSSA) accepted PBQAP manual (BP-PROG-00.04) [104], procedural updates and training must be completed within six months; however Bruce Power completed full implementation by the end of August 2015. Bruce Power has also completed and submitted a roadmap of PBQAP that meets the requirements of Annex N of the updated N285.0 standard [131]. Annex N of the updated CSA N285.0 provides a format for pressure boundary program to comply with the requirements of Clause 15 which states "the licensee shall have a pressure boundary document(s) that indicates how the requirements of this Standard are addressed by the licensee's process and procedures for a nuclear facility". Three internal audits of the PBQAP have been performed by Bruce Power and were reviewed for the purposes of this report (see Section 7). One audit verified if Bruce Power's performance criteria, established in Section 18 of N285.0-12, were met in BP-PROG-00.04 Revision 22 [104]. This audit determined the effectiveness of Section 18 of the program (see Section 7.2.3). As discussed in Section 7.2.3, the audit identified that adverse conditions identified during PB audits are not always completed within timeline requirements.

The second internal audit was performed in 2014 to verify Bruce Power's compliance with all sections of N285.0-08, excluding Section 18 (Audits) (see section 0). The audit identified repeat findings indicating that previous activities taken to address the adverse conditions were not successful. Seven areas were considered to be continuing findings, meaning that there were open assignments that had yet to be completed; therefore the adverse conditions still existed. The audit evaluated that BP-PROG-00.04-R020 [132] was not fully compliant in 18 of the 19 sections. Additionally, the audit found that some elements were either not fully implemented, or organizational compliance is such that the defined process may not function as intended.



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

The third internal audit carried out in 2015 verified Bruce Power's compliance with all sections, excluding Section 18 (Audits), of the requirements of CSA N285.0-12, including Update #1 and Update #2. The criteria used in the audit are from the applicable sections of Bruce Power's Pressure Boundary Quality Assurance Program BP-PROG-00.04 Revision 22 [104], along with the procedures that implement those sections of the program manual. The program was evaluated to be not fully effective in 4 of the 18 Sections that were evaluated under the scope of this audit and not fully compliant in 15 of the 18 Sections that were evaluated under the scope of this audit. One of the more significant challenges to the program is the inadequacy within the suite of PBQA implementing governance for the identification of performance criteria and associated activities for verification and oversight (see Section 7.2.5).

Due to the numerous issues that require effective resolution to ensure a robust program and repeat findings from previous audits this is assessed as a gap (SF1-21) in Table 8. It is noted that the majority of the Station Condition Records (SCRs) related to this audit are complete.

Registration of previously unregistered systems and legacy system design changes has been planned and prioritized. Bruce Power has committed to having all Bruce B system design registrations (including system classification lists) updated by December 31, 2017.

The Program identifies two exceptions to its scope. It does not apply to relief valve testing and repair conducted under Bruce Power Procedure BP-PROC-00078 [133] Quality Program Manual for Testing and Repair of Pressure Relief Valves. The Program does not apply to inaugural and periodic inspection and testing performed in accordance with CSA N285.4 and CSA N285.5, nor to re-inspection and re-certification of in-service pressure vessels.

#### **4.1.1. Relevant Statutory, Regulatory, and Licensing Requirements Addressed by the Program**

BP-PROG-00.04 [104], last revised in May of 2015, does not provide a summary of the relevant statutory, regulatory, and licensing requirements, nor does the document provide a mapping to demonstrate that relevant clauses are met through implementing procedures. This gap is reflected as SF1-21 in Table 8. The document does, however, refer to the following standards within the Program:

- CSA N285.0 (including references to ASME III, Division 1);
- ASME Section III, Article NCA-9000;
- ASME Section III, Appendices;
- ASME NQA-1;
- CSA B51;
- ASME B31.1;
- ASME B31.3; and
- ASME B31.5.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

#### **4.1.2. Implementing Procedures**

The processes identified in PBQAP (BP-PROG-00.04, [104]) Section 3 that control design activities are implemented by procedures in other programs, specifically Plant Design Basis Management, Engineering Change Control, and Configuration Management, as described in the following sections.

Managers responsible for implementing portions of this Program are required to regularly assess the adequacy of that part of the Program for which they are responsible and are to assure its effective implementation. The methods of performing and documenting these assessments are described in BP-PROC-00915 [105], Pressure Boundary Quality Assurance Program Oversight.

#### **4.2. Plant Design Basis Management**

The objective of the plant design basis management program [106] is to maintain the design basis and to ensure that the plant can operate safely for the full duration of the operating life of the plant. The processes contained under the elements of this program provide consistent methods for performance of the Engineering work and other activities required to meet the program objectives.

This program ensures that the plant design meets safety, reliability and regulatory requirements including pressure boundary quality assurance requirements described in BP-PROG-00.04 [104], PB QA. Additionally, this program sets out requirements for engineering analysis and documentation, such that the adequacy of the design can be demonstrated. At Bruce Power, effective June 1, 2015, an individual shall be a Professional Engineer licensed in the Province of Ontario in order to perform engineering work or their work shall be supervised by a Professional Engineer licensed in the Province of Ontario [106].

##### **4.2.1. Relevant Statutory, Regulatory, and Licensing Requirements Addressed by the Program**

As identified in Section 5.1 of the Program [106], the relevant Statutory, Regulatory and Licensing Requirements addressed by the Program are:

- ASME BPVC 2007, Section III, Rules for Construction of Nuclear Facility Components;
- ASME NQA-1-1994, Quality Assurance Requirements for Nuclear Facility Applications;
- Bruce B Nuclear Power Reactor Operating Licence PROL 16.00/2014<sup>2</sup>;
- CSA N285.0-08/N285.6 Series-08 (with Update No. 1, June/09);
- CSA N286-05, specifically:
  - Clauses 5.5, 5.8, 5.9 and 5.10 - Management System Generic Requirements;

<sup>2</sup> BP-PROG-10.01-R009, Plant Design Basis Management, has not been updated since PROL 18.00 came into effect.



 <div style="font-size: small;">Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- Clauses 6.1 - Design, 6.2.1 and 6.2.2 - Safety Analysis and Safety Analysis Control, 6.2.3 Safety Report, 6.3 - Safe Operating Envelope and 6.4 Purchasing and Material Management;
- Annex A.1, A.2, A.3, A.4, A.5, A.6.2, A.7, A.8, A.9 and A.10 Supplementary Requirements for Design;
- Annex B.1 Purchasing Requirements; and
- Annex F.1, F.2 and F.3 Supplementary Requirements for Verification of Design.
- CSA B51-03, Parts 1, 2 and 3;
- CSA N286.7-99;
- CSA N290.13-05;
- CSA N290.15-10;
- CSA N293-07; and
- Professional Engineers Act, R.S.O 1990, Chapter P.28 and its subordinate Regulation 941/90, R.R.O. 1990, and Regulation 260/08, R.R.O. 1990.

Appendix A in BP-PROG-10.02 [112] provides a mapping of relevant Statutory, Regulatory and Licensing Requirements to procedures demonstrating compliance. No gaps are identified in the Appendix. It is noted that the relevant statutory, regulatory and licensing requirements are out of date. This gap is reflected in the report on Safety Factor 10 as SF10-3.

#### **4.2.2. Implementing Procedures**

The Plant Design Basis Management Program [106] is implemented by the following procedures.

- BP-PROC-00335, Design Management [107]:
  - Specifies the design activities and outputs that define and manage the Plant Design Basis such that the nuclear operating stations can operate safely and reliably for the duration of their design life. Design Management relies upon the implementing procedures of BP-PROC-00363 [108] to ensure that nuclear safety requirements are incorporated into the design.
- BP-PROC-00363, Nuclear Safety Assessment [108]:
  - Defines the elements, functional requirements, implementing procedures and key responsibilities associated with the Nuclear Safety Assessment (NSA) process to ensure that all necessary nuclear safety requirements are defined for the actual or proposed design of the plant throughout the design modification process or in addressing emergent issues (e.g., plant ageing) that may affect the Design Basis or the Safety Report Basis.

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- DIV-ENG-00009, Design Authority [109]:
  - Outlines the processes by which the Chief Engineer and Senior Vice President, Engineering executes the role of Design Authority.
- BP-PROC-00582, Engineering Fundamentals [110]:
  - Sets forth the expectations for performing, assessing, and reinforcing the Engineering Fundamentals to ensure Engineering activities achieve industry best performance.
- BP-PROC-00502, Resolution of Differing Professional Opinions [111]:
  - Provides a process to initiate, track and resolve a Differing Professional Opinion in a complete and timely fashion.

A considerable number of additional supporting procedures are identified in the Program. These procedures govern activities related to plant design basis management at the company wide level, engineering division level, department level, and section level. Department level procedures include those associated with Nuclear Safety Analysis and Support (NSAS), Plant Design Engineering (PDE), and Reactor Safety (RS). Section level procedures include those associated with Environmental Qualification (EQ), Procurement Engineering (PE), and Reactor Safety Assessment.


Program Oversight by line management is completed using self-assessments, Station Condition Record (SCR) trending, and management review of performance indicators. Self-assessments are completed on an annual basis in accordance with BP-PROC-00137 [134], Focus Area Self-Assessment. Focus areas are selected from program activities based on a qualitative management review of performance in the previous year. Relevant SCR data is monitored by line management in accordance with BP-PROC-00412 [135], Trend Identification and Reporting of SCRs.

Line management review of performance indicators occurs monthly. Each performance indicator, as defined within the program implementing processes, is assigned an owner who is responsible for performance. During line management review, the reported performance is challenged. When performance is below expectations, the indicator owner is responsible to produce an action plan that will close the gap.

### 4.3. Engineering Change Control Program

The objective of the ECC program BP-PROG-10.02 [112] is to manage design changes and modifications to ensure that they are effectively defined, planned, implemented and controlled. Whereas the Plant Design Basis Management Program [106] ensures that the design basis is robust, the ECC program ensures that changes to the plant design basis maintain this robustness. The ECC process applies to all changes that affect design and associated documents, including:

- New Structures, Systems, Components and Significant Tools (SSCTs);
- Changes to existing SSCTs;

 <div style="font-size: small;">Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- SSCTs to be abandoned in place, removed or demolished; and
- Changes that affect documentation only.

The ECC Program, in Section 3.1.4, defines a design change as any revision or alteration of the technical requirements defined by approved and issued design output documents and approved changes thereto, per ASME NQA-1-1994, Part I, Section 4. In addition, ECC does not apply to modifications made to SSCTs while out of service if the modifications are completely reversed before the SSCT is placed back in service.

The Program applies a graded approach based on risk. The assessment of risk includes elements of safety (industrial safety, reactor safety, environmental safety, radiation safety) and business needs.


BP-PROG-10.02 [112], Section 4.0, states that “it is expected that each person will take responsibility for nuclear safety by:

- Following all applicable procedures as written or ensuring that required procedure changes or alterations occur, and
- Accepting and performing only those tasks for which he or she is qualified in accordance with BP-PROG-02.02 or, in the case of vendors, an appropriate, accepted vendor QA program.”

#### **4.3.1. Relevant Statutory, Regulatory, and Licensing Requirements Addressed by the Program**

As identified in Section 5.1 of the Engineering Change Control Program [112], the relevant Statutory, Regulatory and Licensing Requirements addressed by the Program are:

- Bruce B Nuclear Power Reactor Operating Licence, PROL 16.00/2014;
- Central Maintenance and Laundry Facility, Waste Nuclear Substance Licence, WNSL-W2-323.02/2017;
- S-296 (2006), which has been superseded by REGDOC-2.9.1;
- CSA N286-05:
  - Clauses 5.5, 5.8, and 5.12;
  - Clauses 6.1, 6.7, 6.8, 6.9, and 6.10;
  - Annexes A.2, A.3, A.6, A.7, A.8;
  - Annex B.1;
  - Annex C; Annex D and
  - Annex F.
- CSA N285.0-08 (with Update No. 1, June/09);
  - Clause 6.1.10

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- Clause 10
- Clause 11
- Clause 14.5.3
- Annex J
- ASME BPVC 2007, Section III, Rules for Construction of Nuclear Facility Components;
- ASME NQA-1-1994;
- CSA B51-03;
- CSA N293-07 Fire Protection for CANDU Nuclear Power Plants;
  - Clause 4.6, 4.7, and 4.8 – General Requirements
  - Clause 5.3.2 – Preventing fires, and 5.5.1 – Life safety performance objectives
  - Clause 11.2.2 – FSSA Application
- CSA ISO 14001:04, specifically Section 4.3.1 (a);
- Professional Engineers Act, R.S.O. 1990, Chapter P.28.

In addition, the following Bruce A and B Operating Policies and Principles clauses are met by the Program:

- Bruce B OP&P [136] Section 01.6 Clause 1 (b) and (d); and
- Bruce A OP&P [137] Section 01.6 Clause 1 (b) and (d).

Appendix A in BP-PROG-10.02 [112] provides a mapping of relevant Statutory, Regulatory and Licensing Requirements to procedures demonstrating compliance. No gaps are identified in the Appendix. It is noted that the relevant statutory, regulatory and licensing requirements are out of date. This gap is reflected in Safety Factor 10 as SF10-3.

#### **4.3.2. Implementing Procedures**

The ECC Program (BP-PROG-10.02 [112]) is implemented by the following procedures:

- BP-PROC-00743, Site Services Engineering Change Control [113]:
  - Governs commercial modifications to Centre of Site systems, structures and components, including temporary modification to ensure safety and minimize loss to the company through appropriate risk management activities.
- BP-PROC-00542, Configuration Information Change [114]:
  - Governs the acceptance, creation, revision, obsolescing and superseding of design information when corrections to documentation are necessary without requiring field activities, Operations acceptance/approvals, or changes to operating or maintenance procedures.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- BP-PROC-00539, Design Change Package [115]:
  - Specifies the control of modifications to plant systems, structures, components, and significant tools (including temporary modifications) to meet regulatory requirements, ensure safety, and minimize loss to the company through appropriate risk management activities.
- BP-PROC-00877, Modification Installation Quality Assurance [116]:
  - Includes the production and oversight of Inspection and Test Plans (ITPs) and work packages that support design changes and modifications. An engineering change is the electronic PassPort record of a design change or modification.
- BP-PROC-00615, Commissioning Modifications and Projects [117]:
  - Provides requirements for planning, specification, execution and reporting of commissioning activities for SSCTs.


Program oversight is implemented through BP-PROC-00137, Focus Area Self-Assessment [134] and BP-PROC-00412, Trend Identification and Reporting of SCRs [135]. Line management review of performance indicators occurs monthly.

A number of additional supporting procedures are identified in the Program. These procedures govern activities related to ECC at the company wide level and engineering division level. No department level or section level procedures are identified.

#### 4.4. Configuration Management

The objective of the Configuration Management Program, BP-PROG-10.03 [118], is to ensure that modifications to the plant, operation, maintenance and testing of the physical plant configuration is in accordance with the design requirements as expressed in the facility configuration information and to maintain this consistency throughout the operational life-cycle phase, particularly as changes are being made. The ECC Program, BP-PROG-10.02 [112], governs the management of distinct changes to the plant design basis. The Configuration Management (CM) Program as a stand-alone program establishes, in Section 1.0, guidance to promote consistent application of the following:

- Clearly define and communicate CM scope, responsibilities, authorities, principles and interfaces;
- Design basis and licensing basis requirements, which apply to the plant will be accurately identified, documented, maintained and accessible;
- The plant's physical SSCs, and process computer controls will conform to design basis and licence basis requirements;
- Design basis and licence basis requirements will be accurately reflected in plant documentation and in processes and procedures for altering, maintaining, testing and operating the plant;

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- Consistency will be maintained among sources of plant information (documents and electronic data), as well as between plant information and the plant physical and functional characteristics;
- Continuous improvement of CM will be achieved by monitoring and assessing CM-related activities and by incorporating feedback of lessons learned from in-house and industry best practices and experience.

#### **4.4.1. Relevant Statutory, Regulatory and Licensing Requirements Addressed by the Program**

As identified in Section 5.1 of the Program [118], the relevant Statutory, Regulatory and Licensing Requirements addressed by the Program are:

- Bruce B Nuclear Power Reactor Operating Licence PROL 16.01/2015<sup>3</sup>
  - Clause 5.1
- CSA N286-05, specifically:
  - Clauses 5.2 (d), 5.5, 5.8, 5.9, 5.10, 5.12, 5.13 and 5.14.1 – Management system – Generic Requirements; and
  - Clauses 6.3, 6.5, 6.7, 6.9, and 6.13 – Specific requirements.
- CSA N285.0-08 (with Update No. 1, June/09), specifically:
  - Clause 14.5.4, Temporary Modifications.
- CSA B51-03, Boiler, Pressure Vessel, and Pressure Piping Code, Parts 1, 2 and 3
- CSA N290.15-10, Requirements for Safe Operating Envelope for Nuclear Power Plants
  - Clause 4.2, 4.6
  - Annex A.4.4.1(b), A.4.5, A.4.7.2
- Professional Engineers Act, R.S.O. 1990, Chapter P.28.


Appendix B in BP-PROG-10.03 [118] provides a mapping of relevant Statutory, Regulatory and Licensing Requirements to procedures demonstrating compliance. No gaps in compliance are identified in the Appendix. It is noted that the relevant statutory, regulatory and licensing requirements are out of date. This gap is reflected in Safety Factor 10 as SF10-3.

#### **4.4.2. Implementing Procedures**

This Program is implemented by the following procedures. Refer to Appendix C in BP-PROG-10.03 [113], Document Hierarchy.

- BP-PROC-00470, Configuration Management Program Oversight and Trending [119]:

<sup>3</sup> BP-PROG-10.03-R006, Configuration Management, has not been updated since PROL 18.00 came into effect.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- Establishes a mechanism for monitoring, trending and reporting the health of the Bruce Power Configuration Management (CM) Program.
- BP-PROC-00584, PassPort Equipment Data Management [120]:
  - Governs the standard basis and process requirements for addition, modification and deletion of equipment data in PassPort and sets guidelines for maintaining accurate Master Equipment List (MEL) record information.
- BP-PROC-00638, Temporary Configuration Change Management [121]:
  - Governs the method that satisfies, in part, the regulatory requirement to control Temporary Configuration Changes made to licensed facilities.
- BP-PROC-00647 PassPort Permit Request Processing [122]:
  - Defines the life cycle and management of permit requests across the Bruce Power site in support of scheduling work activities.
- BP-PROC-00786, Margin Management [123]:
  - Governs a systematic process to identify, prioritize and resolve margin issues to help ensure that the operating configuration is conservatively maintained within the design requirements and that design requirements are conservatively maintained within the design basis.
- BP-PROC-00898, Equipment Codes [124]:
  - Governs the method to achieve consistent identification of equipment and is to be used in selecting the structure of an equipment code.
- SEC-DO-00001, Drafting Office Work Management [125]:
  - Governs the Work Management activity from Drafting Office initiation of a Work Package through to Work Package completion and issuance.

Program oversight is implemented through BP-PROC-00137, Focus Area Self-Assessment [134] and BP-PROC-00412, Trend Identification and Reporting of SCRs [135].

A number of additional supporting procedures are identified in the Program. These procedures govern activities related to ECC at the company wide level and engineering division level. No department level or section level procedures are identified.

## 5. Results of the Review

The results of the review of this Safety Factor are documented below under headings that correspond to the review tasks listed in Section 1.2 of this document. The review tasks assessed in this section have not changed from those listed in Section 1.2.



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## 5.1. List of SSCs Important to Safety

This review task requires that the list of all of SSCs important to safety be reviewed for completeness and adequacy. It is important to note that the term “Systems Important to Safety” (SIS) has a very specific meaning within Bruce Power, whereas this review task addresses the broader concept of SSCs that are of importance to safety.

Bruce Power employs a number of SSC lists to serve specific objectives as related to different aspects of safety considered in, for example, design, safety analysis, equipment reliability, and structural integrity. The most important and comprehensive of these is the Safety Related System List (SRSL), as documented in BP-PROC-00169 [130]. Systems in the Safety-Related System list will receive increased emphasis in the area of maintenance, testing availability and qualification requirements. The list applies to all work related to the execution of design, commissioning, maintenance and operation of the systems. The list utilizes a classification system recommended in Appendix A of CSA N286.0-92 [138] and consequently ranks safety-related systems in groups A through G, depending on their significance to safety. Systems in the SRSL receive increased emphasis in the area of maintenance, testing, availability and qualifications requirements. This emphasis is graduated depending on the classifications and the safety-related functions within the listing. The Safety Related System Testing program [139] is focused on testing safety-related SSCs to determine if they are available. It has a direct link to equipment reliability. The PROL and Bruce B Operating Policies and Principles (OP&Ps) require that an approved testing program exist to ensure that specific SSCs are available, reliable and effective. Testing is required on any system which is not normally operating but is required to function in the event of a system failure, to control reactor power, cool the fuel or contain radioactivity (see Section 03.5 of [136]) The methodology and process involved in determining which station systems are systems important to safety and their performance criteria and targets are described in the procedure DPT-RS-00012-R001, Systems Important to Safety (SIS) Decision Methodology [128].

Other lists with more specific safety-related purposes include:

- The System Classification List, which categorizes pressure retaining systems and components in accordance with their importance to nuclear safety with reference to the applicable section of the ASME code for design and construction purposes. This list is established and maintained through procedure DIV-ENG-00017 [140].
- The Environmental Qualification Safety Related Component List (EQ SRCL) is a list of all EQ safety-related equipment and components. It includes the parent components and all associated support components which are required to ensure the parents components function. All EQ SRCL parents and support components are entered in the Environmental Qualification Information System (EQIS) database per SEC-EQD-00022 [141].
- The Bruce Power Seismic Qualification Standard [142] provides a summary of the seismically qualified systems for Bruce B. They are specified in detail in NK29-DG-03650-002 [143] which invokes CAN3-N289.3 and N289.4.
- Fire Safe Shutdown System List in Appendix B DPT-PDE-00028 [144] is a list that identifies all of the SSCs credited for the safe shutdown of the plant in the event of a fire.



	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

This list is derived from the Bruce B Fire Safe Shutdown Analysis [145] Appendix 1 which contains the FSSA-credited equipment list and FSSA-credited cables.

- The SOE system list identifies the systems for which the SOE Operational Safety Requirements apply. This list includes systems that are credited with an accident mitigation function in the Safety Report or supplementary analysis, and includes systems for which their initial conditions could impact on accident consequences. However, the systems on this list are not necessarily in the SRSL. The major systems that support the SOE have been included in the Preparation and Maintenance of Operational Safety Requirements DPT-NSAS-00012 [146]. Table 1 of DPT-NSAS-00012 [146] provides the minimum list for which OSRs are required.
- The Assessment of Systems Important to Safety for the Safety & Licensing Portion of the Nuclear Asset Management Program [147] presents the various system groupings at Bruce Power that rank the importance of SSCs based on safety and production.

Based on the details presented above, it is concluded that all of the systems important to safety have been comprehensively identified and appropriately classified. Bruce Power's programs therefore meet the requirements of this review task.

## 5.2. Verification that Plant Design Supports Plant Safety and Performance

This review task requires verification that design and other characteristics are appropriate to meet the requirements for plant safety and performance for all plant conditions and the applicable period of operation. The verification is discussed under subheadings corresponding with the bullets under this review task in Section 1.2.

### Prevention and mitigation of events (faults and hazards) that could jeopardize safety

Among the key processes for prevention and mitigation of events is the Plant Design Basis Management program [106]. The purpose of this program is to define, document, and control changes to the Design Basis to maintain it within approved safety margins and regulatory requirements, and to perform such Safety Analysis as is required to ensure that plant operation conforms to the Design Basis and licensing assumptions, and remains within the bounds of analyzed conditions and the SOE. This program is supported by the EQ process [148] and the Seismic Qualification (SQ) process [142]. These processes establish an integrated and comprehensive set of requirements that provide assurance that credited essential equipment and components can perform their safety-related functions even if exposed to harsh environmental conditions resulting from Design Basis Accidents, in accordance with the plant design and licensing basis and that this capability is preserved over the life of the plant. However, it is noted that there are no complementary design features specifically included in the Bruce B original design for the management of severe accidents. In preparing the Severe Accident Management Guidelines (SAMG), all systems that are available will be used for the recovery, some of them under conditions not normally envisaged for those systems. In the area of strengthening defence-in-depth Bruce Power, as a result of Fukushima Action Items, has engineered and installed complementary safety features to provide makeup water to the calandria, heat transport system and shield tank to provide overpressure protection to the shield

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

tank against a severe accident by mitigating severe accident progression and protecting containment boundary. As of February 2016 [78] the action items related to strengthening defence-in-depth have been closed through discussion with the CNSC.

In addition to strengthening defence-in-depth, Bruce Power has completed Fukushima Action Items related to enhancing emergency response, including emergency plans, facilities and equipment also closed by the CNSC as of February 2016 [78]. However, the Bruce B design does not provide an onsite emergency facility/facilities that are separate from the plant control rooms for use by the technical support staff and emergency support staff as required by CNSC REGDOC-2.5.2 (see SF1-22 in Table 8).


Application of defence-in-depth and engineered barriers for preventing the dispersion of radioactive material (integrity of fuel, cooling circuit and containment building)

As described in CNSC REGDOC-2.5.2, Clause 6.1, the design of an NPP shall incorporate defence-in-depth [50]. The concept of defence-in-depth has been applied to the design of all CANDU reactors. The various levels of defence-in-depth are independent of each other to the greatest extent practicable. For example, Level 1 defence-in-depth systems, i.e., process systems, are designed so that any failure in the system is not propagated to the control systems that control these processes. Similarly, a failure in a control system does not propagate to the next level of defence-in-depth, i.e., the safety systems. This is accomplished through adequate separation of the control systems from the safety systems. Internationally, this is achieved by ensuring adequate buffering of any components shared between the control and safety systems so that the failure cannot be propagated. In Canada, it has been done to date through the complete separation of the control and safety systems.

Consideration of the prevention and mitigation of events (faults and hazards) that could jeopardize safety in the original design did not include a systematic analysis of the control system capability to cope with Anticipated Operational Occurrences (AOOs), as required by CNSC REGDOC-2.5.2. This is considered a gap and is noted as SF1-6 in Table 8. It is noted that the use of systematic approach for the event identification and classification in accordance with REGDOC-2.4.1 is one of the earliest activities of the Safety Report Improvement plan and it will address this gap.

Safety requirements (for example, on the dependability, robustness and capability of SSCs important to safety)

The physical design of Bruce B is managed through a suite of programs in the Configuration Management Engineering Functional Area. These programs provide a disciplined approach to the control of the physical configuration, design requirements, and facility configuration information (FCI), such that station operators have high confidence that structures, systems, and components are fully functional and support safe, reliable plant operation. The overall objective of the program suite is to ensure that structures, systems, components, and tools meet design basis requirements and enable the plant to operate safely, reliably, and efficiently for the duration of its operating life; which is supported by the Equipment Reliability Program (ERP) [126] and Maintenance Program (MP) [149]. Management of plant design evolution will ensure that all SSCs important to safety have the appropriate characteristics, specifications and material composition so that the required safety functions can be performed and the plant can operate safely with a high degree of reliability for the duration of its design life. Changes to the

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Safety Report, SOE or associated analyses are managed in accordance with procedures and standards that comply with regulatory, statutory and legal requirements.

### Design codes and standards

In accordance with Appendix A of Bruce Power's Plant Design Basis Management Policy BP-MSM-1 [100], the plant design shall "satisfy the requirements of the leading standards of manufacture, construction, inspection, testing and maintenance commensurate with both the design's safety significance and with all relevant reliability and security considerations and requirements of the system or its component parts". Review of relevant design codes and standards is addressed in Section 5.3.

Specifically to the adequacy of plant design documentation pertaining to radiation and environmental protection one gap is noted against modern codes and standards. The assessment of CNSC REGDOC-2.5.2 in Appendix B.2 revealed that the plant design documentation does not describe all necessary suitable provisions to minimize exposure, contamination, and radiological releases to the environment. The sources of this gap are micro-gaps against REGDOC-2.5.2 specific design requirements as noted in SF1-14 in Table 8.


### **5.3. Identification of Differences Between Standards Met by NPPs Design and Modern Codes and Standards**

This review task requires identification of differences between standards met by the nuclear power plant's design (for example, the standards and criteria in force when it was built and the standards applicable when design modifications were made) and modern nuclear safety and design standards. Section 3 lists the applicable regulatory requirements, codes and standards considered in the review of this Safety Factor that have been identified Table C-1 of the Bruce B PSR Basis Document [5].

Bruce Power has a regulatory commitment as tracked by Action Item AI 091413 Bruce B Legacy Registration Project, to bring all pressure retaining systems and components into compliance with licence condition 5.2 Pressure Boundary Program and Authorized Inspection Agency [2]. Bruce Power has committed to provide a prioritization scheme to the CNSC. Periodic updates are provided to the CNSC and the last update was provided in NK29-CORR-00531-12884 [150].

Bruce Power continues to address legacy registration issues as part of its engineering change control. As modifications are made to the systems, legacy issues are being addressed as part of these modifications (e.g., Fukushima modifications). Design organizations have been contracted to update/revise design documentation required to support the registration of systems. In addition, Bruce Power has acquired several qualified augmented staff to assist with registration of the nuclear and conventional systems.

The Bruce B legacy registration project has been focused on the Design Specifications for the nuclear systems and associated work that impacts the Design Specifications. Of the 58 Design Specifications, 6 have been completed and 11 are in progress as of November 2015 [150]. The total number of flow diagrams in the scope of the Bruce B Legacy Registration project is 929 of which 178 have been completed. Bruce Power has committed to having all Bruce B system

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

design registrations (including system classification lists) updated by December 31, 2017 [2]. When built Bruce Power met the standards at that time and as specified in the licence. The Legacy Registration project scope includes bringing all design documentation into compliance with current code and licensing requirements. Code requirements mandated by N285.0 for new systems and modifications have been consistently followed; however there is no code assessment to determine the extent to which the Bruce B design meets the new requirements of N285.0-12. Therefore, this is assessed as design gap see SF1-18 in Table 8.

The procedure DIV-ENG-00018, Design Registration and Reconciliation [151] establishes the process for design registration and reconciliation of pressure retaining components for Bruce Power with the Authorized Inspection Agency (AIA).

Overall, it can be concluded that Bruce Power largely meets the requirements of modern codes and standards, notwithstanding the gaps that have been identified. The following subsections provide more details on codes and standards addressed as part of this Safety Factor review.

### **5.3.1. Review Against Changes to CSA N287.1-14 General Requirements for Concrete Containment Structures for Nuclear Power Plants**

As part of this PSR, a high-level review of standard CSA N287.1-14 was conducted. The clauses in the standard are related to the design, construction, and testing of concrete containment structures. This standard applies to new nuclear power plant concrete containment structures.

This high-level assessment showed that Bruce Power complies with or complies with the intent of Canadian Standards Association (CSA) Standard N287.1-14.

The assessment is presented in Appendix A (Section A.2). No gaps were identified as a result of this assessment.

### **5.3.2. Review Against Changes to CSA N287.3-14 Design Requirements for Concrete Containment Structures for Nuclear Power Plants**

As part of this PSR, a high-level review of standard CSA N287.3-14 was conducted. This standard applies to concrete containment structures of new nuclear power plants. The Bruce B containments were designed to CSA N287.3-1978 [152][153]. Thus, the containments are assumed to comply with that version of the standard. A code-to-code comparison of the 1978 version against the 2014 version of this standard was performed to identify the significant differences and those differences were assessed for design compliance from a high-level perspective.

The code-to-code comparison identified three main topics to be assessed, namely: (1) Assessing containment structures for beyond design basis; (2) Walls, slabs, shells, and domes to be reinforced in accordance with clauses of CSA A23.3 [154]; and (3) More extensive reliance on CSA A23.3. In all cases, the Bruce B containments have been shown to comply with the intent of these significant differences between the 1978 and 2014 versions of CSA N287.3.

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

The assessment is presented in Appendix A (Section A.3). No gaps were identified as a result of this assessment.

### 5.3.3. **Review Against Changes to CSA N289.1-08 (R2013) General Requirements for Seismic Design and Qualification of CANDU Nuclear Power Plants**

As part of this PSR, a high level review of the standard has been performed and documented in Safety Factor 3. The first edition of this standard was issued in 1980 and contained very basic definitions and requirements for seismic qualification. The 2008 edition of the CSA N289.1-08 [62] standard (referred to as the current edition) was substantially expanded to add a greater level of detail and to add the seismic margin assessment (SMA) methodology (which is used in Bruce A). The last update in September 2014 now includes twenty pages of requirements, compared with three pages of requirements in the first edition. The results of this review are presented in Safety Factor 3.

The Bruce plant is located in a region of low seismic hazard as stated in the Bruce B Safety Report, Part 1, Section 2.6.2.1 [155]. The seismic review performed in 2001 as part of the development of the Review Level Earthquake for Bruce A [156] confirmed the low seismic hazard for the Bruce site.

Many definitions currently used in the seismic design, including the definition of the seismic margin assessment qualification methodology and a number of other definitions associated with it are added in the latest revision of CSA N289.1.

The requirements in the latest revision are generally more detailed and provide an update to reflect current practices. This is assessed in Safety Factor 3, which recommends the governing procedure (DPT-PDE-00017 [142]) and its implementing documents (NK29-DG-03650-002 [143]) be updated to reflect the latest requirements of clause 3.1 from CSA N289.1 (i.e., the  $10^{-4}$  requirement for the definition of the Design Basis Earthquake (DBE)), including the 2014 update. The reporting and recording requirements for earthquake events and the more recent site investigations documented in the Probabilistic Seismic Hazard Assessment performed in 2011 [157] are not reflected in the seismic implementing procedures. This is identified as a gap SF1-16 in Table 8. The definition of the DBE for Bruce B is discussed in Section 5.3.4.

The current governing documents do not address the need for recording equipment to be installed in the plant to satisfy the intent of clause 6.5.6 and the specific requirement stated in clause 6.5.6.3 to record all significant earthquake data. It would not be possible to satisfy the overall intent of these clauses (i.e., impact on fatigue usage factor and loss of service life) without earthquake recording equipment in the plant, so this is identified as gap SF3-2 in Safety Factor 3, Equipment Qualification. Clause 6.5.6.4 requires data collected from monitoring instruments installed at different levels in the plant to be compared with the design floor response spectra to assess if the design stress levels have been exceeded. This is identified as gap SF1-15 in Table 8.



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

#### 5.3.4. **Review Against Changes to CSA N289.2-10 Ground Motion Determination for Seismic Qualification of Nuclear Power Plants**

As part of this PSR, a high level review of the standard has been performed and documented in Safety Factor 3. The methodology and practices in the first edition of CSA N289.2 were used to develop the DBE and Site Design Earthquake (SDE) used for seismic qualification in the original design, although the standard was issued late in the design process and is not referenced in NK29-DG-03650-002. The response spectra for the DBE and SDE are included in Section 4 of NK29-DG-03650-002 [143].

Clause 4 of CSA N289.2-10 describes the required investigation of:

- The history of earthquakes and earthquake effects in the region;
- Seismological and geological properties of the region and site vicinity that could have an influence on the seismic ground motion at the site due to future earthquakes in the region; and
- The potential for seismically induced phenomena and other geological hazards in the region and site vicinity.

The original site investigations carried out to establish the seismic parameters for the Bruce site are outlined in the Bruce B Safety Report (Part 1, Section 2.6.2) [155]. The Bruce B Safety Report and the design guide used for the original design of Bruce B Earthquake Design Requirements for CANDU Nuclear Power Plants [158] indicate that regional information from Energy, Mines, and Resources was used to develop the ground response spectra for the DBE for Bruce B. The seismic evaluation done in 2001 to establish the Review Level Earthquake (RLE) for Bruce A [156] stated “there is no available site-specific assessment of the seismic hazard at the Bruce site” (Section 4.0). The evaluation for the Bruce A RLE was based on information from the Darlington site, which was considered to be conservative for the Bruce site, and which resulted in a peak ground acceleration of 0.099 g at 100 Hz (probability of exceedance of  $10^{-4}$ ). Since that time, a Probabilistic Seismic Hazard Assessment [157] has been done for the Bruce B site, which does address the specific seismic characteristics of the site, including the probability of exceedance of  $10^{-4}$ .

The available documentation does not indicate that an investigation of the potential for a seismic seiche and consequent surges along the shore that could affect the safety of the plant were performed. This is identified as gap SF3-3 in Safety Factor 3, Equipment Qualification.

#### 5.3.5. **Review Against Changes to CSA N289.3-10 Design Procedures for Seismic Qualification of Nuclear Power Plants**

As part of this PSR, a high-level review of the 2010 edition of the code has been performed and documented in Safety Factor 3.

The first edition of this standard was issued in 1981, and the second edition was issued in 2010 to be consistent with the content and terminology used in the most recent edition of CSA N289.1 (e.g., Seismic Margin Assessment methodology), and to include more detail for the seismic design of SSCs and for seismic analyses.

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Section 4 of this standard addresses the application of the seismic ground motion to the design, including the requirements for the standard shape design ground response spectra, based on the peak ground motion parameters specified in CSA N289.2 and the amplification factors in Table 1 of N289.3.

The DBE ground response spectra for Bruce B was based on an estimated probability of exceedance less than  $1 \times 10^{-3}$ , according to clause 3.1.1 of DPT-PDE-00017 [142], and the Probabilistic Seismic Hazard Assessment establishes the peak ground acceleration for  $10^{-4}$  at 0.016 g. Clause 4.2 specifies that “The minimum design horizontal response spectra used in the design of new nuclear power plant SSCs shall be: (a) the standard-shape ground response spectrum anchored to a peak ground acceleration of 0.1 g on rock...and (b) modified to take into account the site specific geological conditions.” The current peak ground acceleration specified for Bruce B is 0.05 g [143], which does not appear to satisfy the requirement in Clause 4.2 of CSA N289.3-10. It is noted that this applies only to new plants, rather than to new SSCs in existing plants, as indicated by a positive response to a request for interpretation from the CSA N289.3 Technical Committee [159].

The topics in Section 5 of CSA N289.3 cover seismic analysis of foundations including the soil and rock supporting the nuclear power plant, and were addressed in the original design of the plant, see [158]. However, because of the legacy aspects of the scope of this section, specific design analysis for Bruce B was not reviewed as part of this high-level assessment.


Acceptable methods of dynamic analysis and requirements for analytical methods used for the qualification of SSCs are discussed in Section 6 of the latest revision of CSA N289.3. Similar dynamic analysis methods were used for the seismic qualification of SSCs for Bruce B, but these were not reviewed for compliance against the current detailed requirements listed in this standard. It is noted in CSA N289.1 (Clause 5.4.1.2.3) [62] that SSCs designed to provisions of earlier editions of the reference publications (which include CSA N289.3) are not required to be requalified to meet the provisions of the current standards.

Section 9 requires that seismically induced phenomena be evaluated. Of the events listed, the applicable event for the Bruce site is the seiche, which is also evaluated as part of CSA N289.2 above, for which a gap is identified in Safety Factor 3 (SF3-4). It is noted that although the seiche is addressed in NK29-CORR-00531-11136 [160] it appears to be only due to weather (i.e., wind forces on the water) and atmospheric conditions (differences in air pressure) and not from a seismic event.

The methods and practices included in this standard are similar to those used for the seismic qualification of SSCs in the original design of Bruce B, in that they address the dynamic characteristics of the SSCs being seismically qualified. NK29-DG-03650-002 [143] specifies the requirements of the current standard for replacements or modifications of seismically qualified SSCs, so Bruce B is considered to comply with the requirements of this standard.

### **5.3.6. Review Against Changes to CSA N289.4-12 Testing Procedures for Seismic Qualification of Nuclear Power Plant SSCs**

As part of this PSR, a high-level review has been carried out on the 2012 edition of the standard and documented in Safety Factor 3.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

The first edition of this standard was issued in 1981, and was updated in 2012 to be consistent with the content and terminology used in the most recent edition of CSA N289.1 (e.g., the SMA methodology), and to include more detail for the seismic qualification of SSCs by testing. The original equipment test reports were not reviewed for compliance with the requirements in this standard, as it is noted in CSA N289.1 (clause 5.4.1.2.3) [62] that SSCs designed to the provisions of earlier editions of the reference publications (which include N289.4) are not required to be requalified to meet the provisions of the current standard. The methods and practices included in CSA N289.4 are similar to those used for the seismic qualification of SSCs in the original design of Bruce B, in that they evaluated the dynamic response of the equipment to the input response spectra, so the intent of these requirements was met. NK29-DG-03650-002 (clause 6.1) [143] and DPT-PDE-00017 (clauses 4.1 and 4.2) [142], specify the requirements of the current N289.4 standard for replacements or modifications. Bruce B is considered to comply with the intent of the requirements of this standard. No gaps were identified as a result of this assessment.

### **5.3.7. Review Against Changes to CSA N289.5-12 Seismic Instrumentation Requirements for Nuclear Power Plants and Nuclear Facilities**

As part of this PSR, a high-level review has been carried out on the 2012 edition of the standard and documented in Safety Factor 3. The standard was extensively changed, with the main changes being that the locations requiring seismic instrumentation (i.e., four locations in the reactor building and one outside) and the technical requirements for the instrumentation are more clearly specified and the standard is presented in terms of existing plants (Section 4) and new plants (Section 5).

The words “Where required to be installed...” in clause 1.2, and other words in Note 1 of Table 1 (i.e., “Plants undergoing a life extension follow the requirements established together with the AHJ”) make it clear that this standard applies only if there is a stated requirement from the licensee or the authority having jurisdiction (AHJ), which is the CNSC.

The procedure DPT-PDE-00017, Bruce Power Seismic Qualification Standard [142] in Section 4.1 (second paragraph) includes CSA N289.5 as a basis for seismic qualification, but notes in Section 4.6 (Post-Seismic Response) that notification of an earthquake of magnitude 5 or greater within 500 km of the site will be received from the Southern Ontario Seismograph Network, which has one monitoring station within 20 km of the Bruce site. This is also included in the operating procedures and has been accepted by the CNSC through the acceptance of the procedure noted above, which documents this monitoring approach [161].

Since the post-seismic event notification to the operating staff is considered to be adequate and has been accepted by the CNSC, it is considered that the free field motion accelerometer (CSA N289.5-12 [66], clause 4.2.2) would not be required. However, a gap has been identified in in Safety Factor 3 (SF3-4) that a free-field accelerometer has not been installed on the site to confirm that a seismic event has occurred (clause 4.1.1.3), and accelerometers be placed on structures and equipment as recommended in clause 4.2.3. This gap was identified considering this standard is listed in the recently issued Licence Conditions Handbook [2] in terms of additional recommendations and guidance (Section 5.1, Design Program), and the time period considered is relatively long (until 2025). Damage to critical safety related structures and



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

equipment could be more quickly assessed, probably enabling a return to service much sooner, rather than relying solely on post-seismic walkdowns to assess damage in response to notification of an earthquake, as currently outlined in DPT-PDE-00017 (clause 4.6) [142].

### **5.3.8. Review Against CSA N290.0-11 Requirements for Emergency Core Cooling Systems of Nuclear Power Plants**

A high-level review of CSA N290.0-11 has been conducted. The details of this assessment are provided in Appendix A (Section A.10) Based on this assessment, gaps SF1-1, SF1-5, and SF1-20 have been identified and are listed in Table 8.

### **5.3.9. Review Against Changes to CSA N290.1-13 Requirements for the Shutdown Systems of Nuclear Power Plants**

A clause-by-clause assessment has been performed on the 2013 edition of the standard. The gaps are identified as SF1-9, SF1-12 and SF1-20 in Table 8, and are documented in Appendix B (B.1).

### **5.3.10. Review Against CSA N290.2-11 Requirements for Emergency Core Cooling Systems of Nuclear Power Plants**

A high-level review of CSA N290.2-11 has been conducted. The details of this assessment are provided in Appendix A (Section A.11). Based on this assessment, gap SF1-14 has been listed in Table 8.

### **5.3.11. Review Against CSA N290.3-11 Requirements for Containment Systems of Nuclear Power Plants**

A high-level review of CSA N290.3-11 has been conducted. The details of this assessment are provided in Appendix A (Section A.12). Based on this assessment, SF1-3 and SF1-19 have been identified in Table 8.

### **5.3.12. Review Against CSA N290.11-13 Requirements to Reactor Heat Removal Capability During Outage of Nuclear Power Plants**

A high-level review of CSA N290.11-13 has been conducted. The details of this assessment are provided in Appendix A (Section A.13). Based on this assessment, SF1-3 and SF1-7 have been identified in Table 8.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

### **5.3.13. Review Against CSA N291-15 Requirements for Safety-Related Structures for Nuclear Power Plants**

CSA N291-15 provides material, design, construction, fabrication, inspection, and examination requirements for Safety-Related Structures for nuclear power plants. A high-level review has been performed on the 2008 version (Reaffirmed in 2013). To comply with CSA N291-15, Bruce Power plans to utilize the research described in Reference [162] and experience gained from the Life Cycle Management Program, along with baseline inspection results from 2005/2006 conducted on a large portion of Bruce A and B structures to compile in-service inspection results for safety-related structures.

The results of this review are documented in Appendix A (A.4). No gaps were identified as a result of this assessment.

### **5.3.14. Review Against CNSC G-149 Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors**

A high-level review of CNSC G-149 has been conducted. The details of this assessment are provided in Appendix A (Section A.1). No gaps were identified as a result of this assessment.

### **5.3.15. Review Against CNSC REGDOC-2.5.2**

A clause-by-clause review of CNSC REGDOC-2.5.2 has been conducted. The detailed results of this assessment are provided in Appendix B (B.2).

Based on this assessment, gaps SF1-1 to SF1-6, SF1-8 to SF1-16, SF1-20, SF1-22, and SF1-23 have been identified and are listed in Table 8.


### **5.3.16. Review Against ANSI/NIRMA CM-1.0-2007, Guidelines for Configuration Management of Nuclear Facilities**

A high-level review of ANSI/NIRMA CM-1.0-2007 [80] has been conducted. The details of this assessment are provided in Appendix A (Section A.6). Based on this assessment, SF1-24 has been identified in Table 8.

### **5.3.17. Review Against ASME BPVC Section III, Section VIII and B31.1**

A high-level review of ASME BPVC Section III [81], Section VIII [82] and Section B31.1 [83] has been conducted. The details of this assessment are provided in Appendix A (Sections A.7, A.8, and A.9, respectively).

Based on these assessments, gaps SF1-17 and SF1-18 have been identified and are listed in Table 8.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

### **5.3.18. Review Against NFPA-805 (2015) Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plant**

A high-level review of NFPA 805 has been conducted. The details of this assessment are provided in Appendix A (Section A.5). No gaps were identified as a result of this assessment.


### **5.4. Adequacy of Design Basis Documentation**

This review task requires a review of the adequacy of the design basis documentation. The purpose of this review task is to ensure that all significant documentation relating to the original design basis has been obtained, securely stored and updated to reflect all the modifications made to the plant and procedures since its commissioning.

IAEA SSG-25 [84] Section 5.15 states “Adequate design information, including information on the design basis, should be made available to provide for the safe operation and maintenance of the plant and to facilitate plant modifications.” The design basis of Bruce B is defined in Section 3.1.3 of BP-PROG-10.01, Plant Design Basis Management [106] as “The range of conditions and events taken explicitly into account in the design of a facility, according to established criteria, such that the facility can withstand them without exceeding authorized limits by the planned operation of safety systems.” The Plant Design Management program BP-PROG-10.01 provides the necessary processes required to document and maintain the design basis and to ensure the plant can operate safely for the full duration of its design life. The documented design basis for Bruce B is contained within design descriptions, requirements manuals, drawings and flow sheets maintained under Controlled Document control in accordance with BP-PROG-03.01, Document Management [129], which interfaces with BP-PROG-10.01 [106] via its implementing documents, particularly BP-PROC-00068, Controlled Document Life Cycle Management [163] and BP-PROC-00098, Records Management [164]. Drawing management is managed through BP-PROG-10.03 [118] Configuration Management, and associated implementing procedures, including SEC-DO-00001, Drafting Office Work Management [125]. BP-PROG-10.02, Engineering Change Control [112] describes the manner in which design changes and modifications are defined, implemented and controlled, thereby ensuring that the design basis is met and documented adequately.

The assessment of Bruce B against CNSC REGDOC-2.5.2 clause 5.7 shows that Bruce B complies with the requirement for design documentation (See Appendix B, Section B.2). As described above the design documentation follows well established processes and procedures. The procedure Design Management, BP-PROC-00335 [107] specifies the design activities and outputs that define and manage the Plant Design basis. Design Management relies upon the implementing procedure BP-PROC-00363, Nuclear Safety Assessment [108] to ensure that nuclear safety requirements are incorporated into the design.

Under the Equipment Reliability Program, BP-PROG-11.01 [126], life-cycle management integrates ageing management and economic planning to optimize the service life of SSCs and maintain an acceptable level of performance and safety over the life of the plant. The implementing procedures deal with scoping and identification of critical SSCs, continuing equipment reliability improvement, preventive maintenance implementation, performance monitoring, equipment reliability problem identification and resolution, long-term planning and

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

life-cycle management. As stated in Section 6.0 of the program [126], “All records arising from this program are identified in implementing procedures.” Therefore, the program ensures all systems meet their design intent and performance criteria and the associated changes are properly documented.

The Plant Design Basis Management program BP-PROG-10.01 [106] was established to ensure that the plant design meets safety, reliability and regulatory requirements. The objective of the program is to maintain the design basis and to ensure that the plant can operate safely for the full duration of its life. BP-PROG-10.01 supersedes BP-POLICY-10 Plant Design and Modification and its supporting programs. The procedures for meeting the requirements for CSA N286-05 [27] Annex A.8, Design documentation, which required a suite of design documentation to be used by organizations responsible for construction, commissioning, operation and decommissioning are specified in Appendix A of BP-PROG-10.01 [106]. As part of Bruce Power’s Process and Document Enhancement Project, undertaken since the preparation of the Bruce 1 and 2 ISR, a number of revised procedures have been issued to support the execution of the Plant Design and Modification policy. These improvements include:

- Strengthening the programs by specifying the related codes and standards and identifying the interfacing documents for each process.
- BP-PROG-10.03 on Configuration Management [118] was revised in 2014 to incorporate new implementing document BP-PROC-00647 [122] and in 2015 to provide alignment with responsible program and department management positions. The Configuration Management (CM) Program as a stand-alone program establishes guidance to promote consistent application of the following:
  - Clearly define and communicate CM scope, responsibilities, authorities, principles and interfaces;
  - Design basis and licensing basis requirements, which apply to the plant will be accurately identified, documented, maintained and accessible;
  - The plant’s physical SSCs, and process computer controls will conform to design basis and licence basis requirements;
  - Design basis and licence basis requirements will be accurately reflected in plant documentation and in processes and procedures for altering, maintaining, testing and operating the plant;
  - Consistency will be maintained among sources of plant information (documents and electronic data), as well as between plant information and the plant physical and functional characteristics;
  - Continuous improvement of CM will be achieved by monitoring and assessing CM-related activities and by incorporating feedback of lessons learned from in-house and industry best practices and experience.

These improvements would be strengthened by a controlled, centralized and accessible company database to track licence concessions granted to Bruce Power by the Regulator, as indicated in Appendix A.6. Bruce Power should establish such a database (see SF1-24 in Table 8).

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

As part of the Bruce Power Pressure Boundary Program, discussed in Licence Condition 5.2 of the Licence Conditions Handbook [2] Bruce Power is currently undergoing a reconciliation process. Registration of unregistered systems and legacy system design changes have been planned and prioritized. Bruce Power provides periodic updates under Action Item 091413; the last update was provided in NK29-CORR-00531-12884 [150]. Further information is provided in Section 5.3. Going forward, for any new installations, the records requirements of CSA N285.0 will be followed through the Bruce Power Pressure Boundary QA Program. However, as noted in Section 4.1, gap SF1-21 in Table 8, has been identified due to the numerous issues that require effective resolution to ensure a robust program and repeat findings from previous audits.

For updated and current design documentation, the Policies, Programs and Processes discussed above and identified in Section 4 of this document ensure that Bruce Power will meet the requirements of this review task in future.

Issues relevant to the adequacy of design documentation are identified as SF1-8 to SF1-11, SF1-13, SF1-14, SF1-16 through SF1-21, and SF1-23 in Table 8 are considered gaps. These gaps relate to the adequacy of design documentation. The sources of these issues are micro-gaps against CNSC REGDOC-2.5.2, CSA N289.1 and CSA N290.1 requirements, as presented in Table 8.

## 5.5. Compliance with Plant Design Specifications

This review task requires a review for compliance with plant design specifications.

The original design of Bruce B met the objectives and requirements of the Atomic Energy Control Board (AECB) that were current at the time. It complied with the current design requirements, AECB regulatory requirements, and the AECL/Ontario Hydro Quality Assurance programs. Plant design specifications were not explicitly produced as part of the original design basis of Bruce B.

Design guides for Bruce B safety systems “provide a list of those particular requirements and standards which must be met by those systems in a nuclear power plant associated with public safety” as defined in the purpose and application of Safety System design guides (Section 1, [165]). The Bruce B design guides were modified to recognize the intent of the Bruce-B-repeat concept (Bruce B continued the basic design of the Bruce A station) while following the safety criteria for the newer generation of nuclear power plants at the time. Significant deviations from the design guides were only made with prior approval of the Safety Design Concepts Branch (AECL), Nuclear Studies and Safety Department (Ontario Hydro) and the Manager of Engineering for Bruce B. A system was in place to handle such deviations by means of supplements to the design guides in question (Section 3 of [165]).

Currently, the Design Management Procedure, BP-PROC-00335 [107] applies to design activities required to maintain the plant design basis. Section 4.4.1 of the Design Management Procedure, BP-PROC-00335 [107] lists implementing procedures under design management, which along with the use of good engineering practice and compliance with relevant codes, standards and applicable design, ensure the design is correct.

The plant design basis is the fundamental specification defining the parameters that ensure that owner and regulatory requirements are met. The design basis is the foundation for the



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

development of the detailed design requirements for the individual SSCs. The design basis establishes the fundamental requirements for design. It is supplemented by, and makes reference to, design codes, standards and conventions, engineering analyses, and regulatory requirements. Design management and nuclear safety assessments are complementary and iterative processes, providing assurance that the plant design basis is confirmed by safety analysis, as described in design documentation and documented in the Analysis of Record (AOR), which includes the Safety Report (SR), and provides a consistent basis for safe operation.

The SOE is the set of operational limits and conditions that ensure that the plant is operated in conformance with the safety analysis, which in turn verifies the adequacy of the design from a nuclear safety perspective. The SOE limits identify the safe boundaries for plant operation. These limits identify the safe boundaries for plant operation. The SOE is documented in the Operational Safety Requirements (OSRs), which comprise the operating limits for a system. The OSRs document those aspects of the SOE that are derived specifically from the deterministic safety analysis. The plant configuration baseline for the specification of the OSRs is the as-built design, issued operating documentation and the AOR at the time of OSR issue. Operating limits are compiled from the safety analysis and design limits specified in the design basis documents into system-based requirements that can be implemented by plant staff. The OSRs are supported by Instrument Uncertainty Calculations (IUCs), which quantify the instrumentation errors and uncertainties associated with safety analysis limits. Bruce Power has completed its baseline SOE project, which consisted of documenting the limits and conditions derived from the safety analysis in OSRs, completing the corresponding IUCs, and performing Gap Assessments to verify that the requirements are completely and accurately reflected in the station operating documentation

The preparation and maintenance of the OSRs is governed by DPT-NSAS-00012 [146]. Gap analysis is performed (DPT-RS-00015 [166], Safe Operating Envelope Gap Assessment) to ensure that station design, operation, and maintenance comply with the OSRs and IUCs. The gap analysis to ensure that plant is being operated in accordance with the specified requirements is administered through DPT-RS-00015 [166], Safe Operating Envelope Gap Assessment.

In 2012, the CNSC conducted a pilot Type I Inspection of the implementation of SOE program at Bruce B [167]. CNSC staff observed or identified areas of strengths, as well as areas where improvements are needed, in order for Bruce Power to meet the intent of CSA N290.15-10 [32], which provides requirements for an SOE program. The Bruce Power response to CNSC recommendations on SOE was documented in Attachment A of NK29-CORR-00531-10884 [168]. Bruce Power issued AR 28404125 [169] to track the work to resolve gaps in the governance and implementation of CSA N290.15. The following Bruce Power programs, and their affected implementing procedures, were identified as requiring revision:

BP-PROG-10.01, Plant Design Basis Management [106]

BP-PROG-10.02, Engineering Change Control [112]

BP-PROG-11.01, Equipment Reliability [126]

BP-PROG-12.02, Plant Chemistry Management [170]

BP-PROG-12.03, Fuel Management [171]

 <div style="font-size: small;">Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

These programs and the affected implementing procedures were revised, and AR 28404125 is complete<sup>4</sup>. In all cases, statements were added to describe how each procedure/program relates to the SOE. As applicable for some of the governance documents, specific steps were also added to address impacts to the SOE. The completion of the SOE baseline project and subsequent programmatic activities has established the basis for compliance with CSA N290.15, which outlines the requirements for the SOE.

In summary, Bruce Power meets the intent of the requirements of this review task.

## 5.6. Safety Analysis Report or Licensing Basis

This review task requires a review of the Safety Report or licensing basis documents following plant modifications and in light of their cumulative effects and updates to the site characterization. The purpose of this review task is to assess the extent to which the plant meets modern requirements that may become part of the licensing basis in future.

The Bruce Power ECC program (BP-PROG-10.02) [112] and CM program (BP-PROG-10.03) [118] are the means by which plant modifications are reflected in the design basis for the facility.

BP-PROG-10.02 [112] establishes the scope of engineering change procedures and documentation. Through a screening process, engineering changes are classified by safety significance and scope through the use of comprehensive lists, including a Design Scoping Checklist [172], Design Review of Design Change Notice [173] and Design Products Challenge Board Checklist [174]. With these, the scope of the design plan is established [175], including Design Change Packages (DCPs) and Design Change Notices (DCNs).

Throughout the design modification process, these are routed through stakeholder review and approvals according to design authorities established in DIV-ENG-00009, Design Authority [109].


Design engineers and system engineers of interfacing systems potentially impacted by the design modification are identified as part of the Design Scoping Checklist [172] and required to approve the scope of the modification outline.

The engineering change process requires the identification of documents affected by the design change. An affected document is defined as any document, whose revisions are controlled, that needs to be accepted, created, revised, superseded or declared obsolete due to a design change [115]. Affected equipment is similarly identified in the ECC process.

The impact of the design modifications managed through ECC on the safe operation of the plant is assured by including Reactor Safety and Nuclear Safety as stakeholders in the design scoping checklist. The Safety Report is required to be updated every five years to address the cumulative updates to the safety basis [176].

The current Bruce B Safety Report incorporates the consequences of changes in actual plant configuration into the analyses. This includes the impact of ageing to the number of Effective Full Power Days (EFPD) covering to at least 2019 [177].

<sup>4</sup> AR 28404125 and some of the program and procedure revisions were completed after the freeze date for the Bruce B PSR.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

A suite of safety analyses was performed for design basis accidents most impacted by ageing, incorporating the impacts of ageing to 2019 [177], which meet CNSC REGDOC-2.4.1 requirements and identified relevant gaps. This suite of safety analyses was submitted to the CNSC in support of the licence renewal process [177], and includes:

- Loss of regulation (Neutron Overpower (NOP) trip setpoint calculations) [178];
- Small Loss-of-Coolant Accident (LOCA) [179];
- Loss of Flow [180]; and
- Large Loss-of-Coolant Accident (LLOCA) [181].

This re-analysis demonstrates that the units are safe to operate now, and processes are in place to ensure safe operation up to 10550 EFPD (approximately December 2019). The other events of Part 3 of the Safety Report [53] are not significantly impacted by the current condition of the plant.

Part 3 of the Safety Report includes analysis originally performed at Ontario Hydro/Ontario Power Generation (OPG) under previous safety analysis standards and older safety analysis code quality assurance requirements. All new analysis that have been included in the current Safety Reports and/or the AOR since the implementation of improved analysis procedures are in compliance with quality assurance requirements of CSA N286.7-99 [29]. The continuous improvement in the safety analysis procedures is evident by further modification to the analysis procedures being implemented to introduce CNSC REGDOC-2.4.1 [182] requirements, in preparation for phasing in CNSC REGDOC-2.4.1 implementation in the Safety Report Improvement (SRI) program. The revised safety analysis procedures are in the process of being revised, with an expected completion date of December 2017.

Bruce Power implementation of CNSC REGDOC-2.4.1 and SRI activities are being tracked under Action Item 090739 [183]. The SRI Plan for Bruce A and Bruce B was provided to the CNSC [184]. The SRI Plan and project description, including scheduled timelines, were accepted by the CNSC [185]. The SRI strategy consists of two main elements:

- A three-year SRI Project will be undertaken to upgrade the Bruce B Safety Report to align with the CNSC REGDOC-2.4.1 framework. This update will include an event classification scheme of plant states including AOOs, Design Basis Accidents (DBAs) and Beyond Design Basis Accidents (BDBAs) (identified as gap SF1-1 in Table 8), which is not applied in the current safety analysis. Additionally, a new Safety Report appendix on Common Mode Failures will be introduced into the Bruce B Safety Report. This new appendix will be structured per the CNSC REGDOC-2.4.1 framework, with new CNSC REGDOC-2.4.1 compliant analyses.
- An ongoing Safety Analysis Improvement Program will be implemented to perform CNSC REGDOC-2.4.1 compliant analyses on an ongoing basis. Bruce Power is targeting the end of 2017 to complete these combined activities and has been providing annual updates on progress.

In view of the importance of CNSC REGDOC-2.4.1 as the primary regulatory document for Deterministic Safety Analysis, a clause-by-clause review was conducted against this standard in Safety Factor 5: Deterministic Safety Analysis.



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Bruce Power is transitioning to REGDOC-2.4.2 for PSA over the current licence period and has a plan in place (see Section 4.1 Safety Analysis Program of LCH [2]) to fully comply with it by the June 30, 2019, target date. The combination of S-294 work already completed (which includes Emergency Mitigating Equipment credits) and the Seismically Induced Fire and Flood and Irradiated Fuel Bay Analyses (i.e., Fukushima action items related to PSA are complete [77] and accepted by CNSC [186]) will meet the requirements of CNSC REGDOC-2.4.2. Since the requirements in Section 4 of CNSC REGDOC-2.4.2 are essentially the same as S-294, Bruce Power will close any gaps that have been identified by CNSC staff [187]. There is an on-going industry effort to develop a methodology for site-wide PSA.

To comply with the guidance in Section 5 of CNSC REGDOC-2.4.2, Bruce Power has prepared a summary report of the results and assumptions of the Bruce Power PSAs that has been posted on the Bruce Power Website [188] for the purpose of making this information available to the public.

Any changes to methodologies and the PSA reports will be submitted according to the Bruce Power PSA governance for the required 5 year update of the PSAs. In view of the importance of CNSC REGDOC-2.4.2 as the primary regulatory document for PSA, a clause-by-clause review was conducted against this standard in Safety Factor 6: Probabilistic Safety Analysis

Bruce Power's most recent updates to the Derived Release Limits (DRLs) for Bruce A and Bruce B were completed in accordance with CSA N288.1 and were included in the PROL renewal applications (Bruce B, NK29-CORR-00531-11252 [19]). These CSA N288.1-aligned DRLs for the licensed facility at both Bruce A and B nuclear facilities are summarized in the DRLs table under the compliance verification criteria for licence condition 9.1 Environmental Protection Program of the current Bruce A and Bruce B Licence Condition Handbook [2].

Based on the assessments of the topics above associated with this review task and against requirements of CNSC REGDOC-2.5.2, a number of gaps related to Safety Goals (SF1-2), Initiating Events (SF1-3), Legacy Design Analysis (SF1-4), Operator Emergency Response (SF1-7), Timing of Operator Actions (SF1-9) and Electrical Power Systems (SF1-12) have been identified, and are listed in Table 8.

## 5.7. Plant SSCs Important to Safety


This review task requires a review of plant SSCs important to safety to ensure that they have appropriate design characteristics and are arranged and segregated in such a way as to meet modern requirements for plant safety and performance, including the prevention and mitigation of events that could jeopardize safety.

As presented in Section 5.1, Bruce Power employs a number of SSC lists to serve specific objectives related to different aspects of safety considered in, for example, design, safety analysis, equipment reliability, structural integrity. The SRSL applies to all work related to the execution of design, commissioning and operation of the systems. Systems in the SRSL receive increased emphasis in the area of maintenance, testing, availability and qualification requirements. This emphasis is graduated depending on the classifications and the safety-related functions within the listing. For example, the Safety System Testing program [139] is focused on testing safety related SSCs to determine if they are available and has a direct link to equipment reliability. The Bruce B PROL and OP&P require that an approved

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

testing program exist to ensure that specific SSCs are available, reliable and effective. Specific lists are as follows:

- The System Classification List is established and maintained through procedure System and Item Classification [140], which defines the requirements, processes, and responsibilities for activities associated with pressure retaining SSCs for system and component classification associated with facilities governed by CSA N285.0. It also describes the process for obtaining CNSC approval of the proposed classification for new systems, components, or modifications. The procedure outlines the requirements for preparing, or updating, the System Classifications List with required information (including system classification and registration) for pressure retaining systems or components.
- The EQ SRCL is a list of all EQ safety-related equipment and components. It includes the parent components and all associated support components which are required to ensure the parent components function. All components that are logically, electrically, pneumatically, or hydraulically connected to the parents, and must function or not fail in order to support the correct operation of the parent component, are considered support components of the associated parent(s). This is true up to and including the first isolating device, such as motor starter, circuit breaker, instrument air root valve, normally closed valves, etc. Components beyond this “boundary” are covered by other parent components. All EQ SRCL parents and support components are entered in the Environmental Qualification Information System (EQIS) database per SEC-EQD-00022 [141].
- The Bruce Power Seismic Qualification Standard [143] provides a summary of the seismically qualified systems for Bruce B. They are specified in detail in NK29-DG-03650-002 [143] which invokes CAN-N289.3 and N289.4.
- Fire Safe Shutdown System List in Appendix B DPT-PDE-00028 [144] is a list that identifies all of the SSCs credited for the safe shutdown of the plant in the event of a fire.
- The SOE system list includes systems that are credited with an accident mitigation function in the Safety Report or supplementary analysis. In addition, it includes systems where their initial conditions could impact on accident consequences. The major systems that support the SOE have been included in the Preparation and Maintenance of Operational Safety Requirements DPT-NSAS-00012 [146], the procedure used to prepare and maintain OSRs. It has defined the SOE as “the set of operational limits and conditions within which the nuclear generating station must be operated to ensure conformance with the safety analysis upon which reactor operation is licensed, and which can be monitored by, or on behalf of the operator and which can be controlled by the operator. These collectively identify the safe boundaries for plant operation” (Section 3.1.4). Table 1 of DPT-NSAS-00012 [146] provides the minimum list for which OSRs are required. The systems requiring an OSR for Bruce B are discussed further in Safety Factor 2: Actual Condition of SSCs.
- The groupings in the assessment of Systems Important to Safety for the Safety and Licensing Portion of the Nuclear Asset Management Program [147] are used to establish

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

the overall list of SSCs to be in scope of the Nuclear Safety and Licensing portion of the Nuclear Asset Management Program.


- The scope of which SSCs are included in the performance and condition monitoring program is identified by assessing the criticality of the SSC. This is done by applying the appropriate screening criteria to the function of the SSC and assessing the impact of SSC failure on plant safety, reliability or economics. Tables of Bruce B systems and their relative placement in the hierarchy of importance in the definition of the scope of the performance and condition monitoring program are included in BP-PROC-00781, Performance Monitoring [189]. These tables are divided into three tiers:
  - Tier 1 systems, which are systems important to safety in accordance to RD/GD-98 criteria. These are mandatory inclusions in the performance and condition monitoring.
  - Tier 2 systems, which are systems that are important to generation and asset preservation. These are also included in the performance and condition monitoring program.
  - Tier 3 systems, which are non-critical systems that have been monitored historically. They are excluded from the general system performance and condition monitoring program (as a result of the application of the principles contained within AP913).

As required by RD/GD-98 [190], Bruce Power identifies all systems important to safety. This is implemented through procedure DPT-RS-00012 [128]. The procedure describes the logic and processes involved in evaluating the modelled systems in Bruce Power's Probabilistic Risk Assessment, to determine which safety-related systems are risk-significant. It also specifies the screening criteria for assessing risk significance of systems, and the criteria for monitoring their performance. The procedure forms part of the set of procedures that support the Bruce Power Reliability Standard, which defines the Bruce Power Reliability Program.

As part of the post-Fukushima action items Bruce Power re-evaluated site-specific magnitudes of each external event to which the plant may be susceptible using modern calculations and state of the art methods. Site-specific design protection for each external event was also evaluated.

This work was completed in the S-294 submission in reference NK21-CORR-00531-11729 [191] which included site-specific external hazard analysis. Supporting reports, namely the assessments of Seismic Review Level Conditions (SRLCs) for high winds and seismic events and a review of the potential impacts of seismically induced internal fires and internal floods (Enclosures 4 through 7 of NK29-CORR-00531-12195 [77]), included several recommendations. Bruce Power initiated a project to assess these recommendations, and has completed the conceptual engineering phase (as discussed in Attachment B, Section 2.5 of [78]). Review Level Earthquake (RLE) results are provided in Table 5 of Safety Factor 6.

For beyond design basis accidents, the conclusions from a post-Fukushima assessment is that the existing containment SSCs can accommodate single unit severe accidents that progress to corium/concrete interaction (CCI), provided that no significant failures of mitigating functions occur [192]. However, the existing SSCs cannot sufficiently accommodate simultaneous severe accidents in multiple units, particularly if CCI occurs. Options for enhancing the ability of

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

containment to accommodate severe accidents in multiple units are being evaluated as part of an integrated suite of potential enhancements [192].

The report COG-JP-4426-014-R0 (attachment of NK29-CORR-00531-12981 [193]) summarizes the conditions that must be satisfied, and the plant capabilities that must exist, in order to demonstrate containment integrity. It is concluded that in combination with existing plant features, supporting analyses (e.g., Level 2 PSA) and various plant enhancements, either planned or under active evaluation by the utilities as part of their post-Fukushima response, provide confidence that maintaining containment integrity is an achievable goal following a severe accident.

In 2015, Bruce Power conducted a Bruce B Containment and Vacuum Building Pressure Test, the final results of which are provided in Enclosure 1 and Enclosure 2 of NK29-CORR-00531-12650 [79]. The results of the pressure test for both the containment structure and the vacuum building show that the leakage rates meet the acceptance criteria.

As a result of the review of plant SSCs important to safety, it was noted that reliability requirements for some SSCs do not meet requirements and/or safety goals. This is identified as gap SF1-5 in Table 8. The sources of this issue are micro-gaps against CNSC REGDOC-2.5.2 and CSA N290.1 requirements, as shown in Table 8.

## 5.8. Spent Fuel Storage Strategy

This review task requires a review of the strategy for the spent fuel storage and conduct of an engineering assessment of the condition of the storage facilities, the records management and the inspection regimes being used.

For the purpose of this review spent fuel is referred to as irradiated fuel. The strategy for irradiated fuel storage consists of a primary irradiated fuel bay, secondary irradiated fuel bay, a transfer duct between the two bays, and associated cooling systems, instrumentation and control (Safety Report, Part 2, [155]). The primary irradiated fuel storage bay is used for storing irradiated fuel for a minimum of six months after removal from the reactor to allow the decay heat of the bundles to subside. The designed storage capacity of the primary bay at normal storage is 42,432 bundles (see Design Description, Section 1.2 of NK29-DM-29-35360 [194]). After six months, the fuel may be transferred, underwater, to the secondary irradiated fuel storage bay, as described in Section 10.2.5.2.4 of Part 2 of the Safety Report [155]. After a sufficient cooling period, fuel bundles are transferred to dry storage containers and removed from the Bruce B station. Once removed, the bundles in dry storage are managed by Ontario Power Generation.

The engineering assessment of the condition of the storage facilities has been conducted as part of the Fukushima Action Items as discussed below. The adequacy of the irradiated fuel bay design in Bruce A has been assessed in response to CNSC action items related to the Fukushima event. The Bruce A Primary Irradiated Fuel Bay was selected for detailed analysis as it was determined to be the more limiting than Bruce B from a structural integrity perspective. In the event of a loss of cooling to the Irradiated Fuel Bays (IFBs) in which the bay water could reach boiling temperatures, analysis determined that there would be no structural failure of the bay integrity that could result in a loss of inventory from the bay. The only significant loss of bay inventory would result from boil-off [195]. An assessment of the potential for hydrogen

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

generation in the IFB area showed that significant hydrogen generation will only occur if fuel becomes exposed due to IFB draining (see Enclosure 1, Section 3.5, [192]). Design modifications to enable water to be added to the primary and secondary bays using portable pumps have been completed and are available for service. CNSC staff verified the installation of the emergency water makeup at both stations, and visually traced the pipe from the fire hose connection to where it extends over the top of the primary and secondary irradiated fuel bays (see Section 4.1 of [196]). The IFB structural analysis [195] demonstrated that the heatup (to boiling) and subsequent cooldown cycle of the IFBs will not result in through-wall cracking of the concrete and thus will not result in draining of the IFBs. The analysis recommended that cooling mitigation measures be initiated within the first few hours of an accident to control the propagation of any cracks. Given the results, Bruce Power has no plans to structurally enhance the Bruce B IFBs. Based on the CNSC staff review of Bruce Power's Irradiated Fuel Bay Structural Integrity Analysis, the related Fukushima Action Items were closed [197].

Bruce Power has enhanced the understanding of severe accident phenomena and SAMG capabilities undertaken under CANDU Owners Group (COG) Joint Project 4426 [198], followed by station-specific implementation. The scope of the work involves the enhancement of SAMG to include IFB events [195]. The generic CANDU Severe Accident Management (SAM) Technical Basis Documents (TBD) and guideline document have been revised to include the shutdown state and events that could cause damage to the fuel in a reactor core, in transport to storage, or stored in a spent fuel pool.

The SAMG updates to address multi-unit events and irradiated fuel bay events have been completed per Attachment B of the Bruce Power Progress Report No.7 [199]. The work related to Irradiated Fuel Bay events primarily involved the creation of new documents for each station; e.g., IFB Severe Challenge Guidelines and associated Computational Aids, including IFB Enabling procedures.

In regards to records management, Bruce Power is currently completing the implementation of RD-327 Nuclear Criticality Safety [24]. An internal gap assessment to identify the required changes to processes and procedures has been conducted. The majority of changes address the removal of procedural references to Low Void Reactivity Fuel (LVRF), a project which is no longer being pursued at Bruce Power. Other than LVRF the remaining implementation of the requirements of RD-327 into Bruce Power's governance deals with security sensitive elements. The implementation date was extended to May 31, 2016 [34].

Tracking of irradiated fuel inventory and location within the entire station is performed with the NuFLASH program, as noted in Section 3.5 of Record Irradiated Fuel Discharge Using NuFLASH [200]. This system provides the necessary record keeping capability to ascertain inventories and discharge dates of all fuel in the primary and secondary fuel bays.

In regards to inspection regimes, the Bruce B periodic inspection plan, NK29-PIP-20000-00001 [201], covers the requirements of CSA standard N291 for Bruce B Safety Related Structures, which include facilities for the storage of irradiated fuel and other radioactive waste material. This plan requires that all safety related structures are visually examined, and that the examination shall be of sufficient frequency and physical extent to define any significant changes or degradation. Inspections under the CSA N291 program have been scheduled through recurring Action Requests (AR) in PassPort for each structure.



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

In summary, Bruce Power meets the requirements of this review task with the following exception. The design requirement for sufficient space to accommodate the entire reactor core inventory at all times is not reflected in the design and operating documentation. This is identified as gap SF1-13 in Table 8. The sources of this issue are micro-gaps against CNSC REGDOC-2.5.2 requirements as shown in Table 8.

## 6. Interfaces with Other Safety Factors

There is some degree of interrelationship among most of the 15 Safety Factors that comprise the Bruce B PSR. The following identifies specific aspects of this Safety Factor that are addressed in, or where more detail is provided in, another Safety Factor Report.

- “Safety Factor 2: Actual Condition of SSCs” Section 4.0 provides an overview of the current state of system health monitoring, reporting and management programs and processes. Systems requiring an OSR are discussed in Section 5.3. The results of this assessment have been applied directly to this Safety Factor in support of relevant review tasks.
- “Safety Factor 3: Equipment Qualification” in Appendix A (A.2), assesses the requirements for seismic design and qualification of CANDU plants. The results of this assessment have been applied directly to this Safety Factor in support of relevant review tasks.
- “Safety Factor 4: Ageing” in Appendix C (C.1), performs a code-to-code assessment of CSA N287.1-14, in support of the incremental clause-by-clause assessment of CSA N287.1-14 in Appendix B (B.2).
- “Safety Factor 5: Deterministic Safety Analysis” in Section 5.4, assesses the SOE program. Appendix A (A.2) of Safety Factor 5 presents an assessment of requirements and guidance regarding computer programs used in design and safety. The results of this assessment has been directly applied to the review tasks of this Safety Factor.
- “Safety Factor 6: Probabilistic Safety Analysis” in Section 5.1 addresses the adequacy of the existing probabilistic safety assessment (probabilistic risk assessment (PRA)) including At Power Seismic PRA. Furthermore, in Appendix B (B.1) a clause-by-clause assessment of CNSC REGDOC-2.4.2 is performed. The results of this assessment have been directly applied to the review tasks of this Safety Factor, as applicable.
- “Safety Factor 7: Hazard Analysis” in Appendix B (B.3), performs an incremental clause-by-clause assessment of requirements and guidance from CSA N293-12. The results of this assessment have been directly applied to the review tasks of this Safety Factor, as applicable.
- “Safety Factor 9: OPEX and R&D” provides detailed discussions regarding use of operating experience from other plants and research findings. The results of this review have been applied to clause 5.5 of REGDOC-2.5.2 and the review tasks, as applicable.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- “Safety Factor 10: Organization and Administration” in Section 5.3.3 reviews the control of documents, products and records at Bruce Power. The results of this review have been directly applied to the review tasks of this Safety Factor, as applicable.
- “Safety Factor 12: The Human Factor” in Appendix A (A.1) performs a high-level assessment of G-276, Human Factors Engineering Program Plans.
- “Safety Factor 13: Emergency Planning”, performs a review of Bruce Power’s emergency planning including the implementation of SAMGs. The results of this assessment have been directly applied to clauses 8.6.12 and 8.10.3 of REGDOC-2.5.2 as well as to review tasks of this Safety Factor, as applicable.
- “Safety Factor 14: Radiological Impact on the Environment” presents a high level assessment of CSA N288.1-14 in Appendix A (A.2). The results of this assessment have been summarized in this report and have been applied to the review tasks of this Safety Factor, as applicable.
- “Safety Factor 15: Radiation Protection” in Appendix B.1, has assessed the state of Bruce Power’s Radiation Protection Program against applicable guidance. The results of this review have been directly applied to Clause 8.13.1 of REGDOC-2.5.2, and have been applied to the review tasks of this Safety Factor, as applicable.

## 7. Program Assessments and Adequacy of Implementation

Section 7 supplements the assessments of the review tasks in Section 5, by providing information on four broad methods used to identify the effectiveness with which programs are implemented, as follows:


- Self-Assessments;
- Internal and External Audits and Reviews;
- Regulatory Evaluations; and
- Performance Indicators.

For the first three methods, the most pertinent self-assessments, audits and regulatory evaluations are assessed. Bruce Power has a comprehensive process of reviewing compliance with Bruce Power processes, identifying gaps, committing to corrective actions, and following up to confirm completion and effectiveness of these actions. While there have been instances of non-compliance with Bruce Power processes, Bruce Power’s commitment to continuous improvement is intended to correct any deficiencies.

For the fourth method, the performance indicators relevant to this Safety Factor are provided. These are intended to demonstrate that there is a metric by which Bruce Power assesses the effectiveness of the programs relevant to this Safety Factor.

Taken as a whole, these methods demonstrate that the processes associated with this Safety Factor are implemented effectively (individual findings notwithstanding). Thus, program



	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

effectiveness can be inferred if Bruce Power processes meet the Safety Factor requirements and if there are ongoing processes to ensure compliance with Bruce Power processes. This is the intent of Section 7.

## 7.1. Self-Assessments

Generally, self-assessments are used by functional areas to assess the adequacy and effective implementation of their programs. The results of each assessment are compared with business needs, the Bruce Power management system, industry standards of excellence and regulatory/statutory or other legal requirements. Where gaps are identified, corrective actions are identified and implemented.


The self-assessments:

- Identify internal strengths and best practices;
- Identify performance and/or programmatic gap(s) as compared to targets, governance standards and “best in class”;
- Identify gaps in knowledge/skills of staff;
- Identify the extent of adherence to established processes and whether the desired level quality is being achieved;
- Identify adverse conditions and Opportunities for Improvements (OFI); and
- Identify the specific improvement corrective actions to close the performance/programmatic gap.


Table 7 provides selected relevant Focus Area Self Assessments (FASAs) that have been carried out between 2010 and December 31, 2015. They are listed as evidence of ongoing program effectiveness. A subset of these was reviewed in support of the evaluation of effectiveness of key programs for the review tasks of this assessment. Those selected are shown in **bold** and are summarized below.

**Table 7: Internal Self-Assessments Relevant to Plant Design**

Assessment Number	Title
SA-AUD-2010-03	Pressure Boundary Audit Compliance
SA-RS-2010-03	Fuel Defect Management
SA-COM-2010-04	Fidelity of Configuration Information to Plant
SA-NSAS-2010-03	Use of OPEX in Fuel Channels Life Cycle Management & Life Extension of Fuel Channels
SA-COM-2011-10	Fidelity of Configuration Information to Plant

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Assessment Number	Title
SA-COM-2011-08	ECC Adherence
SA-ELCE-2011-08	Equipment Reliability
SA-RS-2011-01	Fuel and Fuel Channel Program
SA-DMES-2012-03	Design Modifications Implementation
SA-COM-2012-05	MEL Quality Review
SA-COM-2012-04	Assessment of the Catalogue Health Program
SA-WMSI-SA-2013-01	Graded Approach to Shielding
SA-COM-2013-01	Assess Procedural Compliance in P.D.E (June 6, 2013)
SA-COM-2013-11	CAP Effectiveness in Engineering (December 5, 2013)
SA-COM-2013-03	Procedure Effectiveness Assessment of DPT-PDE-00046 Management of Drawdown Contracts (19Dec2013)
SA-COM-2013-05	Configuration Information Change Procedure Adherence (09 Oct 2013)
SA-COM-2013-06	Assess Bill of Materials Health (Aug 26 2013)
SA-OCP-2014-07	Reactivity Management
SA-MPR-2014-02	Foreign Material Exclusion
SA-MPR-2014-08	Equipment Capability
SA-ERI-2014-02	Asset Management Program Effectiveness
SA-ERI-2014-06	Heat Exchanger Program
SA-COM-2014-07	EQ Program Health
SA-COM-2014-03	Design Change Management
SA-COM-2014-01	Engineering Change
SA-BPMS-2014-01	Compliance with CSA N286-05


 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Assessment Number	Title
SA-SSO-2014-02	Radioactive Waste Segregation
SA-PI-2014-04	Effectiveness of FASA Process Improvements (02 Sept. 2014)
SA-COM-2014-04	"Quick Hit" Self-Assessment Project Controls Section (11 Nov. 2014)
SA-MPR-2015-04	Pressure Boundary
SA-BPMS-2015-02	SOFA PBQA Oversight
SA-ERI-2015-10	Technical Advocacy
SA-ERI-2015-11	System Performance Monitoring Plan Effectiveness
SA-COM-2015-14	Engineering Contract Practices
<b>SA-COM-2015-03</b>	<b>Configuration Management Engineering Governance Review</b>
<b>SA-COM-2015-05</b>	<b>N286.7 Design Engineering Implementation</b>
<b>SA-COM-2015-06</b>	<b>Pressure Boundary Assessment</b>
SA-COM-2015-10	Use of Engineering Judgment
<b>SA-ERI-2015-17</b>	<b>Station Engineering Setting and Reinforcing Standards</b>

#### 7.1.1. **SA-COM-2015-03 Configuration Management Engineering Governance Review**

The scope of this self-assessment includes all programs and procedures for the Configuration Management Engineering functional area. The in-scope documents include BP-PROG-10.01, 10.02, 10.03 and implementing procedures (BP-PROC-00244 and BP-PROC-00231 and DIV-ENG-00014 excluded).

N286-05 Annex A outlines the supplementary requirements for design that complement the generic requirements in Clause 5 of CSA N286-05, which requires design work be conducted in a planned and systematic progression of activities and work methods. BP-PROC-00363 [108] and its implementing procedures along with BP-PROC-00539 [115] were reviewed. It was concluded that the required elements are in place to meet the requirements of N286, although the FASA noted that interfaces are not always defined.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

It was identified that a separate procedure exists for Software Records, and recommended that that procedure be integrated into Section 6.0 of the required procedures. An SCR was raised (28513934) to correct this adverse condition which is targeted for November 2016.

During the last Bruce B peer review, an area for improvement was noted with respect to the timely update of operating documents following changes to safety analysis and the licensing basis. In particular it was noted that design requirements and operating documents were not always consistent with current safety analysis and licensing basis requirements. It was recommended that interfaces between safety analysis and the detailed design be clearly defined as laid out in CSA N286-05 Annex A, Figure A.1, Detailed design process map. This recommendation is captured by AR 28513935.

As all adverse conditions and opportunities for improvement are tracked and managed they are not identified as gaps for the purposes of this review.

### **7.1.2. SA-COM-2015-05 N286.7 Design Engineering Implementation**

The objective of this Self-Assessment was to determine the extent to which records required by procedure BP-PROC-00933 R000, Design Analysis Software Configuration Management and Standard CSA N286.7-99 are retrievable, legible and accurate. The scope focused on engineering design analysis software, used within the Mechanical and Civil Department of Engineering Support Division. Bruce Power Licence [2] condition 4.2, prescribes compliance with CSA N286.7-99.

The FASA concluded that BP-PROC-00933 was more aligned with the guideline (CSA N286.7.1-09) than the standard CSA N286.7-99. The procedure provides more instructions outlining how the requirements of the guideline and the standard are to be implemented at Bruce Power.

It was also concluded that documentation requirements listed in CSA N286.7-09 guideline have generally been met for commercial off-the-shelf software. Documents required for software development listed in the CSA N286.7-99 Standard, however were not found at Bruce Power. Only commercial off-the-shelf software is being used with software development documentation requirements covered by ASME NQA-1 (where noted).

The majority of analysis software in use at Bruce Power is commercial off-the-shelf software developed under vendor SQA program with compliance verified, typically, by the Nuclear Procurement Issues Committee (NUPIC). An SCR (28522224) was raised to confirm with the regulator that NQA-1 with audit by NUPIC is an acceptable practice instead of verification by Bruce Power of compliance with CSA N286.7-99. AR 28522224 has since been cancelled noting that: "CSA N286.7 requirements may be satisfied through a variety of methods. Compliance with other QA program elements pertinent to N286.7 and documented through recognized audits (such as NUPIC) is already permitted in this standard" [202].

An opportunity for improvement to seek out best practices by benchmarking other organizations' analysis software governance to streamline and improve the process at Bruce Power was also initiated under SCR 28522226, targeted for completion by the end of 2016.

As all adverse conditions and opportunities for improvement are tracked and managed these are not identified as gaps for the purposes of this review.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

### 7.1.3. SA-COM-2015-06 Pressure Boundary Assessment

The purpose of this FASA was to prepare for the 2015 PBQA Audit by evaluating the Engineering Support Division Compliance against the PBQA Program BP-PROG-00.04 [104] by evaluating the following two specific areas:

- Determine the effectiveness of actions that were assigned from the previous pressure boundary audit, AU-2014-00002; and
- Determine if existing Pressure Boundary procedures contain specific performance criteria to meet the licence requirement.

The effectiveness review of actions assigned during the 2014 audit (AU-2012-0002) was successful in identifying several actions that were completed prior to the start of the 2015 pressure boundary audit. A significant finding during the 2014 audit of not updating the SCLs as required by Bruce Powers Licence was successfully resolved, with CNSC correspondence supporting Bruce Power's Legacy Registration project as the SCL update vehicle.

The review of pressure boundary procedures to determine whether they contained performance criteria (verification and/or oversight activities) was performed. It was determined the majority of procedures had the required section in place. There were however four of 37 procedures that did not have the required section in place. SCR 28519572 was raised to rectify this gap for the identified procedures, and therefore this is not considered a gap for the purposes of this report.


### 7.1.4. SA-ERI-2015-17 Station Engineering Setting and Reinforcing Standards

The objective of this FASA was to assess areas of strengths and gaps in Station Engineering Managers establishing and reinforcing standards. Establishing and reinforcing standards is paramount to ensure core functions are performed in a consistent and thorough manner. It is very important that Station Engineering adhere to the processes that have been established to ensure a safe and reliable plant. One way is to ensure that this is adhered to is by having Section Managers reinforce this established standard within these processes.

The FASA assessed the Station Engineering Manager's establishing and reinforcing standards through the use of key engineering products and deliverables such as:

- Health Reporting
- Risk Identification and Escalation
- Engineering Evaluations
- Performance Monitoring
- Walk downs

The scope included interviews of Section Managers from across Station Engineering and a random review of some health report documents to assess that quality standards are being met. The interview guide and questions were developed using the World Association of Nuclear Operators (WANO) Performance Objectives and Criterias (PO&Cs) and the PO&C 2013-1, How

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

to Review Guide on Leadership. Based on interview question responses 13 strengths and 8 gaps were identified. This led to one opportunity for improvement to be identified with three assignment identified. SCR 28468121 was raised to track this opportunity for improvement and therefore this is not considered a gap for the purposes of this report.

## 7.2. Internal and External Audits and Reviews

The objective of the audit process as stated in BP-PROG-15.01 [203] is threefold:

- To assess the Management System and to determine if it is adequately established, implemented, and controlled;
- To confirm the effectiveness of the Management System in achieving the expected results and that risks are identified and managed; and
- To identify substandard conditions and enhancement opportunities.

The objective is achieved by providing a prescribed method for evaluating established requirements against plant documentation, field conditions and work practices. The process describes the activities associated with audit planning, conducting, reporting, and closing-out. The results of the independent assessments are documented and reported to the level of management having sufficient breadth of responsibility for resolving any identified problems (as stated in Section 5.14.2 of [28]).

As specified in BP-PROC-00295, Planning & Scheduling Audits [204], Bruce Power's Oversight Management Program is comprised of audits, performance based assessments and external performance assessments. The audit frequency is generally determined to be at least once every three calendar years. However, frequencies may vary depending on the identified areas of concern.

The following is a subset of audits relevant to this Safety Factor that have been carried out between 2012 and December 31, 2015:

- AU-2015-00020 Fire Protection Program
- AU-2015-00018 Temporary Change Control
- AU-2015-00006 Pressure Boundary Quality Assurance Program Section 18
- AU-2015-00007 Pressure Boundary Quality Assurance Program (excluding Section 18 Audit)
- AU-2014-00002 Pressure Boundary Quality Assurance Program (excluding Section 18 Audit)
- AU-2013-00015 PassPort Equipment Data Management
- AU-2012-00001 Critical Drawing Management

These audits are summarized in the following subsections to support the evaluation of effectiveness of key programs for the review tasks discussed in Section 5 herein.



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

### 7.2.1. AU-2015-00020 Fire Protection Program

A fire protection audit was performed by a third party to satisfy the station licence conditions with three main objectives:

- Audit the fire protection program to confirm compliance with CSA N293-07 (In accordance with Clause 8.3.4, Fire Protection Program Audit);
- Audit of an emergency drill to assess performance level of Emergency Response Team as required by CSA N293-07 Clause 8.3.4.2(h)); and
- Conduct annual plant condition inspection in accordance with CSA N293-07 clause 8.3.5.1 to confirm compliance with the standard and the National Fire Code of Canada.

For the purposes of Safety Factor 1: Plant Design, only the third objective is discussed.

CSA Standard N293-12 [33], Clause 8.3.5.1 requires plant condition inspection be conducted by a qualified third party at least once a year. The Bruce B site inspections were conducted during the week of October 19, 2015. Auditors witnessed a response to an emergency drill by the Bruce Power Emergency and Protective Services - Fire Team (EPS-Fire) conducted on October 6, 2015. Auditing this emergency response exercise is a component of the fire protection program assessment, CSA N293-12 – clause 8.3.4.2(h), and serves as the annual drill as required by CSA N293-12 - clause 10.5.3 [33]. Accessible areas of the station were visually inspected to confirm the fire protection program was being implemented.

The Plant Condition Inspection found that facilities were generally compliant with operational requirements of the N293-12 Standard and the NFCC (2010). Exceptions to general compliance were noted which have been internally addressed by Bruce Power.

Overall, the station had better housekeeping practices in place than the previous annual inspections and it was noted that the station is following very good housekeeping procedures in all areas. In addition a lot of the miscellaneous materials such as brooms, tools, etc., located throughout the station have been cleaned up.

The Plant Condition Inspection found that facilities were compliant with the operational requirements of the CSA N293-12 Standard and the NFCC (2010).

The complete audit resulted in two findings and 13 opportunities for improvements; actions have been initiated on all items.

### 7.2.2. AU-2015-00018 Temporary Change Control

An audit evaluated the completeness of, and compliance to, BP-PROC-00638, Temporary Configuration Change Management [121] process. The audit was performed on Temporary Configuration Change Management activities from March 2013 through March 2015 and conditions found in the field at Bruce A and Bruce B during the conduct of the audit.

Document reviews included the following:

- BP-PROC-10.03 R005 Configuration Management
- BP-PROC-0638 R012 Temporary Configuration Change Management



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- FORM-12112 Temporary Configuration Change (TCC) Backup Record
- FORM-12113 Temporary Configuration Change (TCC) Backup Tag
- FORM-12523 Temporary Configuration Change Tag
- FORM-13096 Temporary Configuration Change Engineering Technical Verification
- Reports and data from the Temporary Configuration Change Software Database

Due to the Vacuum Building Outage and multiple unit outages at Bruce B during the conduct of the audit, the audit team focused on activities at Bruce A. Some sampling was done at Bruce B, but to a lesser extent.

This audit concluded that the Temporary Change Management process is incomplete but generally effective in meeting the objectives and purpose of BP-PROC-00638 [121]. Specifically it concluded that:

- The Temporary Configuration Change Management process is not always used where required to ensure temporary changes are adequately controlled, resulting in undocumented configuration changes and discrepancies between station documentation and configuration of field equipment. Failure to control changes can result in unknown/unexpected equipment status. Ongoing corrective actions are managed under AR 28506621.
- Staff are not always complying with the requirements of BP-PROC-00638. Non-compliances were found to exist with Engineering Technical Verification and other instructions. Failure to adhere to established processes can increase the risk that temporary changes are not adequately controlled. Ongoing corrective actions are managed under AR 28506629.
- The Temporary Change Management Procedure (BP-PROC-00638) contains inadequate procedure instructions and out-of-date information. The update of this procedure is being tracked under AR 28506636.
- The Temporary Change Management Procedure (BP-PROC-00638) does not adequately specify the applicable TCC records requirements to ensure documentary evidence exists to demonstrate that TCCs meet specified requirements for tracking temporary plant configuration changes from design basis. Corrective actions are tracked under AR 28506641.
- Personnel were found to be performing Peer Verification without holding the required qualification. The corrective actions are tracked under AR28506643.

As appropriate, these adverse conditions were assigned as actions and the corrective action process was followed for this audit to improve the adequacy of its implementation. Given that planned and monitored initiatives are underway for improvements in the efficiency.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

### **7.2.3. AU-2015-00006 Pressure Boundary Quality Assurance Program Section 18**

An audit of Bruce Power PBQAP was completed in February 2016 by the Bruce Power Nuclear Oversight and Regulatory Affairs Division (NORA) team. It was performed to verify Bruce Power's compliance with the audit requirements in Section 18 of the PBQAP [104], and to determine the effectiveness of the audit program. The audit scope involved sampling of the PBQAP audit activities completed or in progress since November 28, 2014. The audit included the applicable requirements of Section 1 (Organization), Section 2 (QA Program), Section 6 (Document Control), Section 16 (Corrective Action), Section 17 (QA Records) and training requirements of PBQAP audit personnel. Additionally, an evaluation of the status of Station Condition Records (SCRs) from the previous audit (AU-2014-00001) was completed.

Overall, it was found that Section 18 of the PBQAP and implementing procedures were effectively implemented. With one exception, performance criteria as defined in the audit processes were met.


Contrary to the requirements of BP-PROC-00635, Audits, R009 (including alterations dated September 1, 2015) suitability reviews and compliance assurance evaluations of corrective action plans and completed corrective actions as a result of adverse conditions identified during PB audits are not always completed within timeline requirements. This adverse condition is being tracked using SCR 28540061, and has the attention of management.

Due to the numerous issues that require effective resolution to ensure a robust program and repeat findings from previous audits this is assessed as a program gap (SF1-21) in Table 8, see further discussion in Section 4.1.

### **7.2.4. AU-2015-00007 Pressure Boundary Quality Assurance Program (excluding Section 18 Audit)**

An audit to verify Bruce Power's compliance with all sections, excluding Section 18 (Audits), of the requirements within the Pressure Boundary Quality Assurance Program Manual (BP-PROG-00.04 R022 [104]) along with the procedures that implement those sections of the program has been carried in October 2015. The audit scope included sampling of code activities completed since October 4<sup>th</sup>, 2014 and included activities completed at the Bruce A and Bruce B stations, and applicable Centre of Site locations.

Bruce Power's Pressure Boundary Quality Assurance Program (PBQAP) was evaluated to be generally effective at meeting the requirements of the latest CSA N285.0-12/N285.6 Series-12, including Update # 1 and Update # 2, General Requirements of Pressure-Retaining Systems and Components In CANDU Nuclear Power Plants/Material Standards for Reactor Components for CANDU Nuclear Power Plants. The program was found to be not fully effective in 4 of the 18 Sections that were evaluated under the scope of this audit (i.e., do not capture all of the requirements); Not fully compliant in 15 of the 18 Sections that were evaluated under the scope of this audit; and Performance Criteria are not adequately defined and implemented (identified within Adverse Condition # 4), and, where implemented, are not always being met.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

The Audit Results include Twelve (12) identified Adverse Conditions and Two (2) Opportunities for Improvement. Five (5) of the identified Adverse Conditions were deemed to be Programmatic, and Nine (9) of the identified Adverse Conditions are categorized as Continuing Adverse Conditions, identified in previous PBQA Audits. The audit team identified an Opportunity for Improvement for the identification in governance for use of low halogen tape and second Opportunity for Improvement was noted to enhance welding consumables traceability.

One of the more significant challenges to the program, and common thread throughout each Adverse Condition, is the inadequacy within the suite of PBQA implementing governance for the identification of Performance Criteria (Quantitative and Qualitative) and associated activities for Verification and Oversight, to monitor and ensure that processes are implemented and effective, and that staff adheres to requirements.

Improvements were noted within these 'problematic' areas; for example there is evidence of improvement for compliance in the use of Measure & Test Equipment (M&TE), recording of pre- and post-use testing using torque checking stations, and of recording of information for M&TE within PassPort for traceability to work activities. Since the issues identified during the audit are already captured in the program gap (SF1-21) in Table 8, no additional gap is identified for the purpose of this assessment.


#### **7.2.5. AU-2014-00002 Pressure Boundary Quality Assurance Program (excluding Section 18 Audit)**

An audit to verify Bruce Power's compliance with all sections, excluding Section 18 of the Pressure Boundary Quality Assurance Program (BP-PROG-00.04-R020 [104]), along with the procedures that implement those sections of the program, was performed in July 2014. The audit scope included pressure boundary activities that were completed since November 2013. This included activities completed at Bruce A, Bruce B and applicable Centre of Site locations. The program was evaluated to be generally effective at meeting the requirements of CSA N285.0-08/N285.6 Series-08 Update #1 (June 2009), but it was not fully compliant in 18 of the 19 Sections.

Issues reducing the effectiveness of the program were found in eight of the 19 Sections. It is noted that none of these sections by themselves, or in aggregate, significantly reduced the overall effectiveness of the program. Considerable effort has been taken to address sections with reduced effectiveness identified in previous years and some of the corrective actions are still in progress.

Eighteen of the 19 Sections had at least one area of program noncompliance identified. Only Section 19 (Authorized Inspection Agency) was determined to be compliant. The lack of a fully implemented Management Assessment process (which would allow for the line management to identify and correct issues during program execution) and the inability of line management to effectively use the corrective action system to correct identified adverse conditions were determined to be contributing factors.

The audit identified 31 Adverse Conditions and two Opportunities for Improvement that have been documented in 55 SCRs and one Escalation Letter. A further five SCRs were generated to address immediate concerns discovered during the course of the audit. An Opportunity for Improvement was identified for the design review process of Engineering Change Control

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

(ECC). The audit team also recommended modifications to the PassPort system to allow the identification of the Contract Manager associated with each contract (second Opportunity for Improvement).

The adverse conditions identified within the audit have been corrected through the Station Condition Records process. BP-PROG-00.04 was revised in December 2014 to address the audit findings and in 2015 for alignment with the requirements of 2012 edition of N285.0, including Updates No. 1 and No. 2.

Due to the numerous issues that require effective resolution to ensure a robust program and repeat findings from previous audits this is assessed as a program gap (SF1-21) in Table 8, see further discussion in Section 4.1.

### **7.2.6. AU-2013-00015 PassPort Equipment Data Management**

An audit of Bruce A and B Master Equipment (MEL) List records, Station Condition Records, and other relevant documentation was completed in June 2013 to evaluate implementation effectiveness of and compliance with BP-PROC-00584-R006, PassPort Equipment Data Management [120]. The completed audit identified requirements that were not completely implemented as numerous gaps were present between the procedural requirements and the actual MEL. The gaps identified with BP-PROC-00584 during the audit are listed below:

- There are no current initiatives to update the MEL to meet requirements;
- Not all requirements in the procedure are followed;
- The role of the MEL Single Point of Contact (SPOC) is not performed;
- CMT-66415-00001, PassPort V10 Configuration Management and Master Data Rollout (referred to in BP-PROC-00584 R006 [120]) is out of date and does not reflect current MEL management practices. Only select personnel have received this training;
- There are deficiencies between the procedure and the Bruce Power Controlled Document requirements; and
- MEL records were found to be inconsistent across different fields.

Overall, it was the auditor's insight that the lack of conformance to BP-PROC-00584-R006 has led to the increased tolerance for incomplete MEL records. This lack of complete records leads to increased burdens for the work groups on site. The audit found that BP-PROC-00584-R006 is not consistently adhered to. Master Equipment List records have numerous information gaps compared to the requirements of BP-PROC-00584. Thus, implementation of BP-PROC-00584 is not fully effective at satisfying its purpose of ensuring the MEL is maintained to current standards. Four adverse conditions were identified:

- BP-PROC-00584-R006 Procedural Non-Adherence
  - There were significant deviations in the sampled data from the procedural expectations.
- MEL Discrepancies

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- Multiple MEL records had errors and inconsistencies.
- BP-PROC-00584-R006 has errors, discrepancies, and non-adherence to the Bruce Power Controlled Document procedures.
- Ineffective use of the Self-Assessment Process
  - Actions to resolve performance gaps are not always completed which impacts the program effectiveness.

As appropriate, these adverse conditions were assigned as actions and the corrective action process was followed for this audit to improve the adequacy of the procedure's implementation. Given that planned and monitored initiatives are underway for improvements in the efficiency, these are not identified as gaps for the purpose of this assessment.

### 7.2.7. AU-2012-00015 Critical Drawing Management

An audit of Bruce Power Critical Drawing Management was completed in February 2012. The objective of the audit was to assess the implementation and compliance to DPT-COM-00004-R002, Critical Drawing Management [205] (now obsolete), to ensure time at risk for critical drawings is managed. The audit supports BP-PROG-10.03, Configuration Management [118]. For this audit, a sample of data and records was reviewed to assess compliance. The audit focused on higher priority drawings associated with the defined process that were applicable to the Bruce A and B Stations. Units 1 and 2 Restart activities, Center of Site, and Security Projects were excluded from the audit. The COG OPEX (Operating Experience) database was reviewed for relevant entries from January 2011 to February 2012. Four items were identified and it was recommended that a review of these items for lessons and actions gathered from the events be completed. Three adverse conditions were identified in the audit:

- Inadequate Procedural Compliance
  - An evaluation of ECC data showed consistent non-compliance with the approved work instructions.
- Inadequate Procedure Implementation and Quality
  - Procedures do not provide adequate integrated instructions as there are gaps in the instructions along with misalignments, duplication, and contradicting information which result in staff not working to an approved procedure. Not all of the process requirements are fully implemented.
- Ineffective use of the Corrective Action Process
  - The SCRs that were raised to identify and resolve the Critical Drawing Management adverse conditions were found to be closed when the adverse conditions within the SCRs were unresolved.

Overall, the audit deemed the implementation and compliance to DPT-COM-00004-R002 [205] was inadequate as the procedure was not fully implemented and not all work was compliant with the stated expectations. It was the auditor's insight that DPT-COM-00004 provides little value and expectations could be placed within existing procedures. As appropriate, the corrective



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

action process was followed for this audit to improve the adequacy of the implementation of this procedure. This was documented in SCR 28266458 as, “Investigate Obsolete DPT-COM-00004 and move all relevant information into the appropriate interfacing procedures”. Given that planned and monitored initiatives are underway for improvements in the efficiency, these are not identified as gaps for the purpose of this assessment.

### 7.3. Regulatory Evaluations and Reviews

After a licence is issued, the CNSC stringently evaluates compliance by the licensee on a regular basis. In addition to having a team of onsite inspectors, CNSC staff with specific technical expertise regularly visit plants to verify that licensees are meeting the regulatory requirements and licence conditions. Compliance activities include inspections and other oversight functions that verify a licensee’s activities are properly conducted, including planned Type I inspections (detailed audits), Type II inspections (routine inspections), assessments of information submitted by the licensee to demonstrate compliance, and other unplanned inspections in response to special circumstances or events.

Type I inspections are systematic, planned and documented processes to determine whether a licensee program, process or practice complies with regulatory requirements. Type II inspections are planned and documented activities to verify the results of licensee processes and not the processes themselves. They are typically routine inspections of specified equipment, facility material systems or of discrete records, products or outputs from licensee processes.

The CNSC carefully reviews any items of non-compliance and follows up to ensure all items are quickly corrected.

The Regulatory Oversight Report for Canadian Nuclear Power Plants: 2014 (the 2014 NPP Report) [206] provides the CNSC staff’s assessment of the Canadian nuclear power industry’s safety performance during 2014 and details the progress of regulatory issues up to April 30, 2015. The evaluations of all findings for the safety and control areas (SCAs) led CNSC staff, through site inspections, reviews and assessments, to the conclusions in Section 3.1.1.5 of the report. That section concludes that the physical design SCA at Bruce B met performance objectives and all applicable regulatory requirements. As a result, Bruce B received a “satisfactory” rating, unchanged from the previous year. The CNSC staff observations related to Bruce B Physical Design are listed below:

- Design governance
  - Equipment qualification – CNSC Staff found that Bruce Power’s environmental qualification program is in compliance with CSA N290.13-05, which is the design governing document. There were no significant compliance verification observations for Bruce B’s EQ program in 2014.
  - Pressure Boundary Design – Bruce Power continued the transition to CSA N285.0-08. Bruce B confirmed that SSC’s important to safety and security meet the design basis. On the basis of ongoing oversight activities in 2014 CNSC staff concluded that Bruce Power’s pressure boundary program is in compliance with the requirements of CSA N285.0-08.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- System design
  - Electrical power systems – Electrical inspections at Bruce B in previous years confirmed the electrical power systems are being maintained and tested to ensure that they will be able to perform their design functions. However some areas for improvement have been identified. Overall, there remains one outstanding item related to the “as-found conditions” of the battery capacity testing. This issue will be resolved by the end of 2016 and is of low safety significance.
  - Fire Protection Design – In November 2014, CNSC staff carried out a focused fire protection inspection against the requirements of CSA N293-07, as well as conducted oversight activities including document reviews and walk-downs. CNSC staff concluded that Bruce B’s fire protection program is both comprehensive and in compliance with the requirements of CSA N293-07.
- Component design
  - Fuel design – Bruce Power has a well-developed reactor fuel inspection program. In 2014, the fuel defect rate for Units 3 to 8 is below the industry average of about one bundle per year. Bruce Power has been effective at locating and defueling defective bundles. No regulatory limits were exceeded during 2014.

### 7.3.1. **Bruce B: CNSC Type II Compliance Inspection Report: BRPD-B-2016-002, Environmental Qualification Program, New Action Item 2016-07-7682**

The CNSC conducted a compliance inspection of Bruce Power’s Environmental Qualification Program in NK29-CORR-00531-13148 [207]. The onsite portion of the inspection was conducted from October 19<sup>th</sup> to 23<sup>rd</sup> 2015. The inspection assessed Bruce Power’s compliance to the regulatory requirements associated with this program. This inspection focused on verifying:

- That environmentally qualified (EQ) equipment will perform its required function when exposed to relevant operating and design basis accident environmental conditions,
- EQ equipment is properly maintained to preserve its EQ status, and
- Compliance with the EQ interface and configuration requirements.

CNSC staff measured regulatory compliance of Bruce Power with respect to the Safety and Control Area of Physical Design, specifically design governance, and system design as well as other Safety and Control Areas not reiterated for the purpose of this assessment.

Two areas of design governance were reviewed - environmental qualification assessments and barriers. Environmental qualification assessments were assessed against the requirements in CSA N290.13-05 clauses 4.6 and 5. It was concluded that Bruce Power met these regulatory requirements demonstrating qualification is in auditable form for verified EQ components/cables. In the area of EQ barriers, CNSC assessed Bruce Power against requirements in CSA



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

N290.13-05 clause 7 and Bruce Power was found compliant with the regulatory requirements based on the outputs measured. However, as per the requirements of Section 4.7 of DPT-PDE-00019, Steam Protection Barriers, Bruce Power has not demonstrated that records are kept of steam barrier inspections nor that leak testing of steam protected rooms is performed as required. Given that planned and monitored initiatives are underway for improvements this is not identified as a gap for the purpose of this assessment.

In the area of system design, the technical operability evaluation (TOE) process was assessed against the requirements of CSA N286-05 clause 6.1. It was concluded that Bruce Power met the technical operability assessment requirements. CNSC staff performed a search of the TOE database for the Emergency Coolant Injection Supply system to identify any related to EQ. No open TOEs were found; therefore, the Emergency Coolant Injection Supply (ECIS) system is operated within the safety parameters intended by the original design.

### **7.3.2. CNSC Type II Compliance Inspection Report: BRPD-AB-2015-013 Bruce A and B Generating Stations Quarterly Field Inspection Report for Q1 2015-16 [208], Q2 2015-16 [209] and Q3 2015-16 [210]**

These reports communicate the results from field inspections from Q1 (April 1-June 30, 2015); Q2 (July 1- September 30, 2015) and Q3 (October 1 –December 31, 2015). These inspections measure compliance with regulatory requirements for various licensee programs subject to observation in the field, including the SCA of Physical Design.

Physical design relates to activities that impact on the ability of SSCs to meet and maintain their design basis given new information arising over time and taking changes in the external environment into account. The specific area which was focused on included Component Design – Seismic.

In Q4 2014-15, the CNSC concluded that Bruce Power is meeting, or meeting the intent of, the requirements in regards to ensuring aspects of the seismic qualification are meeting standards. In Q3, the CNSC concluded that Bruce Power was compliant with the licence condition 5.1 based on outputs measured.

However in each quarter there were instances observed of licensee procedural non-compliance such as failure to adequately secure an object in a seismic room in accordance with BP-PROC-00500. There were no enforcement actions as a result of this aspect of the inspection.

### **7.3.3. Action Item 2015-07-6855: CNSC Type II Compliance Inspection Report : BRPD-AB-2015-004 Fukushima Verifications [211]**

The CNSC conducted a compliance inspection of Fukushima-related engineering design change packages from May 26<sup>th</sup> to 29<sup>th</sup>, 2015. The inspection focused on assessing compliance of a sample of engineering design change packages and procedures resulting from Fukushima Action Items (FAIs). Section 4.4, Physical Design relates to activities that impact the ability of SSCs to meet and maintain their design basis given new information arising over time and taking external environment changes into account.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Human Factors in design was reviewed. It was concluded that Bruce Power is controlling the performance of Human factors in design work with respect to work related to Fukushima Action Items, in accordance with regulatory requirements. However some inconsistencies and instances of non-compliance with Bruce Power procedures were observed and areas for improvement were identified. The CNSC carefully reviews any items of non-compliance and follows up to ensure all items are quickly corrected.

#### **7.3.4. CNSC Type II Compliance Inspection: Implementation of the Engineering Change Control Process [212]**


The purpose of this inspection was to verify that the Bruce Power Engineering Change Control process is in compliance with the Bruce A and B Operating Licences PROL 15.00 and 16.00. The inspection was focused on the outputs (records) generated during ECC processes for safety systems and addressed the CNSC Safety Control Areas of Management System and Physical Design. The inspection noted that the activities to control the design changes were accomplished in accordance with the current documented arrangements. Bruce Power provided records indicating that the scope of the design was properly assessed, the reason for the change was provided, the assessment of the potential impact of the change on reactor safety was performed and the stakeholders were involved in the assessment process. CNSC staff identified a number of weaknesses and deficiencies associated with the implementation of the ECC processes including replacement components. An action notice was raised by the CNSC requiring that a corrective action implementation plan for the establishment of a process that will review the quality of records in order to improve the quality of Engineering Change Control records and therefore become compliant with BP-PROC-00539. As appropriate, the corrective action process was followed for this audit. Bruce Power raised SCRs for the weaknesses and deficiencies and put corrective actions in place that will resolve the issues. The CNSC has since concluded that Action Item 1307-4427 is closed concluding that all corrective actions taken in response to the Action Notice and all recommendations have been effective [213].

#### **7.3.5. Bruce B CNSC Compliance Inspection Report : BRPD-AB-2012-011-Pressure Boundary Program Compliance at Bruce Power [214]**

As part of the CNSC compliance inspection activities, CNSC staff conducted a Type II compliance inspection of the Bruce A & B Pressure Boundary Program and Authorized Inspection Agency (AIA) Agreement. The onsite part of the inspection was carried out between 2<sup>nd</sup> and 4<sup>th</sup> of October, 2012. The main purpose of the Type II inspection was to verify that the Bruce Nuclear Generating Stations are in compliance to the Operating Licences PROL 15.00/2014 (Bruce A) and 16.00/2014 (Bruce B) Licence Conditions LC 6.1 & 6.2 and Licence Conditions Handbook Section 6.1 & 6.2 on the implementation of:

- System Code Classification, Registration and Reconciliation Procedures
- The AIA service agreement

The inspection also verified that the implementation of the Bruce A and B pressure boundary program was in compliance with the requirements of CSA N285.0-08, Update No. 1. The

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

inspection identified minor non-compliances with respect to implementation of Bruce Power's code classification procedure, specifically where information on forms was not always complete, and areas for improvement with respect to implementation of the registration and reconciliation procedure (tracking Temporary Modifications removal), and information sharing with the TSSA as part of the AIA agreement. The inspection resulted in three recommendations raised by the CNSC staff, these are managed through AR 28332140. Given that planned and monitored initiatives are underway for improvements in the efficiency, these are not identified as gaps for the purpose of this assessment.

#### 7.4. Performance Indicators

Performance indicators are defined as data that are sensitive to and/or signal changes in the performance of systems, components, or programs.

The following Engineering performance indicators are monitored under the Equipment Reliability program, BP-PROG-11.01 [126], and each System Health Report includes statistics, along with colour coding in regards to:

- TMOD (Temporary Modification) > 6 Months
- Temporary Configuration Change Backlog > 90 Days
- Modification Backlog


In addition, the web-based Plant IQ software, which is designed to automate the process of determining, documenting, and reporting the conditions of equipment at Bruce Power, provides an integrated view of the Key Performance Indicators for each unit and centre of site, where the total number in each colour is shown. Plant IQ can be accessed via the Bruce Power intranet under the Engineering tab.

In addition, the CNSC produces an annual report on the safety performance of Canada's NPPs (see discussion in Section 7.3). For 2014, the Bruce B rating for the physical design SCA was "satisfactory".

## 8. Summary and Conclusions

The overall objectives of the Bruce B PSR are to conduct a review of Bruce B against modern codes and standards and international safety expectations, and to provide input to a practicable set of improvements to be conducted during the MCR in Units 5 to 8, as well as U0B, and during asset management activities to support ongoing operation of all four units, that will enhance safety to support long term operation. The specific objective of the review of this Safety Factor is to determine the adequacy of the design of the nuclear power plant and its documentation by assessment against modern national and international standards and practices. This specific objective has been met by the completion of the review tasks specific to Plant Design.

Table 8 summarizes the key issues arising from the Integrated Safety Review of Safety Factor 1.


	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

**Table 8: Key Issues**

Issue Number	Gap Description	Source(s)
SF1-1	<p>Safety Objectives and Concepts</p> <p>Event classification scheme of plant states (AOOs, DBAs, BDBAs and DEC's) is not applied in the current safety analysis.</p>	<p>Sections 5.3.8, 5.3.15 and 5.6</p> <p>Micro-gaps against requirement clauses:</p> <p>REGDOC-2.5.2 - Clause 4.2.1  REGDOC-2.5.2 - Clause 4.2.3 (Gap 1)  REGDOC-2.5.2 - Clause 6.1  REGDOC-2.5.2 - Clause 6.4  REGDOC-2.5.2 - Clause 7.3  REGDOC-2.5.2 - Clause 7.3.2  REGDOC-2.5.2 - Clause 7.3.4  REGDOC-2.5.2 - Clause 7.4  REGDOC-2.5.2 - Clause 7.4.1  REGDOC-2.5.2 - Clause 7.5  REGDOC-2.5.2 - Clause 7.13.1 (Gap 2)  REGDOC-2.5.2 - Clause 7.15.1  REGDOC-2.5.2 - Clause 8.1  REGDOC-2.5.2 - Clause 8.1.1  REGDOC-2.5.2 - Clause 8.3.2  REGDOC-2.5.2 - Clause 8.4.1  REGDOC-2.5.2 - Clause 9.1 (Gap 2)  REGDOC-2.5.2 - Clause 9.2  CSA N290.0 - Clause 4.2  CSA N290.0 - Clause 4.12.4  CSA N290.0 - Clause 4.12.5</p>
SF1-2	<p>Safety Goals</p> <p>Although the results of Bruce B PRA meet the safety goal limits set up for Bruce B PRAs, they do not meet the more stringent quantitative safety goal targets set up in the requirement clause. The aggregate SCDF and LRF obtained by summation across all available PRA types are higher than the safety goal targets set forth in the requirement Clause 4.2.2 of CNSC REGDOC-2.5.2.</p>	<p>Sections 5.3.15 and 5.6</p> <p>Micro-gaps against requirement clauses:</p> <p>REGDOC-2.5.2 - Clause 4.2.2</p>
SF1-3	<p>Initiating Events</p> <p>A systematic approach to identifying a comprehensive set of postulated initiating internal and external events, including common-cause initiating events, has not been consistently applied.</p>	<p>Sections 5.3.11, 5.3.12, 5.3.15 and 5.6</p> <p>Micro-gaps against requirement clauses:</p> <p>REGDOC-2.5.2 - Clause 4.2.3 (Gap 2)  REGDOC-2.5.2 - Clause 6.1.1  REGDOC-2.5.2 - Clause 6.6.1  REGDOC-2.5.2 - Clause 7.6.2 (Gap 2)  CSA N290.3 - Clause 10.1  CSA N290.11 - Clause 5.2.2.10</p>

 <div style="font-size: small;">Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Issue Number	Gap Description	Source(s)
SF1-4	<p>Legacy Design Analysis</p> <p>Many of the original design analyses were produced using tools that predated N286.7-99.</p>	<p>Section 5.3.15 and 5.6</p> <p>Micro-gaps against requirement clauses:</p> <p>REGDOC-2.5.2 - Clause 5.3</p>
SF1-5	<p>Design for Reliability</p> <p>Reliability requirements for some SSCs do not meet the requirements and/or safety goals.</p>	<p>Sections 5.3.8, 5.3.15 and 5.7</p> <p>Micro-gaps against requirement clauses:</p> <p>REGDOC-2.5.2 - Clause 7.6.2 (Gap 1)</p> <p>CSA N290.0 - Clause 4.7</p> <p>CSA N290.0 - Clause 4.11.2.13</p>
SF1-6	<p>Systematic Analysis of Overpressure Protection of pressure-retaining SSCs</p> <p>There is not a systematic analysis of the control system capability to cope with AOOs.</p>	<p>Sections 5.2 and 5.3.15</p> <p>Micro-gaps against requirement clauses:</p> <p>REGDOC-2.5.2 - Clause 7.7</p>
SF1-7	<p>Operator Emergency Response</p> <p>Requirement related to sufficiency of staff credited with performing contingency activities on outage heat sinks has not been demonstrated to be met.</p>	<p>Sections 5.3.12 and 5.6</p> <p>Micro-gaps against requirement clauses:</p> <p>CSA N290.11 – Clause 5.2.2.4</p>
SF1-8	<p>Guaranteed Shutdown State (GSS)</p> <p>Current design documentation does not reflect required functional test frequency for the equipment associated with GSS.</p>	<p>Sections 5.3.15 and 5.4</p> <p>Micro-gaps against guidance clauses:</p> <p>REGDOC-2.5.2 - Clause 7.11</p>
SF1-9	<p>Timing of Operator Actions</p> <p>The current safety analysis does not meet the timing requirements of operator actions of 30 min and 1 h. In addition, the current design documentation does not reflect the requirement for long-term services for emergency support systems.</p>	<p>Sections 5.3.9, 5.3.15, 5.4, and 5.6</p> <p>Micro-gaps against requirement clauses:</p> <p>REGDOC-2.5.2 - Clause 7.10</p> <p>REGDOC-2.5.2 - Clause 8.10.4</p> <p>CSA N290.1 – Clause 4.3.1.4</p>

 <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Issue Number	Gap Description	Source(s)
SF1-10	<p>Lifting and handling of large loads</p> <p>Identification and justification of traversing routes for large loads, and analysis to justify safe operations when considering the drop of large loads does not exist in current Bruce Power design documentation.</p>	<p>Sections 5.3.15 and 5.4</p> <p>Micro-gaps against requirement clauses:</p> <p>REGDOC-2.5.2 - Clause 7.15.3 (Gap 1, Gap 2)</p>
SF1-11	<p>Design Extension Conditions</p> <p>The current design documentation does not explicitly consider the load conditions on containment during DEC's.</p>	<p>Sections 5.3.15 and 5.4</p> <p>Micro-gaps against requirement clauses:</p> <p>REGDOC-2.5.2 - Clause 8.6.12</p>
SF1-12	<p>Electrical Power Systems</p> <p>Design limits are not specified for electromagnetic emissions.</p> <p>The design manuals and OSR do not explicitly state that the SSCs employed are qualified for electromagnetic noise disturbances and mechanical vibrations.</p> <p>The capacity requirements and design provisions for periodic testing are not sufficiently documented.</p> <p>The existing safety analysis does not consider events with station blackout.</p>	<p>Sections 5.3.9 5.3.15 and 5.6</p> <p>Micro-gaps against requirement clauses:</p> <p>REGDOC-2.5.2 - Clause 8.9 REGDOC-2.5.2 - Clause 8.9.2 REGDOC-2.5.2 - Clause 8.9.3 CSA N290.1 - Clause 4.7.2</p>
SF1-13	<p>Fuel Handling and Storage</p> <p>The requirement for sufficient space to accommodate the entire reactor core inventory at all times is not reflected in the design and operating documentation. The radioactive sources other than the reactor core, such as the spent fuel pool and fuel handling systems, are not addressed in Part 3 of the Safety Report.</p>	<p>Sections 5.3.15, 5.4 and 5.8</p> <p>Micro-gaps against requirement clauses:</p> <p>REGDOC-2.5.2 - Clause 8.12.2 REGDOC-2.5.2 - Clause 9.1 (Gap 1)</p>



 <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Issue Number	Gap Description	Source(s)
SF1-14	<p>Radiation and Environmental Protection and Mitigation</p> <p>The existing design documentation does not describe all necessary suitable provisions to minimize exposure, contamination, and radiological releases to the environment.</p>	<p>Sections 5.2, 5.3.10, 5.3.15 and 5.4</p> <p>Micro-gaps against requirement clauses:</p> <p>REGDOC-2.5.2 - Clause 8.13.1 (Gap 1)  REGDOC-2.5.2 - Clause 8.13.3  CSA N290.2 - Clause 5.12.5</p> <p>Micro-gaps against guidance clauses:</p> <p>REGDOC-2.5.2 - Clause 8.13  REGDOC-2.5.2 - Clause 8.13.1 (Gap 2)  REGDOC-2.5.2 - Clause 10.1</p>
SF1-15	<p>Seismic Instrumentation</p> <p>Earthquake monitoring instrumentation is not installed in the plant.</p>	<p>Sections 5.3.3 and 5.3.15</p> <p>Micro-gaps against requirement clauses:</p> <p>REGDOC-2.5.2 - Clause 7.13  CSA N289.1 – Clauses 6.5.6.3 and 6.5.6.4</p>
SF1-16	<p>Seismic Qualification Documentation</p> <p>Governing and implementing documents for seismic qualification do not consistently indicate the application of CSA N289 series. The more recent site investigations documented in the Probabilistic Seismic Hazard Assessment are not reflected in the design documentation.</p>	<p>Sections 5.3.3, 5.3.15, and 5.4</p> <p>Micro-gaps against requirement clauses:</p> <p>REGDOC-2.5.2 - Clause 7.13.1 (Gap 1)</p> <p>Micro-gaps against guidance clauses:</p> <p>CSA N289.1 – Clause 3.1</p>
SF1-17	<p>Revision Changes ASME Section III</p> <p>There is no evidence that pressure boundary design governance documentation and safety margins has been reviewed for impact of changes in Stress Limits, Bolting <math>S_m</math> Values, Stress Indices for Straight Pipe, Branch Connections and Load Limit values.</p>	<p>Section 5.3.17 and 5.4</p> <p>Micro-gaps against requirement clauses:</p> <p>ASME Section III</p>



 <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Issue Number	Gap Description	Source(s)
SF1-18	<p>Revision Changes to Pressure Boundary Design Requirements</p> <p>Pressure boundary design governance documentation and safety margins have not been reviewed for impact of new requirements introduced with the latest revisions of CSA N285.0 and changes in ASME Section VIII.</p>	<p>Sections 5.3, 5.3.17 and 5.4</p> <p>Micro-gaps against requirement clauses:</p> <p>ASME Section VIII</p>
SF1-19	<p>Barriers for Containment Penetrations</p> <p>The safety significance of identified differences between the current design documentation and the requirements of CSA N290.3-11, Annex A has not been assessed.</p>	<p>Sections 5.3.11 and 5.4</p> <p>Micro-gaps against requirement clauses:</p> <p>CSA N290.3 Clause A.2.3, CSA N290.3 Clause A.2.5, CSA N290.3 Clause A.3.1 CSA N290.3 Clause A.3.4</p>
SF1-20	<p>Special Safety System Requirements</p> <p>There are documented exceptions for design of special safety system components such that the most likely failure modes are not in the failsafe direction.</p> <p>There remains some instances where the failure mode is unsafe and the operator must monitor or test SDS availability.</p> <p>Bruce B design includes sharing of special safety systems without justification that such sharing contributed to enhanced safety as required by CNSC REGDOC-2.5.2 clause 7.6.5.2.</p>	<p>Sections 5.3.8, 5.3.9, 5.3.15 and 5.4</p> <p>Micro-gaps against requirement clauses:</p> <p>REGDOC-2.5.2 - Clause 7.6.3 REGDOC-2.5.2 – Clause 7.6.5.2 CSA N290.0 - Clause 4.8 CSA N290.1 – Clause 4.2.6</p>
SF1-21	<p>Pressure Boundary Quality Assurance Program Deficiencies</p> <p>Implementation of certain elements of BP-PROG-00.04 were found ineffective. Some program elements do not meet implementing process pressure boundary quality assurance requirements.</p>	<p>Sections 4.1, 4.1.1, 5.4, 7.2.3, 7.2.4, and 7.2.5</p>


 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Issue Number	Gap Description	Source(s)
SF1-22	<b>Emergency Support Facilities</b> The Bruce B design does not provide an onsite emergency facility (or facilities) that are separate from the plant control rooms which include a Safety Parameter Display System (SPDS) similar to those in the MCR and the SCA.	Sections 5.2 and 5.3.15 Micro-gaps against requirement clauses: REGDOC-2.5.2 - Clause 8.10.3
SF1-23	<b>Emergency Heat Removal System</b> Since Bruce B emergency heat removal function is provided by more than one system; it cannot be confirmed that the same function will be available during DEC's, if required.	Sections 5.3.15 and 5.4 Micro-gaps against requirement clauses: REGDOC-2.5.2 - Clause 8.8 (Gap 1, Gap 2)
SF1-24	<b>Tracking Licence Concessions</b> Bruce Power should establish a controlled, centralized and accessible company database available to support design activities	Sections 5.3.16 and 5.4 Micro-gaps against requirement clauses: ANSI/NIRMA CM 1.0-2007 – Section 3.2


The overall conclusion is that, with the exceptions noted in Table 8, Bruce Power meet the requirements of the Plant Design Safety Factor.

## 9. References

- [1] NK21-CORR-00531-12136/NK29-CORR-00531-12546/E-DOC 4723908 , Nuclear Power Reactor Operating Licence, Bruce Nuclear Generating Stations A and B, PROL 18.00/2020, Canadian Nuclear Safety Commission, May 27, 2015.
- [2] NK21-CORR-00531-12135/NK29-CORR-00531-12545/E-DOC 4659316, Licence Conditions Handbook, LCH-BNGS-R000, Bruce Nuclear Generating Station A and Bruce Nuclear Generating Station B Nuclear Reactor Operating Licence, PROL 18.00/2020 (Effective: June 1, 2015), Canadian Nuclear Safety Commission, May 27, 2015.
- [3] CNSC REGDOC-2.3.3, Operating Performance: Periodic Safety Reviews, CNSC, April 2015.
- [4] BP-PROC-01024-R000, Periodic Safety Reviews, Bruce Power, December 2015.
- [5] NK29-CORR-00531-12932, Bruce B Periodic Safety Review Basis Document, Bruce Power Letter, F. Saunders to K. Lafrenière, January 25, 2016.

 <b>candesco</b> <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- [6] NK21-CORR-00531-11005/NK29-CORR-00531-11397, Submission of Safety Basis Report, Bruce Power Letter, F. Saunders to R. Lojk, December 30, 2013.
- [7] NK21-CORR-00531-00514, Bruce A: CNSC Approval to Restart Units 3 and 4 and Application to Amend PROL 15.01/2003, Bruce Power Letter, F. Saunders to J.H.M. Douglas, November 16, 2001.
- [8] NK21-CORR-00531-04636, Bruce A Units 1 and 2 Return to Service: Systematic Review of Safety – Basis, Bruce Power Letter, F. Saunders to D.A. Desjardins, December 22, 2006.
- [9] NK21-CORR-00531-04059, Bruce A Refurbishment for Life Extension – Systematic Review of Safety: Plant Design, Bruce Power Letter, F. Saunders to P. Webster, March 30, 2006.
- [10] NK21-CORR-00531-04339, Bruce A Units 1 and 2 Return to Service – Systematic Review of Safety, Bruce Power Letter, F. Saunders to P. Webster, July 31, 2006.
- [11] NK21-CORR-00531-05749, Bruce A Refurbishment for Life Extension and Continued Operation of Units 3 and 4 – Integrated Safety Review Basis, F. Saunders to P. Elder, February 29, 2008.
- [12] NK21-CORR-00531-05976, Bruce A Units 3 and 4 Refurbishment for Life Extension and Continued Operations: ISR Safety Factor Reports, Bruce Power Letter, F. Saunders to P. Elder, June 2, 2008.
- [13] NK21-CORR-00531-06596, Bruce A Units 3 and 4 Refurbishment for Life Extension and Continued Operation: ISR Safety Factor Reports 1, 2, 3 and 4, Bruce Power Letter, F. Saunders to K. Lafrenière, December 18, 2008.
- [14] NK21-CORR-00531-06076, Bruce A Units 3 and 4 Refurbishment for Life Extension and Continued Operation: ISR Safety Factor Reports 5, 6, and 7, Bruce Power Letter, F. Saunders to P. Elder, July 22, 2008.
- [15] NK21-REP-03600-00025-R001, Bruce NGS A Units 3 and 4 Global Assessment Report and Integrated Implementation Plan, May 29, 2009.
- [16] NK21-CORR-00531-11617, Integrated Safety Review for Bruce A, Bruce Power Letter, F. Saunders to K. Lafrenière, including enclosure K-421231-00010-R00, Candesco Report, October 27, 2014.
- [17] NK21-CORR-00531-12269, Bruce A Integrated Safety Review – Safety Factor Reports, Bruce Power Letter, F. Saunders to K. Lafrenière, August 27, 2015.
- [18] NK21-CORR-00531-10576/NK29-CORR-00531-10975, Application Requirements for Renewal of Power Reactor Operating Licences for Bruce Nuclear Generating Stations A and B, Bruce Power Letter, F. Saunders to R. Lojk, July 17, 2013.
- [19] NK29-CORR-00531-11252, Application for the Renewal of the Power Reactor Operating Licence for Bruce Nuclear Generating Station B, Letter, F. Saunders to M. Leblanc, October 31, 2013.
- [20] NK21-CORR-00531-11711/NK29-CORR-00531-12101, Bruce A and Bruce B Licence Renewal – Supplemental Update, F. Saunders to M. Leblanc, November 27, 2014.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- [21] NK21-CORR-00531-11715/NK29-CORR-00531-12105, Bruce Power: Requests and Supplemental Information for Licence Renewal, F. Saunders to M. Leblanc, November 28, 2014.
- [22] Nuclear Safety and Control Act, 1997, c. 9, N-28.3, Assented to March 20, 1997.
- [23] CNSC REGDOC-2.4.2, Probabilistic Safety Assessment for Nuclear Power Plants, May 2014.
- [24] CNSC RD-327, Nuclear Criticality Safety, December 2010.
- [25] CNSC G-278, Human Factors Verification and Validation Plans, June 2003.
- [26] CAN/CSA N285.0-12, General Requirements for Pressure-Retaining Systems and Components in CANDU Nuclear Power Plants, 2012 (Update 1 – 2013; Update 2 – 2014).
- [27] CAN/CSA N286-05, Management System Requirements for Nuclear Power Plants, CSA, February 2005, (Update No.2, 2010), R2010.
- [28] CAN/CSA N286-12, Management System Requirements for Nuclear Facilities, CSA, 2012.
- [29] CAN/CSA N286.7-99, Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants, March 1999 (Reaffirmed 2012).
- [30] CAN/CSA N288.4-10, Environmental Monitoring Programs at Class I Nuclear Facilities and Uranium Mines and Mills, 2010 (R2015).
- [31] CAN/CSA N290.13, Environmental Qualification of Equipment for CANDU Nuclear Power Plants, 2005 (Reaffirmed 2010).
- [32] CAN/CSA N290.15-10, Requirements for the Safe Operating Envelope of Nuclear Power Plants, 2010 (Reaffirmed 2015).
- [33] CAN/CSA N293-12, Fire Protection for Nuclear Power Plants, 2012.
- [34] NK21-CORR-00531-12443/NK29-CORR-00531-12854, Bruce A and Bruce B: Regulatory Document RD-327, Compliance Update, October 28, 2015.
- [35] NK21-CORR-00531-11494/NK29-CORR-00531-11881, Response to Bruce Power letter, CSA N286-12 “Management system requirements for nuclear facilities”, Action Item 1307-4697, CNSC Letter, K. Lafrenière to F. Saunders, July 24, 2014.
- [36] NK21-CORR-00531-11189/NK29-CORR-00531-11593, Action Item 1307-4697: CSA N286-12 Management System Requirements for Nuclear Facilities, Bruce Power Letter, F. Saunders to K. Lafrenière, May 16, 2014.
- [37] NK21-CORR-00531-11563/NK29-CORR-00531-11946, CSA N286-12 - Management System Requirements for Nuclear Facilities, Action Item 1307-4697, Bruce Power Letter, F. Saunders to K. Lafrenière, September 9, 2014.
- [38] NK21-CORR-00531-12570/NK29-CORR-00531-12996, Action Item 1307-4697: CSA N286-12 - Management Systems Requirements for Nuclear Facilities, Bruce Power Letter, F. Saunders to K. Lafrenière, January 29, 2016.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


- [39] CNSC G-149, Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors, October 2000.
- [40] BP-PROC-00326-R004, Software Management, Bruce Power, November 6, 2012.
- [41] DIV-ENG-00006-R000, Engineering Analysis Software, March 21, 2006.
- [42] COG-02-901, Principles and Guidelines for the Definition, Implementation and Maintenance of the Safe Operating Envelope at CANDU Power Plants in Canada, March 2003.
- [43] NK21-03600/NK29-03600, Documentation Requirements in Support of CSA N290.15 Compliance, Bruce Power Memorandum, A. Maksymyk to A. Ikeda, September 30, 2015.
- [44] NK21-CORR-00531-12829, Action Item 2016-07-7836: SOE Compliance Gaps – Event Report B-2015-28529845, Bruce Power Letter, F. Saunders to K. Lafrenière, June 7, 2016.
- [45] B-REP-00701-29NOV2013-059, Assessment of Fire Protection at Bruce Power, November 29, 2013.
- [46] CNSC R-10, The Use of Two Shutdown Systems in Reactors, Canadian Nuclear Safety Commission, January 11, 1977.
- [47] CNSC R-77, Overpressure Protection Requirements for Primary Heat Transport Systems in CANDU Power Reactors Fitted with Two Shutdown Systems, Canadian Nuclear Safety Commission, October 20, 1987.
- [48] CNSC G-276, Human Factors Engineering Program Plans, June 2003.
- [49] CNSC RD-346, Site Evaluation for New Nuclear Power Plants, November 2008.
- [50] CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants, May 2014.
- [51] 13-M25, Regulatory Framework Program Update, CNSC, May 16, 2013.
- [52] B-REP-09701-16MAY2016, Bruce NGS A and Bruce NGS B Compliance to Overpressure Protection Requirements of CNSC Regulatory Document R-77, May 16, 2016.
- [53] NK29-SR-01320-00002-R005, Bruce B Safety Report, Part 3: Accident Analysis, Bruce Power, November 2011.
- [54] IAEA NS-R-3, Site Evaluation for Nuclear Installations, International Atomic Energy Agency, Safety Requirements, November 2003.
- [55] CAN/CSA B51-14, Boiler, Pressure Vessel, and Pressure Piping Code, 2014.
- [56] CAN/CSA N287.1-14, General Requirements for Concrete Containment Structures for Nuclear Power Plants, February 2014.
- [57] CAN/CSA N287.2-08, Material Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, March 2008 (Reaffirmed 2013).
- [58] CAN/CSA N287.3-14, Design Requirements for Concrete Containment Structures for Nuclear Power Plants, February 2014.



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- [59] CAN/CSA N287.4-09, Construction, Fabrication, and Installation Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, October 2009.
- [60] CAN/CSA N287.5-11, Examination and Testing Requirements for Concrete Containment Structures for Nuclear Power Plants, May 2011.
- [61] CAN/CSA N287.6-11, Pre-Operational Proof and Leakage Rate Testing Requirements for Concrete Containment Structures for Nuclear Power Plants, May 2011.
- [62] CAN/CSA N289.1-08, General Requirements for Seismic Design and Qualification for CANDU Nuclear Power Plants, September 2008, (R2013).
- [63] CAN/CSA N289.2-10, Ground Motion Determination for Seismic Qualification of Nuclear Power Plants, May 2010, (R2015).
- [64] CAN/CSA N289.3-10, Design Procedures for Seismic Qualification of Nuclear Power Plants, May 2010, (R2015).
- [65] CAN/CSA N289.4-12, Testing Procedures for Seismic Qualification of Nuclear Power Plant Structures, Systems, and Components, August 2012.
- [66] CAN/CSA N289.5-12, Seismic Instrumentation Requirements for Nuclear Power Plants and Nuclear Facilities, August 2012.
- [67] CAN/CSA N290.0-11, General Requirements for Safety Systems of Nuclear Power Plants, October 2011.
- [68] CAN/CSA N290.1-13, Requirements for the Shutdown Systems of Nuclear Power Plants, December 2013.
- [69] CSA Group N290.2-11, Requirements for Emergency Core Cooling Systems of Nuclear Power Plants, October 2011.
- [70] CAN/CSA N290.3-11, Requirements for the Containment System of Nuclear Power Plants, October 2011.
- [71] CAN/CSA N290.4-11, Requirements for Reactor Control Systems of Nuclear Power Plants, October 2011.
- [72] CAN/CSA N290.5-06, Requirements for Electrical Power and Instrument Air Systems of CANDU Nuclear Power Plants, 2006 (Reaffirmed 2011).
- [73] CAN/CSA N290.6-09, Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of an Accident, March 2009 (Reaffirmed 2014).
- [74] CAN/CSA N290.11-13, Requirements for Reactor Heat Removal Capability During Outage of Nuclear Power Plants, December 2013.
- [75] CAN/CSA N290.12-14, Human Factors in Design for Nuclear Power Plants, December 2014.
- [76] CAN/CSA N291-15, Requirements for Safety-Related Structures for Nuclear Power Plants, November 2015.
- [77] NK21-CORR-00531-11801/NK29-CORR-00531-12195, Bruce Power Progress Report No.6 on CNSC Action Plan – Fukushima Action Items, January 30, 2015.




 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


- [78] NK21-CORR-00531-12554/NK29-CORR-00531-12979, Bruce Power Progress Report No. 8 on CNSC Action Plan – Fukushima Action Items, February 4, 2016.
- [79] NK29-CORR-00531-12650, Bruce B 2015: Containment and Vacuum Building Pressure Test Final Results, July 31, 2015.
- [80] ANSI/NIRMA CM 1.0 – 2007, American National Standard for Guidelines for Configuration Management of Nuclear Facilities, August 2007.
- [81] ASME BPVC Section III, Rules for Construction of Nuclear Power Plant Components.
- [82] ASME BPVC Section VIII, Design and Fabrication of Pressure Vessels, 2015.
- [83] ASME B31.1-2014, Power Piping, ASME Code for Pressure Piping, 2015.
- [84] IAEA SSG-25, Periodic Safety Review of Nuclear Power Plants, 2013.
- [85] NFPA-805, Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants, 2015 Edition.
- [86] Darlington-DG-38-03650-1, Purpose and Application of Nuclear Safety Design Guides.
- [87] Darlington-DG-38-03650-2A, Common Mode Incidents – Overview and Design Requirements.
- [88] Darlington-DG-38-03650-2B, Common Mode Incidents – Seismic Design.
- [89] Darlington-DG-38-03650-3, Limiting Consequential Damage of Postulated Pipe Ruptures.
- [90] Darlington-DG-38-03650-4, Shutdown Systems.
- [91] Darlington-DG-38-03650-5, Emergency Coolant Injection.
- [92] Darlington-DG-38-03650-6, Containment.
- [93] Darlington-DG-38-03650-7, Extensions of the Containment Envelope.
- [94] Darlington-DG-38-03650-8, Environmental Qualification of Safety Related Equipment.
- [95] Darlington-DG-38-03650-9, Safety Assessments.
- [96] National Building Code of Canada, Government of Canada, 2015.
- [97] National Fire Code of Canada, Government of Canada, 2015.
- [98] NK21-CORR-00531-05728, Bruce 1&2 Integrated Safety Review – Category 2 Issue #4, Bruce Power Letter, F. Saunders to P. Elder, February 29, 2008.
- [99] NK29-REP-71400-00002-R003, Bruce Nuclear Generating Station “B” - Fire Protection Code Compliance Review, December 2012.
- [100] BP-MSM-1-R012, Management System Manual, Bruce Power, June 23, 2014.
- [101] BP-MSM-1 Sheet 0001-R020, MSM-Bruce Power Program Matrix, Bruce Power, January 23, 2015.
- [102] BP-MSM-1 Sheet 0003-R005, MSM-List of Applicable Governing Acts, Regulations, Codes & Standards, Bruce Power, September 30, 2014.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- [103] BP-PROG-01.02-R009, Bruce Power Management System (BPMS) Management, Bruce Power, December 15, 2015.
- [104] BP-PROG-00.04-R022, Pressure Boundary Quality Assurance Program, Bruce Power, May 27, 2015.
- [105] BP-PROC-00915-R000, Pressure Boundary Quality Assurance Program Oversight, Bruce Power, April 3, 2013.
- [106] BP-PROG-10.01-R009, Plant Design Basis Management, Bruce Power, December 4, 2014.
- [107] BP-PROC-00335-R007, Design Management, Bruce Power, July 30, 2015.
- [108] BP-PROC-00363-R003, Nuclear Safety Assessment, Bruce Power, January 24, 2013.
- [109] DIV-ENG-00009-R005, Design Authority, Bruce Power, November 1, 2013.
- [110] BP-PROC-00582-R003, Engineering Fundamentals, Bruce Power, July 25, 2014.
- [111] BP-PROC-00502-R002, Resolution of Differing Professional Opinions, Bruce Power, October 12, 2010.
- [112] BP-PROG-10.02-R010, Engineering Change Control, Bruce Power, December 15, 2015.
- [113] BP-PROC-00743-R003, Site Services Engineering Change Control, Bruce Power, November 28, 2012.
- [114] BP-PROC-00542-R007, Configuration Information Change, Bruce Power, November 24, 2015.
- [115] BP-PROC-00539-R016, Design Change Package, Bruce Power, June 23, 2015.
- [116] BP-PROC-00877-R000, Modification Installation Quality Assurance, Bruce Power, October 29, 2012.
- [117] BP-PROC-00615-R001, Commissioning Modifications and Projects, Bruce Power, September 20, 2013.
- [118] BP-PROG-10.03-R006, Configuration Management, Bruce Power, February 5, 2015.
- [119] BP-PROC-00470-R004, Configuration Management Program Oversight and Trending, Bruce Power, October 1, 2012.
- [120] BP-PROC-00584-R008, PassPort Equipment Data Management, Bruce Power, October 19, 2015.
- [121] BP-PROC-00638-R012, Temporary Configuration Change Management, Bruce Power, May 7, 2014.
- [122] BP-PROC-00647-R002, PassPort Permit Request Processing, Bruce Power, September 11, 2013.
- [123] BP-PROC-00786-R003, Margin Management, Bruce Power, August 5, 2014.
- [124] BP-PROC-00898-R000, Equipment Codes, Bruce Power, June 19, 2013.
- [125] SEC-DO-00001-R009, Drafting Office Work Management, November 29, 2012.

 <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- [126] BP-PROG-11.01-R005, Equipment Reliability, Bruce Power, December 16, 2015.
- [127] BP-PROC-00778-R002, Scoping and Identification of Critical SSCs, September 3, 2015.
- [128] DPT-RS-00012-R001, Systems Important to Safety (SIS) Decision Methodology, Bruce Power, September 24, 2013.
- [129] BP-PROG-03.01-R016, Document Management, Bruce Power, August 31, 2015.
- [130] BP-PROC-00169-R002, Safety-Related System List, Bruce Power, September 28, 2007.
- [131] NK21-CORR-00531-12286/NK29-CORR-00531-12716, Roadmap of the Pressure Boundary Quality Assurance (PBQA) Program, Email, J. Boyadjian to K. Lafrenière, August 21, 2015.
- [132] BP-PROG-00.04-R020 (Superseded), Pressure Boundary Quality Assurance Program, Bruce Power, March 21, 2014.
- [133] BP-PROC-00078-R008, Quality Program Manual for Testing and Repair of Pressure Relief Valves, Bruce Power, May 19, 2015.
- [134] BP-PROC-00137-R015, Focus Area Self-Assessment, Bruce Power, March 10, 2015.
- [135] BP-PROC-00412-R006, Trend Identification and Reporting of SCRs, Bruce Power, August 18, 2014.
- [136] BP-OPP-00001-R019, Operating Policies and Principles-Bruce B, Bruce Power, July 15, 2015.
- [137] BP-OPP-00002-R013, Operating Policies and Principles- Bruce A, Bruce Power, March 31, 2014.
- [138] CAN/CSA N286.0-92, Overall Quality Assurance Program Requirements for Nuclear Power Plants, September 1992 (Reaffirmed 2003).
- [139] BP-PROC-00268-R007, Safety System Testing (SST) Program Procedure, Bruce Power, August 28, 2015.
- [140] DIV-ENG-00017-R002, System and Item Classification, Bruce Power, September 3, 2015.
- [141] SEC-EQD-00022-R003, Development of the Environmental Qualification Lists (EQL), July 23, 2013.
- [142] DPT-PDE-00017-R005, Bruce Power Seismic Qualification Standard, Bruce Power, July 4, 2012.
- [143] NK29-DG-03650-002, Seismic Qualification of Safety Related Systems, Units 05678, R007, June 2012.
- [144] DPT-PDE-00028-R004, Fire Safe Shutdown Analysis Maintenance, Bruce Power, October 28, 2013.
- [145] NK29-REP-71400-00003-R003, Fire Safe Shutdown Analysis, Bruce-B Nuclear Generating Station, December 2012.
- [146] DPT-NSAS-00012-R004, Preparation and Maintenance of Operational Safety Requirements, Bruce Power, October 28, 2014.


 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- [147] B-REP-00701-21OCT2013-058, Assessment of Systems Important to Safety for the Safety & Licensing Portion of the Nuclear Asset Management Program, Bruce Power, October 2013.
- [148] BP-PROC-00261-R005, Environmental Qualification, Bruce Power, November 7, 2012.
- [149] BP-PROG-11.04-R006, Plant Maintenance, Bruce Power, November 27, 2013.
- [150] NK29-CORR-00531-12884, Action Item 091413, Bruce B Legacy Registration Project Update, Bruce Power Letter, F. Saunders to K. Lafrenière, November 23, 2015.
- [151] DIV-ENG-00018-R003, Design Registration and Reconciliation, November 24, 2015.
- [152] NK29-DM-34200-001, Negative Pressure Containment System, Bruce Nuclear Generating Station Design Manual, July 1981.
- [153] CSA Standard, N287.3-1978, Design Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, July 1978.
- [154] CAN/CSA A23.3-14, Design of Concrete Structures, June 2014. (CSA N287)
- [155] NK29-SR-01320-00001-R005, Bruce B Safety Report, Bruce Power, August 31, 2012.
- [156] NK21-CALC-20091-00001-R001, Review Level Earthquake, Bruce Power, November 28, 2001.
- [157] NK29-03500.8, Bruce B Nuclear Generating Station Seismic Hazard Assessment (AMEC report B1062/RP/002 R01) Bruce Power, December 9, 2011.
- [158] NK29-DG-29-01040-1 R00, Earthquake Design Requirements for CANDU Nuclear Power Plants, Atomic Energy of Canada Limited, June 1980.
- [159] NK21-CORR-00531-12059/NK29-CORR-00531-12453, Interpretation of Clause 4.2 of CSA Standard N289.3-10, Bruce Power, April 15, 2015.
- [160] NK21-CORR-00531-10753/NK29-CORR-00531-11136, External Flood Clarifications, CNSC Letter, R. Lojk to F. Saunders, September 4, 2013.
- [161] NK21-CORR-00531-04340, Bruce A Units 1 and 2 Return to Service – Review Against Design Standards, Bruce Power Letter, F.Saunders to P.Webster, July 31, 2006.
- [162] NK21-CORR-00531-11339/NK29-CORR-00531-11742, 2014 Annual COG Research and Development Reporting, Bruce Power Letter, F. Saunders to K. Lafrenière, June 16, 2014.
- [163] BP-PROC-00068-R023, Controlled Document Life Cycle Management, Bruce Power, December 11, 2015.
- [164] BP-PROC-00098-R015, Records Management, Bruce Power, November 27, 2014.
- [165] NK29-DG-29-03650-001-R003, Bruce 'B' Generating Station, Purpose and Application of Safety System Design Guides, November 1985.
- [166] DPT-RS-00015-R000, Safe Operating Envelope Gap Assessment, Bruce Power, May 31, 2011.
- [167] NK29-CORR-00531-10306, Bruce B: Pilot Type I Inspection of the Bruce Power Safe Operating Envelope, CNSC Letter, R. Lojk to F. Saunders, September 5, 2012.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- [168] NK29-CORR-00531-10884, Response to the CNSC Inspection of the Safe Operating Envelope Implementation Program at Bruce B, Bruce Power Letter, F. Saunders to R. Lojk, June 6, 2013.
- [169] AR 28404125, Complete Admin Updates: Implementation of CSA N290.15-11, completed on February 23, 2016.
- [170] BP-PROG-12.02-R006, Chemistry Management, Bruce Power, June 8, 2015.
- [171] BP-PROG-12.03-R003, Fuel Management, Bruce Power, November 20, 2008.
- [172] FORM-10700-R021, Design Scoping Checklist, Bruce Power.
- [173] FORM-12608-R002, Design Review of Design Change Notice, Bruce Power.
- [174] FORM-13200-R006, Design Products Challenge Board Checklist, Bruce Power.
- [175] DPT-PDE-00006-R013, Design Plan, Bruce Power, June 26, 2014.
- [176] CNSC REGDOC-3.1.1, Reporting Requirements for Nuclear Power Plants, CNSC, May 2014.
- [177] NK21-CORR-00531-10943/NK29-CORR-00531-11325, Safety Analysis in Support of Operation of Bruce A and B to 2019, Bruce Power Letter, F. Saunders to R. Lojk, December 12, 2013.
- [178] NK29-63720/63780 P NSAS, Bruce NGS B: Assessment of NOP Trip Coverage at 2019 Aged Core Conditions, August 16, 2013.
- [179] NK21-CORR-00531-10943/NK29-CORR-00531-11325, Safety Analysis in Support of Operation of Bruce A and Bruce B to 2019, Bruce Power Letter, F. Saunders to R. Lojk, December 12, 2013, Attachment 2: NK29-03507.1 P NSAS, Bruce B Small LOCA Analysis in Support of Operation to 2019, November 28, 2013.
- [180] NK21-CORR-00531-10943/NK29-CORR-00531-11325, Safety Analysis in Support of Operation of Bruce A and Bruce B to 2019, Bruce Power Letter, F. Saunders to R. Lojk, December 12, 2013, Attachment 1: NK29-03507.1 P NSAS, Bruce NGS B Loss of Flow Analysis in Support of Operation to 10550 EFPD, December 11, 2013.
- [181] NK21-CORR-00531-10943/NK29-CORR-00531-11325, Safety Analysis in Support of Operation of Bruce A and Bruce B to 2019, Bruce Power Letter, F. Saunders to R. Lojk, December 12, 2013, Attachment 4: NK29-03503.7 LOF NSAS, Analysis of Large Break Loss of Coolant Accident for Bruce B NGS in Support of Operation to 10550 EFPD, November 22, 2013.
- [182] CNSC REGDOC-2.4.1, Safety Analysis: Deterministic Safety Analysis, May 2014.
- [183] NK21-CORR-00531-07548/NK29-CORR-00531-08524, Action Item 090739 - Implementation of RD-310/Action Items 070718/071402: Safety Report Improvement Program, Bruce Power Letter, F. Saunders to K. Lafrenière, December 10, 2009
- [184] NK21-CORR-00531-10774/NK29-CORR-00531-11155, Safety Report Improvement Plan for Bruce A and B, Bruce Power, November 20, 2013.




 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- [185] NK21-CORR-00531-11214/NK29-CORR-00531-11621, Action Item 090739: Acceptance of Safety Report Improvement Plan for Bruce A and Bruce B, CNSC Letter, K. Lafrenière to F. Saunders, March 25, 2014.
- [186] NK21-CORR-00531-11940/NK29-CORR-00531-12323/NK37-CORR-00531-02372, Bruce Power Progress Report No. 6 on CNSC Action Plan-Fukushima Action Items, CNSC Letter, K. Lafreniere to F. Saunders, February 13, 2015.
- [187] NK21-CORR-00531-11710/NK29-CORR-00531-12099, Action Item 2014-07-5551: CNSC Type II Compliance Inspection Report: BRPD-AB-2014-012 - Probabilistic Safety Assessment Inspection, CNSC Letter, K. Lafrenière to F. Saunders, November 6, 2014.
- [188] Bruce Power, Summary of the Methodology and Results of the Bruce A and Bruce B Probabilistic Safety Assessments, Web accessed, May 2016:  
<http://www.brucepower.com/wp-content/uploads/2013/11/Microsoft-Word-Public-Website-Whitepaper-R04.pdf>
- [189] BP-PROC-00781-R003, Performance Monitoring, Bruce Power Procedure, September 11, 2015.
- [190] CNSC RD/GD-98, Reliability Programs for Nuclear Power Plants, June 2012.
- [191] NK21-CORR-00531-11324/NK29-CORR-00531-11729, Submission of S-294 Probabilistic Risk Assessment Final Reports, Bruce Power Letter, F. Saunders to K. Lafrenière, July 31, 2014.
- [192] NK21-CORR-00531-10063/NK29-CORR-00531-10482, Bruce Power Progress Report No.2 on CNSC Action Plan – Fukushima Action Items, Bruce Power Letter, F. Saunders to R. Lojk, January 31, 2013.
- [193] NK21-CORR-00531-12555/NK29-CORR-00531-12981, Action Item 2015-07-3683: Research Documents from Joint Project 4426 Pertinent to Containment Integrity, Bruce Power Email, J. Boyadjian to A. Robert, December 21, 2015.
- [194] NK29-DM-29-35360-R001, Bruce Generating Station Units 5-8, Design Manual, 29-35360 Primary Irradiated Fuel Bay, July 1981.
- [195] NK21-CORR-00531-10341/NK29-CORR-00531-10750, Bruce Power Irradiated Fuel Bay Structural Integrity Analysis, Bruce Power Letter, F. Saunders to R. Lojk, March 26, 2013.
- [196] NK21-CORR-00531-11381/NK29-CORR-00531-11784, CNSC Type II Compliance Inspection Report: BPRD-AB-2014-005 Fukushima Action Item Field Verification, CNSC Letter, K. Lafrenière to F. Saunders, June 3, 2014.
- [197] NK21-CORR-00531-10565/NK29-CORR-00531-10965, CNSC Review of Bruce Power's Irradiated Fuel Bay Structural Integrity Analysis (Fukushima Action Items 1.5.1, 1.6.1 and 1.6.2), CNSC Letter, R. Lojk to F. Saunders, June 3, 2013.
- [198] COG-JP-4426-005-R0, Multi-Unit Events Update of SAMG and Technical Basis Documents, CANDU Owners Group, June 2013.
- [199] NK21-CORR-00531-12209/NK29-CORR-00531-12635, Bruce Power Progress Report No.7 CNSC Action Plan – Fukushima Action Items, August 7, 2015.



 <div style="font-size: small;">Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- [200] NK29-OM-35030-R006, Bruce B Operating Manual – Record Irradiated Fuel Discharge Using NuFLASH, Section 3.5, October 2009.
- [201] NK29-PIP-20000-00001-R000, CSA N291 In-Service Inspection Program for Bruce NGS B Safety Related Structures, September 2014.
- [202] AR 28522224, Action Request Report: FASA SA-COM-2015-05, CSA N286.7-99 (R2012) Compliance with Bruce Power Licence Condition, October 20, 2015.
- [203] BP-PROG-15.01-R004, Nuclear Oversight Management, Bruce Power, December 18, 2013.
- [204] BP-PROC-00295-R012, Planning & Scheduling Audits, Bruce Power, September 16, 2013.
- [205] DPT-COM-00004-R002, Critical Drawing Management, Bruce Power, Obsolete.
- [206] CC171-25E-CNSC, Regulatory Oversight Report for Canadian Nuclear Power Plants: 2014, Canadian Nuclear Safety Commission, September 2015.
- [207] NK29-CORR-00531-13148, Bruce B: CNSC Type II Compliance Inspection Report: BRPD-B-2016-002, Environmental Qualification Program, New Action Item 2016-07-7682, March 11, 2016.
- [208] NK21-CORR-00531-12285/NK29-CORR-00531-12715, CNSC Type II Compliance Inspection Report : BRPD-AB-2015-006, Bruce A and B Generating Stations Quarterly Field Inspection Report for Q1 2015-16, August 13, 2015.
- [209] NK21-CORR-00531-12492/NK29-CORR-00531-12910, CNSC Type II Compliance Inspection Report : BRPD-AB-2015-011, Bruce A and B Generating Stations Quarterly Field Inspection Report for Q2 2015-16, November 16, 2015.
- [210] NK21-CORR-00531-12619/NK29-CORR-00531-13047, CNSC Type II Compliance Inspection Report : BRPD-AB-2015-013, Bruce A and B Generating Stations Quarterly Field Inspection Report for Q3 2015-16, January 22, 2016.
- [211] NK21-CORR-00531-12278/NK29-CORR-00531-12707, Action Item 2015-07-6855: CNSC Type II Compliance Inspection Report : BRPD-AB-2015-004 Fukushima Verifications, August 10, 2015.
- [212] NK21-CORR-00531-10926/NK29-CORR-00531-11305, New Action Item 1307-4427: Compliance Inspection Report BRPD-AB-2013-011 – Engineering Change Control Process, CNSC Letter, R. Lojk to F. Saunders, November 15, 2013.
- [213] NK21-CORR-00531-11707/NK29-CORR-00531-12096, Closure of Action Item 1307-4427: Compliance Inspection Report BRPD-AB-2013-011 – Engineering Change Control Process, November 5, 2014.
- [214] NK21-CORR-00531-10076/NK29-CORR-00531-10491, Bruce B CNSC Compliance Inspection Report BRPD-AB-2012-011 – Pressure Boundary Program Compliance at Bruce Power, R. Lojk to F. Saunders, November 26, 2012.

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## Appendix A – High-Level Assessments Against Relevant Codes and Standards

### A.1. CNSC G-149, Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors

CNSC G-149 [1] provides guidance to licensees in the development, maintenance and use of computer programs used in the design and safety analysis of nuclear power plants and research reactors. This guidance addresses the entire lifecycle of developing a computer program from coding, verification, validation, maintenance and documentation.

A high-level assessment of G-149 in Safety Factor Report 5 concludes that all G-149 requirements are encompassed by those of CSA N286.7-99 [2]. Accordingly, meeting CSA N286.7-99 requirements will satisfy the intent of G-149 guidance.


Per licence condition 4.2 [3] design and analysis computer codes and software used to support the safe operation are in accordance with CSA N286.7-99. Engineering analysis software covers the domain of highly specialized, high performance systems or software, used by a group of specialists for analysis and analytical simulation in support of the business, as defined in BP-PROC-00326 [4]. Systems in this domain are normally qualified in a manner to satisfy CSA N286.7, regulators or professional licensing. As noted in the Engineering Analysis Software procedure DIV-ENG-00006 [5], if the software is to be used for design analysis of nuclear safety related systems, CSA N286.7 must be specified as a quality requirement.

It is noted that some of the safety analysis in Part 3 of the Bruce B Safety Report were performed using legacy tools that predate 1999 and, thus, do not meet the requirements of CSA N286.7-99 and CNSC G-149. However, all new analyses are performed with the Industry Standard Toolset (IST) that are qualified according to CSA N286.7-99 requirements. Relevant deterministic safety analysis Bruce Power governance documents that satisfy N286.7-99 are:

- BP-PROG-10.01, Plant Design Basis Management [6],
- BP-PROC-00363, Nuclear Safety Assessment, Bruce Power [7],
- DPT-NSAS-00011 Configuration Management on Safety Analysis Software [8],
- DPT-NSAS-00013, Guidelines for Managing Reference Data Sets [9].


Moreover, DPT-NSAS-00011, Configuration Management on Safety Analysis Software [8] also indicates its consideration to CNSC G-149 guidance.

The Safety Analysis Improvement task team of the CANDU industry has established guidelines for performing Deterministic Safety Analysis [10], for conduct of computer code validation [11], and for computer code accuracy assessment [12]. These guidelines were established in compliance with the relevant requirements of CSA N286.7-99 and in consideration with the relevant guidance of CNSC G-149. The Bruce A and Bruce B SRI plan [13] is based on the use of these guidelines.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## A.1 References

- [1] CNSC G-149, Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors, October 2000.
- [2] CAN/CSA N286.7-99, Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants, March 1999 (Reaffirmed in 2012).
- [3] NK21-CORR-00531-12135/NK29-CORR-00531-12545/E-DOC 4659316, Licence Conditions Handbook, LCH-BNGS-R000, Bruce Nuclear Generating Station A and Bruce Nuclear Generating Station B Nuclear Reactor Operating Licence, PROL 18.00/2020 (Effective: June 1, 2015), Canadian Nuclear Safety Commission, May 28, 2015.
- [4] BP-PROC-00326-R004, Software Management, Bruce Power, November 6, 2012.
- [5] DIV-ENG-00006-R001, Engineering Analysis Software, Bruce Power, February 28, 2008.
- [6] BP-PROG-10.01-R009, Plant Design Basis Management, Bruce Power, December 4, 2014.
- [7] BP-PROC-00363-R003, Nuclear Safety Assessment, Bruce Power, January 24, 2013.
- [8] DPT-NSAS-00011-R004, Configuration Management of Safety Analysis Software, Bruce Power, October 11, 2013.
- [9] DPT-NSAS-00013-R003, Guidelines for Managing Reference Data Sets, Bruce Power Procedure, September 20, 2011.
- [10] COG-09-9030-R003, Principles & Guidelines for Deterministic Safety Analysis, CANDU Owners Group, November 2014.
- [11] ISTR-12-5044, Code Validation Guidelines Document, IST Report/COG, November 2012.
- [12] ISTO-09-5092, Guidelines for Generic Methodology for Estimation of Computer Code Accuracy, IST Report/COG, September 2012.
- [13] NK21-CORR-00531-10774/NK29-CORR-00531-11155, Safety Report Improvement Plan for Bruce A and B, Bruce Power, Bruce Power Letter, F. Saunders to R. Lojk, November 20, 2013.


 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## A.2. Changes to CSA N287.1-14, General Requirements for Concrete Containment Structures for Nuclear Power Plants


As part of this Periodic Safety Review (PSR), a high-level review of standard CSA N287.1-14 [1] was conducted. The clauses in the standard ensure that the design, construction, and testing of concrete containment structures will meet a quality standard commensurate with the safety principles necessary to comply with the Canadian nuclear safety philosophy. This standard applies to concrete containment structures for new nuclear power plants.

To conduct the assessment, a summary statement of the first-level headings of CSA N287.1-14 was prepared and compliance discussed against the summary statements. Where subsections are deemed essential to clarification of the scope of the first-level headings or they are considered "modern" requirements, the second-level headings are summarized and discussed. The following table contains the high-level review.

Clause	Summary Description	Compliance Discussion	Compliance Code
4	Requires classification of components as "class containment".	NK29-DM-34200 [2] states that the CSA N285.1-75 applies to the containment design. This assures that the classification is according to the requirement. Repairs and modifications will be done according to N287, as required by the LCH [3].	C
4.4	All phases of the containment life cycle will consider the effects of ageing.	Bruce Power has established a Life Cycle Management Plan for Civil Structures [4] that outlines a plan to detect and mitigate ageing mechanisms for civil structures and components, along with the acceptance criteria and safety margins for civil structures and components subjected to ageing degradation. Surveillance and the LRT (see discussion for Clause 8 below) address the effects of ageing in terms of monitoring components subjected to ageing degradation and the consequences of ageing effects.	IC

 <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Clause	Summary Description	Compliance Discussion	Compliance Code
5	Defines the responsibilities throughout the containment life cycle.	At this point in the life of the station, Bruce Power has responsibility for all aspects of the containment.	IC
6	Specifies the documentation requirements for constructing and commissioning containments.	Design requirements are specified in NK29-DM-34200 [2]. Since the containments have been constructed, all the design drawings required to construct had been prepared. Construction and commissioning documents are found in the corresponding history docket.	IC
7	Stipulates containment commissioning requirements.	The content of this clause is irrelevant at this point, since the containments have been constructed and commissioned. On-going testing is the subject of Clause 8 discussed below.	NA
8	Stipulates the requirements for in-service examination and testing.	Bruce Power performs a periodic inspection on the containment structures according to NK29-PIP-21100-00001 Periodic Inspection Program for Bruce NGS B Concrete Containment Structures and Appurtenances (Excluding Vacuum Building) [5], which was most recently executed in June, 2015 [6].	C
9	Requires CSA N286 as the basis for quality assurance.	CSA N286 is the basis for the Bruce Power Management System. See Section 3.2 of this report for further details. Processes for maintenance and modifications to containment comply with N286.	C

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

**Conclusion** – The high-level assessment above shows that Bruce Power complies with or complies with the intent of CSA Standard N287.1-14, General requirements for concrete containment structures for nuclear power plants.

## A.2 References

- [1] CAN/CSA N287.1-14, General Requirements for Concrete Containment Structures for Nuclear Power Plants, February 2014.
- [2] NK29-DM-34200-001-R003, Negative Pressure Containment System, Bruce Nuclear Generating Station Design Manual, July 1981.
- [3] NK21-CORR-00531-12135/NK29-CORR-00531-12545/E-DOC 4659316, Licence Conditions Handbook, LCH-BNGS-R000, Bruce Nuclear Generating Station A and Bruce Nuclear Generating Station B Nuclear Reactor Operating Licence, PROL 18.00/2020 (Effective: June 1, 2015), Canadian Nuclear Safety Commission, May 28, 2015.
- [4] B-PLAN-20000-00001-R000, Life Cycle Management Plan for Civil Structures, July 2010.
- [5] NK29-PIP-21100-00001-R003, Periodic Inspection Program for Bruce NGS B Concrete Containment Structures and Appurtenances (excluding Vacuum Building), September 2014.
- [6] NK29-CORR-00531-12650, Bruce B 2015: Containment and Vacuum Building Pressure Test Final Results, Bruce Power Letter, F. Saunders to K. Lafrenière, CNSC, July 31, 2015.



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

### A.3. CSA N287.3-14, Design Requirements for Concrete Containment Structures for Nuclear Power Plants

A high-level review was performed on the 2014 version of CSA standard N287.3 [1]. This standard applies to concrete containment structures for new nuclear power plants. The Bruce B containments were designed to CSA N287.3-1978 [2][3]. Thus, the containment structures are assumed to comply with that version of the standard. A code-to-code comparison of the 1978 version against the 2014 version of this standard was performed to identify the significant differences and those differences were assessed for design compliance from a high-level perspective.

This assessment identified three main differences in the 2014 version, which are discussed below.

**Beyond design basis** – The objective of this new requirement is to assess containment structures under beyond-design-basis conditions to ensure adequate safety margins against containment failure exist. Assessments of adequacy of the existing means to protect containment integrity and prevent uncontrolled release in beyond-design-basis accidents including severe accidents have been carried out as part of Fukushima Action Items initiatives. Bruce B containment has been shown capable of withstanding the conditions of severe accidents such that the leakage requirements are met. The results of Level 2 PRA showed that containment integrity can be challenged during a multi-unit severe accident if no mitigating measures are available. Bruce Power has completed analysis and assessment activities to evaluate options for ensuring containment integrity and filtered venting in the event of a multi-unit severe accident. The analysis examined the effectiveness of various Containment Filtered Venting System (CFVS) designs as well as the effectiveness of other options for protecting containment integrity and limiting fission product release during a multi-unit severe accident. A final report summarizing the results of the analysis is provided in [4]. Based on the conclusions of the report, which indicate that existing means to protect containment integrity and uncontrolled releases are adequate, Bruce Power requested closure of FAI 1.3.2. CNSC staff agreed that the closure criteria had been met as indicated in [5].

**Walls, slabs, shells, and domes** – The objective of the requirements in this subsection is reinforcement of the concrete in these structures in accordance with the seismic design rules of CSA A23.3. Bruce B seismic qualification is based on Design Basis Earthquake (DBE) Category A [2]. Since the containment design complies with the requirements of the 1973 version of CSA A23.3 [6] and the 1978 version of CSA N287.3 [3], the design complies with the intent of the modern standards.

**CSA A23.3 Reliance** - The 2014 version of CSA N287.3 [1] relies on CSA A23.3 more so than does the 1978 version. In many instances of use of this reference in the 2014 version, the detail in the corresponding clauses of the 1978 versions has been reduced, often now appearing in the version (2014) of CSA A23.3 [7]. From this point of view, the overall intent of N287.3 has not changed. Furthermore, while there has been an increase in overall detail over the years in CSA A23.3, the overall intent remains the same. A comparison of the tables of contents shows that all topics in the 1973 version have been addressed in the 2014 version. However, the 2014 version reflects modern design developments, such as the use of finite element analysis. The use of these modern requirements is intended to improve confidence in the design margins, but

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

adequacy of the containment design according to the 1973 version is periodically demonstrated with the periodic inspection plan [8]. Therefore, the design satisfies the intent of the 2014 version of this standard.


Two chapters have been added to the 2014 version of A23.3. Specifically, they are Chapter 22, Plain Concrete, and Chapter 23, Tilt-up Wall Panels.

Neither of these chapters is applicable to containments, so compliance is not required.

**Conclusion** – The Bruce B containments have been shown to comply with the intent of the three significant differences between the 1978 and 2014 versions of CSA N287.3 discussed above.

### A.3 References

- [1] CAN/CSA N287.3-14, Design Requirements for Concrete Containment Structures for Nuclear Power Plants, February 2014.
- [2] NK29-DM-34200-001-R003, Negative Pressure Containment System, Bruce Nuclear Generating Station Design Manual, NK29-DM-34200-001, July 1981.
- [3] CSA Standard, N287.3-1978, Design Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, July 1978.
- [4] NK21-CORR-00531-11801/NK29-CORR-00531-12195, Bruce Power Progress Report No. 6 on CNSC Action Plan – Fukushima Action Items, Bruce Power Letter, F. Saunders to K. Lafrenière, January 30, 2015.
- [5] NK21-CORR-00531-12417/NK29-CORR-00531-12829/ eDoc 4811376, Bruce Power Progress Report No. 7 on CNSC Action Plan – Fukushima Action Items: New Action Item 2015-07-3683, CNSC Letter, K. Lafrenière to F. Saunders, October 14, 2015.
- [6] CAN/CSA, A23.3-1973, Code for the Design of Concrete Structures for Buildings, December 1973.
- [7] CAN/CSA A23.3-14, Design of Concrete Structures, June 2014.
- [8] NK29-PIP-21100-00001-R003, CSA N287.7-08 Periodic Inspection Program for Bruce B Concrete Containment Structures and Appurtenances (excluding Vacuum Building), September 2014.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

#### **A.4. CSA N291-15, Requirements for Safety-Related Structures for Nuclear Power Plants**

CSA N291-15 [1] specifies requirements for the material, analysis and design, construction, fabrication, inspection, examination, and aging management of safety-related structures for nuclear power plants. The safety-related structures covered in this standard are:


- structures that support, house, or protect nuclear safety systems;
- components of structures that are required for the safe operation and/or safe shutdown of the reactor;
- structures for the storage of wet and dry irradiated fuel; and
- structures for the storage of radioactive waste material.

This standard is mentioned in the Licence Conditions Handbook (LCH) [2] as one of the documents that are providing additional recommendations and guidance in support of Licence Condition 5.1 (design program) of the PROL [3].

The standard is also mentioned in the LCH [2] in support of Licence Condition 6.1 (fitness for service) of the Power Reactor Operating Licence (PROL). Specifically, elements of the in-service inspection programs for safety related structures are expected to address the requirements of clause 7.3 (in-service examination) of CSA standard N291-08<sup>5</sup>.

The Management System Manual's List of Applicable Governing Acts, Regulations, Codes & Standards - Sheet 0003 [4] refers to N291-08. The overall objective of the Equipment Reliability program at Bruce Power [5] is to ensure that all systems important to safety (SIS) meet their defined design and performance criteria at defined levels of reliability throughout the life of the NPP. One of the implementing procedures of the program is the Long Term Planning and Life Cycle Management [6]. This procedure describes the process for developing and implementing Life Cycle Management Plans (LCMPs) for critical long lived SSCs, and is implemented by BP-PROC-00400 [7]. The latter procedure includes buildings and structures as part of the LCMP list and the safety related buildings and structures are identified in Appendix C of BP-PROC-00169 [8]. The LCMP for civil structures is outlined in [9]. It describes industry best practice in understanding ageing degradation of civil structures, and best practice for detection and mitigation. Acceptance criteria and required safety margins are discussed as these provide a basis for remaining life assessment of the structure. Acceptance criteria and required safety margins are discussed as these provide a basis for remaining life assessment of the structure. Condition Assessments are being developed for those structures that are shown to be critical to safety and generation. The governance requires that Preventive Maintenance procedures be developed for the other civil structures, if required. To meet the N291- requirements related to materials, Bruce Power plans to utilize the research described in Work Packages WP40533 and WP40534 in Enclosure 5 of Reference [10], COG-14-9405, Chemistry, Materials & Components R&D Program 2014/2015 Operational Plan.

<sup>5</sup> For the purpose of the Safety Factor 1 high level (HL) assessment of the CSA N291, the differences between the N291-08 and N291-15 versions of the standard are not significant enough to affect the assessment.

 <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

The in-service examination program required by CSA N291-08 is documented in NK29-PIP-20000-00001, CSA N291 In-Service Inspection Program for Bruce NGS B Safety Related Structures, September 2014 [11]. NK21-PIP-20000-00001 includes the inspection schedule and the report names for the safety-related structures to be inspected.

The high-level assessment above shows that Bruce Power complies with the requirements for safety-related structures specified in CSA N291-15.

#### **A.4 References**

- [1] CSA N291-15, Requirements for Safety-Related Structures for Nuclear Power Plants, November 2015.
- [2] NK21-CORR-00531-12135/NK29-CORR-00531-12545/E-DOC 4659316, Licence Conditions Handbook, LCH-BNGS-R000, Bruce Nuclear Generating Station A and Bruce Nuclear Generating Station B Nuclear Reactor Operating Licence, PROL 18.00/2020 (Effective: June 1, 2015), Canadian Nuclear Safety Commission, May 27, 2015.
- [3] NK21-CORR-00531-12136/NK29-CORR-00531-12546/E-DOC 4723908 , Nuclear Power Reactor Operating Licence, Bruce Nuclear Generating Stations A and B, PROL 18.00/2020, Canadian Nuclear Safety Commission, May 27, 2015.
- [4] BP-MSM-1 SHT0003 R005, MSM - List of Applicable Governing Acts, Regulations, Codes & Standards - Sheet 0003, Bruce Power, September 30, 2014.
- [5] BP-PROG-11.01-R005, Equipment Reliability, Bruce Power, December 16, 2015.
- [6] BP-PROC-00783-R001, Long Term Planning & Life Cycle Management, Bruce Power, September 25, 2013.
- [7] BP-PROC-00400-R002, Life Cycle Management for Critical SSCs, Bruce Power, July 5, 2013.
- [8] BP-PROC-00169-R002, Safety-Related System List, Bruce Power, September 28, 2007.
- [9] B-PLAN-20000-00001-R000, Life Cycle Management Plan for Civil Structures, Bruce Power, July 5, 2010.
- [10] NK21-CORR-00531-11339/NK29-CORR-00531-11742, 2014 Annual COG Research and Development Reporting, Bruce Power Letter, F. Saunders to K. Lafrenière, June 16, 2014.
- [11] NK29-PIP-20000-00001-R000, CSA N291 In-Service Inspection Program for Bruce NGS B Safety Related Structures, September 2014.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## **A.5. NFPA-805 (2015), Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plant**

Standard NFPA 805 [1] specifies the minimum fire protection requirements for existing Light Water NPPs during all phases of plant operation, including shutdown and decommissioning. Its requirements are largely included in the more detailed requirements of CSA standard N293-12, which defines the minimum fire protection requirements for design, construction, commissioning, operation and decommissioning of nuclear power powers. However, NFPA 805 is cited in CSA N293-12 as a source of guidance in several areas, namely:

- using economic loss prevention as an objective;
- the level of fire resistance rating for closures (e.g., doors and shutters);
- minimum fire sprinkler performance criteria for hazards other than fire;
- preparation of Fire PSAs.

The compliance with NFPA 805 guidance in each of these areas is discussed below.

### **Economic Loss Prevention**

NFPA 805 Section 1.4.4 requires that the following objectives are to be met during all operational modes and plant configurations:


- Potential property damage due to fire shall be limited to an acceptable level as determined by the owner/operator;
- Potential business interruption due to a fire shall be limited to an acceptable level as determined by the owner/operator;

These elements are reflected in the Bruce Power Fire Safety Management Plan [2]. The Plan's purpose includes minimizing interruption of power generation due to fires and minimizing economic loss resulting from fire damage to SSCs.

**Fire Resistance Rating for Closures:** NFPA Section 5.11.3 requires that passive fire protection devices such as doors and dampers shall conform to NFPA 80, Standard for Fire Doors and Other Opening Protectives [3].

It is noted in the Bruce A Code Compliance Review (CCR) [4] that checklists were prepared for code conformance review against NFPA 80 (1995) for the Bruce A Construction Retube Building, Amenities Building, Bruce A Main Guardhouse and Garage Building.

Similarly, it is noted in the Bruce B CCR [5] that checklists were prepared for code conformance review against NFPA 80 (1995) for the Bruce B Main Guardhouse and Garage Building, Emergency Response Building, and the Construction Office Trailer; and against NFPA 80 (1973) for the Powerhouse Complex, Unit Pumphouses, BNPD Site Pumphouse, Water Treatment Plant, Emergency Water and Power Supply Building, Fuel Oil Pumphouse (including fuel oil storage tanks), Standby Generator Buildings, Accumulator Building and Grade Level Storage Building, Vacuum and Emergency Filtered Air Discharge System (EFADS) Building and Ancillary Services Building. The checklists consists of code section, code section requirements and summary to capture the results of the evaluation. Supporting compliance justification is provided in the checklist when the requirement is met and further explanation is presented when

 <div style="font-size: small;">Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

a deviation resulted from the evaluation. The summary field for each identified deviation also includes a reference to a specific recommendation for the disposition of the code deficiencies. In some instances (e.g., the NBC), a checklist format for review of sections of the code was determined to not be appropriate for the review, and a more generic written evaluation was utilized to capture the relevant information of only certain sections (e.g., exposure protection).

### **Minimum Fire Sprinkler Performance Criteria - Hazards other than Fire**

Standard NFPA 805 Section 5.5.20 requires that the fire protection water supply system shall be dedicated for fire protection use only unless otherwise permitted by the following:

- (1) Fire protection water supply systems shall be permitted to be used to provide backup to nuclear safety systems, provided that the fire protection water supply systems are designed and maintained to deliver the combined fire and nuclear safety flow demands for the duration specified by the applicable analysis.
- (2) Fire protection water storage shall be permitted to be provided by plant systems serving other functions, provided that the storage has a dedicated capacity capable of providing the maximum fire protection demand for the specified duration as determined in this section.

Section 2.1.1.3 of the Bruce A Fire Protection System Design Manual (DM) [6] and of the Bruce B Fire Protection System DM [7] discuss the circumstances under which fire water otherwise dedicated for fire protection can be used during Beyond Design Basis Events.

### **Preparation of Fire PSAs**

NFPA 805 Section 4.4.3 has general requirements for Probabilistic Safety Assessment (PSA) modelling of fires, and Annex D provides guidance as to acceptable fire PSA methods and data, including the use of qualitative screening, quantitative screening and detailed probabilistic analysis.

Bruce Power is compliant by virtue of having generated and submitted to CNSC staff a PRA Guide on Internal Fire [8].


### **Summary**

A high-level review of those clauses in NFPA 805 which provide guidance cited in CSA Standard N293-12 indicates that Bruce Power is compliant.

### **A.5 References**

- [1] NFPA-805, Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants, 2015 Edition.
- [2] BP-PLAN-00008-R004, Fire Safety Management, Bruce Power, September 14, 2015.
- [3] NFPA 80, Standard for Fire Doors and Other Opening Protectives.
- [4] NK21-REP-71400-00005-R005, Bruce A Code Compliance Review, August 2012.
- [5] NK29-REP-71400-00002-R003, Bruce B Code Compliance Review, December 2012.
- [6] NK21-DM-71410-001-R007, BNGS A Fire Protection (Water) System Design Manual, August 2013.



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- [7] NK29-DM-71410-001-R003, BNGS B Fire Protection (Water) System Design Manual, December 2007.
- [8] B-REP-03611-00008-R000, Bruce Power PRA Guide, Internal Fire, Bruce Power, February 2011.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## **A.6. ANSI/NIRMA CM 1.0-2007, Guidelines for Configuration Management of Nuclear Facilities**

This standard provides guidelines for the planning, development and implementation of configuration management at a nuclear facility. The primary focus of the standard is to establish the key elements of a successful configuration program and identify the associated guidelines and considerations for each of these elements. The main purpose is to ensure consistency amongst the design requirements, physical configuration and facility configuration information.

Under Licence condition 5.1, Design Program [1], Bruce Power shall ensure configuration management is aligned with the design and safety analysis and incorporated into purchasing, construction, commissioning, operating and maintenance documentation. Conformance is to be maintained between design requirements, physical configuration and facility configuration information. Bruce Power shall establish a design authority function with the authority to review, verify, approve (or reject), document the design changes and maintain design configuration control [2].


A high level review of Bruce Power programs against the requirements in this standard was performed as part of this PSR. The review is focused on the applicable requirements for the six specific areas that are necessary for the configuration management implementation. The assessment compared the policies, programs and procedures in place at Bruce Power against the guidelines and considerations specified for each area of implementation. The assessment concluded that Bruce Power's Configuration Management Program provides a well-developed and systematic approach to the control of the plant configuration, design requirements, and facility configuration information to ensure the plant is operated, maintained and modified in a safe and reliable manner. The existing programs in place for Bruce Power meet the intent of the requirements.

It should also be noted that Configuration Management was assessed in SF-10 and results summarized in Section 5.3.10 of the SFR as well as in SF-11 as part of the Clause-by-Clause review of IAEA SSR 2/2 Safety of Nuclear Power Plants: Commissioning and Operation Specific Safety Requirements in Appendix B.2 Article 4.38. These reviews did not identify any gaps against the requirements assessed.

**Sections 1 and 2** present the scope of the standard and the relevant definitions used in the standard respectively. These are introductory sections and no assessment is deemed necessary.

**Section 3** lists the criteria for the six areas included in successful implementation of configuration management for nuclear facilities.

The Bruce Power Management System (BPMS) establishes the way Bruce Power manages all aspects of its business to ensure compliance with its operating licence, applicable codes, standards, legal and business requirements. The Management System Manual (MSM) [3] and associated MSM sheets define and document Bruce Power's Management System.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


Bruce Power uses programs to implement the MSM [3] and define regulatory and business requirements. BP-MSM-1 Sheet 0001 [4] contains the list of programs, program owners and approvers. The Bruce Power programs that relate to plant design are identified in BP-MSM-1 Sheet 0001 [4] under the functional areas of Configuration Management Engineering and Equipment Reliability.

The BPMS Management Program [5] establishes the framework for the ongoing implementation and change management of the BPMS. As specified in Section 4.5.2 of the BPMS Management Program [5] all functional areas consider change control with some functional areas developing specific procedures to manage changes within their processes and activities. The Executive Team of Bruce Power is considered the “senior leadership” of the Company and that role is defined in BP-MSM-1 SHEET 0002, MSM - Approved Reference Chart Authorities and Responsibilities – Sheet 0002 [6]. The management principles and policy statements are listed in Appendix A of [1] and reflect the top management support for the configuration management objectives.

**Section 3.1 Program Management** establishes the considerations related to program planning, physical configuration and facility configuration information scope criteria, concepts, interfaces and implementation of successful configuration management program.

The top level management commitment to the Bruce Power Management System is documented in MSM [3] The President and Chief Executive Officer is “personally committed to the Bruce Power Management System and expect the leadership, management and staff of Bruce Power to be individually and collectively committed to this Management System and to performing within its requirements and principles”. As stated under Configuration Management in Appendix A of the MSM [3] Bruce Power “shall operate, maintain and modify its plant in a manner that ensures that the physical plant, its design basis, and associated configuration information are consistent with each other at all times. Inconsistencies or deviations are to be identified and corrected through the Configuration Management process. The physical configuration of the plant shall be maintained in accordance with the design and licensing basis, and remain within the bounds of the Safe Operating Envelope. Design and operating margins will be understood and conservatively maintained within the bounds defined by the plant’s design basis. All physical modifications to the plant shall be implemented in accordance with approved procedures governing the initiation, preparation, review, approval, installation, performance verification and closeout of such modifications. All changes to the plant’s design basis, the Safety Report, the Safe Operating Envelope, and all analysis methods associated with them shall be managed in accordance with prescribed procedures and quality standards”.

Under the governance of BPMS, the Configuration Management Program [7] is established to ensure modifications to the plant, operation, maintenance and testing of the physical plant configuration are in accordance with the design requirements as expressed in the facility configuration information and to maintain this consistency throughout the operational life-cycle phase, particularly as changes are being made. The main principles that define the CM Program are listed in Appendix A Configuration Management Program Principles [7]. The Plant Design Basis Management Program BP-PROG-10.01 [8] and the Engineering Change Control Program BP-PROG-10.02 [9] govern the management of distinct changes to the plant design basis.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Under BP-PROG-10.02, Engineering Change Control, design changes and modifications are controlled so the design documentation remains consistent with the as-built and as-operated station and the design basis and design requirements. This includes non-physical changes to the design, which are covered via BP-PROC-00542, Configuration Information Change [10]. Physical changes are covered via BP-PROC-00539, Design Change Package [11].

The link to Safety Analysis is captured in BP-PROC-00363, Nuclear Safety Assessment [12]. Lower tier procedures under BP-PROC-00363, including DPT-NSAS-00011 Configuration Management of Safety Analysis Software [13], DPT-NSAS-00012 Preparation and Maintenance of Operational Safety Requirements [14], DPT-NSAS-00015 Planning and Execution of Nuclear Safety Assessments [15], cover: the updating of the SOE; execution of new analysis ensuring its review by those knowledgeable in the SOE; and the requirement to ensure that the condition of the plant is monitored and inspected so the results can be used to ensure that current safety margins of the aged plant remain adequate.

The Configuration Management (CM) Program [7] is established to document the implementation of configuration management and to promote consistent application of the CM objectives across the site:

1. Clearly define and communicate CM scope, responsibilities, authorities, principles, and interfaces.
2. Design basis and licensing basis requirements, which apply to the plant will be accurately identified, documented, maintained, and accessible.
3. The plant's physical structures, systems and components, and process computer controls will conform to design basis and license basis requirements.
4. Design basis and license basis requirements will be accurately reflected in plant documentation and in processes and procedures for altering, maintaining, testing, and operating the plant.
5. Consistency will be maintained among sources of plant information (documents and electronic data) as well as between plant information and the plant's physical and functional characteristics.
6. Continuous improvement of CM will be achieved by monitoring and assessing CM-related activities and by incorporating feedback of lessons learned from in-house and industry best practices and experience.

The Chief Engineer and Senior Vice President Engineering, acts as Bruce Power's designated Design Authority. As described in Section 3.1.4 of [7] the Design Authority is "a nuclear utility management assurance function with the accountability for ensuring that all design changes to the plant are properly designed, authorized, installed and commissioned and that the approved design basis is maintained". The processes by which the Chief Engineer and Senior Vice President, Engineering executes the role of Design Authority are outlined in DIV-ENG-00009 [16].

Independent mechanisms for initiation of review and appropriate dispositions of upsets in the configuration management model are incorporated in the Bruce Power programs. Configuration program oversight by line management is completed using self-assessments, Station Condition Records (SCR) trending, and management review of performance indicators.

The Engineering Change Control (ECC) program [9] specifies the manner in which design changes and modifications are defined, planned, implemented, and controlled. The ECC

 <div style="font-size: small;">Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

program objective is to ensure that design changes and modifications are controlled such that System, Structure, Component, and Significant Tools (SSCTs) continue to meet the design basis and operate safely for the full duration of design life. The program is applicable to all changes that affect design documents. The program applies a graded approach based on risk. The assessment of risk included elements of safety (industrial safety, reactor safety, environmental safety, radiation safety) and business needs.

PassPort is a database information system used by Bruce Power for identification, storage, control and retrieval of information important to configuration management.

With regards to physical configuration scope criteria, Bruce B Structures, Systems and Components (SSCs) have never been formally categorized as suggested in clause 3.1.2. Bruce Power employs a number of SSC lists to serve specific objectives as related to different aspects of safety considered in, for example, design, safety analysis, equipment reliability, structural integrity. The most important and comprehensive of these is the Safety Related System List (SRSL), as documented in BP-PROC-00169 [17]. The list utilizes a classification system that ranks safety-related systems groups depending on their significance to safety. This emphasis is graduated depending on the classifications and the safety-related functions within the listing. The methodology and process involved in determining which station systems are systems important to safety and their performance criteria and targets are described in the procedure DPT-RS-00012, Systems Important to Safety (SIS) Decision Methodology [18]. Given the clause allows for additional categories or a further decomposition of these categories to be developed as necessary, it is judged that Bruce Power meets the intent of graded approach to configuration management implementation.

The configuration management concepts, terminology and definitions are established and documented in Section 3.1 and in Appendix A of BP-PROG-10.03 [7]. As required in clause 3.1.4, these definitions are incorporated into the associated facility procedures. As specified in C.1 of Appendix A [7], one of the CM principles is to “clearly define and communicate CM scope, responsibilities, authorities, principles, and interfaces”. “CM awareness is promoted and training is included in initial and continuing training programs if required by the position”.

The CM program interfaces with implementing processes of BP-PROG-10.01, Plant Design Basis Management [8] and BP-PROG-10.02, Engineering Change Control [9]. This interface ensures the correct tools are used during design changes and modifications, the changes are controlled and documented. The requirement for clear definition and assignment of key roles and responsibilities is reflected in Section 7 of BP-PROG-10.03 [7]. The responsibilities of all plant, engineering and support staff, Chief Engineer and Senior Vice President Engineering, division and department managers are specified in Section 7 Responsibilities of BP-PROG-10.03 [7].

As described in Section 4.6 of BP-PROC-00335 Design Management [19] must control modifications to plant systems, structures and components, including temporary modifications and complex tools with a significant impact on nuclear safety. Change control must also be applied to changes or revisions which only involve design documentation, including instances where design document is discovered to not align with field configuration. The change control of engineering documentation is implemented through BP-PROG-10.02, Engineering Change Control [9] and BP-PROG-10.03, Configuration Management [7].



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

DPT-PDE-00025, Engineering Change Paper Management [20], provides direction for establishing requirements for preparing and controlling Engineering Change Papers used to identify approved changes to engineering controlled documents. The design programs for specialized and common areas of design along with the requirements associated with the execution of design activities for these areas are described in Section 4.9 of BP-PROC-00335 [19].

CM awareness is promoted and training is included in initial and continuing training programs if required by the position as defined in C.1 of BP-PROG-10.03 [7].

**Section 3.2 Design Requirements** presents the principles for establishment of design requirements and their basis, system and process boundaries, specific Structure, System or Component (SSC) list and assignment of SSC classes, margin information and communication of design requirements.

The design basis is the foundation for the development of the detailed design requirements for the individual SSCs. Plant Design Basis Management [8] defines the elements, functional requirements, implementing procedures and key responsibilities associated with the management of the plant's design basis. The system Design Requirements were originally specified as part of the System Design Manuals and were provided to the AECB at the time of the design. Design Requirements for modifications are prepared according to BP-PROG-10.02 Engineering Control [9].

The procedure DPT-PDE-00034 Preparation and Revision of System Design Manuals, Design Requirements and Design Description [21] provides a systematic and uniform process for preparation and revision of System Design Manuals (SDM) for Bruce Power. It includes instructions for the preparation of Design Requirements and Design Descriptions (DD) which are temporary documents until they are assembled to create the SDM.

The Operational Safety Requirements (OSRs) define the operating limits for a system and translate the assumptions used in the safety analyses into system-based requirements. The preparation and maintenance of the OSRs are governed by DPT-NSAS-00012 [14]. The OSRs are implemented with a gap analysis (administered through DPT-RS-00015 [22] of the Safe Operating Envelope Gap Assessment) to ensure that the plant is being operated in accordance with specified requirements.

As described in [10] any document that is used to describe the design basis and the detailed design is classified as a design document. Design documents are flagged in PassPort as "EC Required". The procedure B-LIST-08133-00001 [23] identifies the Bruce Power standard numbering format for controlled documents. The requirements for proper control and maintenance of the subject indexes in PassPort database to achieve consistency across Bruce Power are defined in [24]. Indexes are a critical component of nuclear operating systems and are embedded throughout its business processes, including financial management, materials management, plant equipment identification and documentation classification.

The Equipment Codes process (Section 4.6 of [7]), as documented in BP-PROC-00898 [24], governs the method to achieve consistent identification of equipment and is to be used in selecting the structure of an equipment code. This process applies to all Bruce Power design, engineering, and operations documentation. Equipment codes are used on engineering



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

drawings, manuals, procedures, flowsheets, computer databases, shop records, spare parts lists, orders-to-operate, work protection, and on the equipment itself in the field.

BP-PROC-00320, Management of System/Subject Classification Indexes [25], establishes the requirements for proper control and maintenance of the subject indexes for equipment identification and system/component design documentation. The identification and labelling of systems and components shall be controlled. The requirements to do so are implemented through BP-PROG-10.03, Configuration Management [7].

As specified in Section 1.0 of [7] “the plant’s physical structures, systems and components, and process computer controls will conform to design basis and license basis requirements”; hence the CM procedure [7] applies to all SSCs. Since there are no exceptions (per Section 2.0 in [7]) to the configuration management program, the requirement in clause 3.2.3 for identifying specific equipment list included in the program scope is not applicable.

Bruce Power employs a number of SSC lists based on ranking scheme, which meets the intent of the requirement in clause 3.2.4 for classification based on the degree of control placed on all activities associated with the SSCs.


One of the configuration management principles defined in C.2 of Appendix A of [7] is to accurately identify, document, maintain and access the design basis and licensing basis requirements. In addition, as per design input definition (Section 3.1.5 of [8]) “design inputs are criteria, parameters, bases, and other design requirements upon which the final design is based”. Section 4.3 of BP-PROC-00335, Design Management [19], requires applicable design inputs to be appropriately specified in a timely manner, documented and correctly translated into design output documents. These design inputs form the bases for design decisions, and their selection and modification is reviewed, verified and approved by the responsible design organization.

As identified in Section 2.4 of the PSR Basis Document [26], a comprehensive review of the tracking of licence concessions granted to Bruce Power by the Regulator was conducted [27]. It was concluded that Bruce Power should establish a controlled, centralized and accessible company database of licence concessions to support design activities, and this is identified as gap SF1-24 in Table 8.

Design and safety analysis margins against applicable acceptance criteria are documented in the design documentation and Safety Analysis Report. Margin Management, as documented in BP-PROC-00786 [28] governs a systematic process to identify, prioritize and resolve margin issues to help ensure that the operating configuration is conservatively maintained within the design requirements and that design requirements are conservatively maintained within the design basis. As required in clause 3.2.6, Design and Operating Margin Management (BP-PROC-00786 [28]) fulfills the following main objectives:

1. Support safe and reliable plant operation.
2. Ensure plant equipment configuration and performance are consistent with design and licensing requirements.
3. Conduct day-to-day operations reflecting consideration of design and operating margins.

The requirement for communicating new and/or revised design information is addressed in Sections 4.6 and 4.7 of BP-PROC-00335 [19]. As described in Section 4.7 of [19] “Design information, including changes, shall be communicated from one organization to another, and

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

within an organization, by controlled documents that are uniquely identified and issued by authorized persons. For design changes, interface requirements for developing and reviewing the design and establishing documentation interface status are identified in design plans as per DPT-PDE-00006, Design Plan [29]. This ensures that design interfaces are appropriately fulfilled and established.”


**Section 3.3 Information Control** specifies the requirements for identification, categorization, storage, control and tracking systems, retrieval of facility configuration information, minimization of redundant information and operational configuration information status control.

The requirements for information identification are reflected in Section 4.8 of BP-PROC-00335, Design Management [19], as follows: The records that are to be produced and retained shall be identified and their retention period specified in accordance with their respective procedures. Records that are deemed quality assurance records shall be identified as such. The records shall be complete, valid, legible, retrievable, and traceable to the parts and activities to which they refer. Processing of official records is described in BP-PROC-00972 Records Retrieval and Secure Storage [30], and BP-PROC-00098, Records Management [31]. Retention of records is managed through BP-PROC-00238, Retention Process for Bruce Power Records [32]. The process for managing the life cycle of Bruce Power Controlled documents is defined in BP-PROC-00068 [33].

All records are managed according to Records Management procedure BP-PROC-00098 [31] to ensure all records regardless of media are properly categorized. BP-PROC-00972, Records Retrieval and Secure Storage [30], defines the controls for storage of and access to Bruce Power records to ensure their integrity and protection against damage, deterioration or loss. Records are stored in a predetermined storage facility for the retention period specified for each record. The retention process for Bruce Power records follows the steps outlined in BP-PROC-00238 [32] for Bruce Power Records.

The control and tracking of records is performed through the PassPort system. According to Section 4.1.3 of BP-PROC-00584 [34] PassPort Equipment Data Management for Design Change Packages depending on the type of Engineering Change (EC); configuration changes resulting from plant modifications, design changes, or revisions to configuration information in documents and databases are implemented according to the timelines found in BP-PROC-00542 [10] for Configuration Information Changes (CIC) or BP-PROC-00539 [11]. Configuration information changes include creation of new equipment codes, revision of existing information and update with missing data. Configuration Management equilibrium upsets that identify discrepancies where the physical equipment is installed, but the design information does not list the equipment, will require an EC type CIC subtype Intent in accordance with BP-PROC-00068, Controlled Document Life Cycle Management [33], to be submitted. Design Engineering and Drafting Office representatives are responsible for restoring plant configuration by updating the PassPort MEL database and design documents (Section 7 of [34]). Throughout this process the Drafting Office is performing a quality check to ensure MEL records are created and maintained in compliance with the minimum standards defined in this procedure.

The most current documentation is readily available in PassPort to all users. As described in BP-PROC-00972 [30] (Section 4.2.2) for records that have been approved by the Records Officer to be retained in electronic format shall be stored in Content Server. Electronic records that are stored in Content Server have controls such as user authentication and permissions

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

control, firewall protection, system back-ups, disaster recovery and audit trail. Information Technology supports the Document Management Program in the management of information technology as governed by BP-PROG-03.02, Information Technology [35].

The facility information is available in a database and readily retrievable. Section 4.3 of BP-PROC-00972, Records Retrieval and Secure Storage [30], applies to all records and defines the controls applied for records retrieval. Per Section 3.1.6 of BP-PROC-00972 [30], records are designated permanent or non-permanent. The non-permanent records minimum retention period is defined to minimise redundant information. Access to records is controlled to ensure the integrity of all records as defined in Section 4.2.6 of BP-PROC-00972 [30]. The document management program is subject to records management oversight activities per BP-PROC-00238, Retention Process for Bruce Power Records [32].

As specified in Appendix A principle C.5 (d), of BP-PROG-10.03 [7] “consistency will be maintained among sources of plant information (documents and electronic data) as well as between plant information and the plant’s physical and functional characteristics. Data is controlled at its source and resides in one location. Redundant plant configuration information is minimized”. Section 1 of BP-PROG-10.03 [7] requires that the plant’s “physical structures, systems and components, and process computer controls to conform to design basis and license basis requirements.”


The operations documentation for normal and abnormal operation are governed by BP-PROG-12.01, Conduct of Plant Operations [36]. Operations Documentation procedures include Operating Manuals, Operating Memos, Alarm Response Manuals, and Safety System tests. Procedures for the safe and reliable operation of plant equipment are prepared, approved, controlled and readily available to the operating staff. These procedures are prepared for anticipated normal, abnormal and emergency conditions (Section 4.1 of [36]).

Operating procedures are created as controlled documents, in accordance with the requirements of BP-PROG-03.01, Document Management [37] to ensure that document lifecycle management requirements defined in BP-PROC-00068, Controlled Document Life Cycle Management [33] are met.

**Section 3.4 Change Control** discusses the requirements for identification, review, implementation and documentation of changes.

The Configuration Management Program ensures all changes are independently reviewed and assessed for impact on the design and operating margins. This is reflected in the principle C.4 of Configuration Management Program [7], i.e., the controls for making changes include a formal review of the design input requirements and personnel are trained on changes prior to operating or maintaining modified equipment. The associated documentation (procedures, operational drawings, etc.) are revised before implementation of the change (Appendix A of [7]).

The BP-PROG-10.02, Engineering Change Control (ECC) Program [9], specifically addresses how design changes and modifications are identified, planned, implemented, and controlled to ensure design changes and modifications are controlled. This approach ensures the Structures, Systems, Components and Tools (SSCTs) continue to meet the design basis and operate safely for the full duration of design life and the design documentation remains consistent with the as-built and as-operated station, the design basis and the design requirements (Section 1.0 of [9]). The ECC Program [9] defines the steps necessary to ensure that proper reviews are

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

conducted prior to the change, so that the Plant Design Basis, Operations and Maintenance procedures can remain synchronized with the implementation of the design changes. According to Section 4.0 of [9], the Program includes the following implementing procedures:

- BP-PROC-00743, Site Services Engineering Change Control [38];
- BP-PROC-00542, Configuration Information Change [10];
- BP-PROC-00539, Design Change Package [11];
- BP-PROC-00877, Modification Installation Quality Assurance [39]; and
- BP-PROC-00615, Commissioning Modifications and Projects [40].

Non-physical changes to the design are covered via BP-PROC-00542, Configuration Information Change [10], whereas the physical changes are covered via BP-PROC-00539, Design Change Package [11].

The ECC program applies a graded approach based on risk. Section 4.0 of [9] requires the elements of safety (industrial safety, reactor safety, environmental safety, radiation safety) and business needs to be included in the assessment of risk.

All changes that may affect the design basis or the safety report are governed through the BP-PROC-00363, Nuclear Safety Assessment [12] and associated lower tier procedures under BP-PROC-00363. Any exceptions to this procedure require approval by the Chief Engineer and Senior Vice President, Engineering (Section 2 of [12]). As described in Section 4.0 of [12], Nuclear Safety Assessment addresses proposed or planned changes such as design changes, changes to operating procedures, maintenance and surveillance requirements, or plant status changes.

Section 4.7 of BP-PROG-10.03 [7] requires configuration management control of the temporary changes. The Temporary Configuration Change Management process is documented in BP-PROC-00638 [41] to ensure that the temporary changes are adequately controlled and documented.

The documentation of design changes and modifications is subject to configuration control processes depending on the change. As specified in Section 4.2 of BP-PROG-10.02 [7], the Configuration Information Change process, BP-PROC-00542 [10], governs the acceptance, creation, revision, obsolescing and superseding of design information when one or more of the following apply:

- Design information is being corrected.
- No inspection, testing, or commissioning activities are required to verify the field against the new design information.
- Operations acceptance via Operations Manager sign-off of the new design information is not required.
- Senior Operations Authority approval is not required in accordance with the OP&Ps.
- Operations activities are covered by approved operating or maintenance procedures at the time they are performed.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

The Design Change Package process, as documented in BP-PROC-00539 [10], specifies the control of modifications to plant systems, structures, components, and significant tools, including temporary modifications. The overall objective is to meet regulatory requirements, ensure safety, and minimize loss to the company through appropriate risk management activities (Section 4.3 of [9]).

The Configuration Management Program requires that the impact on the plant simulator be identified. Principle C.4 in Appendix A of [7] specifically requires “modifications of station simulators and training materials to coincide with or precede each plant modification”.

The Modification Installation Quality Assurance process, as documented in BP-PROC-00877 [39], governs modification installation quality assurance and includes the production and oversight of Inspection and Test Plans (ITPs) and work packages that support design changes and modifications. An EC is the electronic PassPort record of a design change or modification. The EC provides information necessary to develop and prepare an ITP which lists work activities in sequence and indicates the associated verification activity and acceptance criteria. Associated documents that satisfy installation and verification documentation requirements are added to the ITP to create a work package that is issued to the installing trades for execution (Section 4.4 of [9]).

BP-PROC-00703 [42] procedure governs the approach towards managing change at Bruce Power and is applicable to organizational, documentation and process changes. As specified in Section 1.0 of [42] before changes are made, they need to be justified and subject to review. Change requirements, including the reason for changes, are to be identified and controlled. The level and extent of this review depends on the scope or complexity of the change, and its impact on business requirements including safety. The type of change and associated procedures are specified in Section 4.1 of [42].

**Section 3.5 Assessments** establishes the requirements for assessment of configuration management effectiveness, performance monitoring and health reports.

The adequacy of processes and procedures to achieve the CM objectives is periodically assessed through Programmatic Assessments.

The Nuclear Oversight Management Program, BP-PROG-15.01 [43] identifies the processes required to independently oversee the Bruce Power’s Management System. This program implements the process objectives and policy statements stated in BP-MSM-1, Management System Manual [3], Appendix A. As part of the MSM, the Configuration Management Program is subject to nuclear oversight to ensure its effectiveness. The key elements of the nuclear oversight process are listed in Section 4.0 of BP-PROG-15.01[43]. The audit basis and approach for independently assessing the Management System Programs is presented in Appendix B of BP-PROC-00295, Planning and Scheduling Audits [44]. The Configuration Management Program [7], Document Management [37], Plant Design Basis Management [8] and Engineering Change Control Program [9] are audited at least once over a 3-year period and the audits are conducted by the Audit Department within the Nuclear Oversight and Regulatory Affairs Division.

The requirement for physical configuration assessment follow up and staff walkdowns are reflected in BP-PROC-00539 Design Change Package [10], BP-PROC-00615 Commissioning of Modifications and Projects [40], and BP-PROC-00877 Modification Installation Quality



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Assurance [39]. The objective of the Bruce Power Corrective Action Program BP-PROG-01.07 [45] is to identify and eliminate or mitigate adverse conditions that have resulted in or could result in loss. As required in Section 4.0 of BP-PROG-01.07 [45], all adverse conditions and non-conformances are to be promptly identified, documented and reported. The corrective actions taken to address identified causes are tracked to completion. Non-conformances in configuration are identified as per BP-PROC-00060 [46], the Station Condition Record Process. Trends in configuration are captured and the ongoing implementation is also monitored through reviews of audit findings related to configuration management. As per Section 4.4 of BP-PROG-01.07 [45] corrective actions are tracked to completion through the PassPort system as defined in BP-PROC-00019, Action Tracking [47]. Due dates for actions are commensurate with the importance of the item, station priorities and the consideration of preventing recurrence.

The requirement for periodic equipment performance monitoring is implemented through system performance monitoring as described in Section 4 of the Equipment Reliability Program BP-PROG-11.01 [48] and assessed in detail in SF-2 and SF-4.

The mechanism for monitoring, trending and reporting the health of the Bruce Power Configurational Management Program is described in the Configuration Management Program Oversight and Trending, BP-PROC-00470 [49]. The Configuration Management program indicators are monitored and performance metrics reported regularly as part of the business health reporting process (Sections 4.1 and 4.2 of BP-PROC-00470 [49]). Program oversight consists of assessing station condition records against CM activities/events, performance indicators, results of audits, inspections and self-assessments. Self-assessments are completed on an annual basis in accordance with BP-PROC-00137, Focus Area Self-Assessment [50]. Focus areas are selected from program activities based on a qualitative management review of performance in the previous year. Relevant SCR data is monitored by line management in accordance with BP-PROC-00412, Trending, Analyzing and Reporting of SCRs [51]. Line management review of performance indicators occurs monthly. Each performance indicator, as defined within the program implementing processes, is assigned an owner who is responsible for performance. During line management review, the reported performance is challenged. When performance is below expectations, the indicator owner is responsible to produce an action plan that will close the gap (Section 4.8 of BP-PROG-10.03 [7]). Effectiveness of Bruce Power's configuration management activities is also addressed in Section 5.3.10 of SF-10 report.

**Section 3.6 CM Awareness Training** provides the training content requirements for facility personnel training of the configuration management concepts, terminology, definitions and associated procedures.

The requirement for configuration management training is defined in principle C.1 of Appendix A of BP-PROG-10.03 [7] as follows: "CM awareness is promoted and training is included in initial and continuing training programs if required by the position". Principle C.4 (d) of Appendix A of [7] further requires that "training materials should coincide with or precede each plant modification".

Section 3.1.1 of BP-PROG-10.03 [7], the CM is an integrated management process to ensure that "plant configuration documents specifying operations, maintenance, testing, installation, procurement, inspection, and training requirements are updated and maintained consistent with the plant design".



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


Appendix 1 Specific Qualifications of TQD-00082 [52] presents the qualifications which apply to Configuration Management and are controlled and specified by the line organization. The overall structure of the CMS training program is provided in Section 6 of TQD-00082 R001 [52].

## A.6 References


- [1] NK21-CORR-00531-12136/NK29-CORR-00531-12546, Nuclear Power Reactor Operating Licence, Bruce Nuclear Generating Stations A and B, PROL 18.00/2020, eDoc 4723908, May 27, 2015.
- [2] NK21-CORR-00531-12135/NK29-CORR-00531-12545, Licence Conditions Handbook (LCH-BNGS-R000), Bruce Nuclear Generating Station A and Bruce Nuclear Generating Station B, Nuclear Power Reactor Operating Licence, PROL 18.00/2020, eDoc 4659316, May 27, 2015.
- [3] BP-MSM-1-R012, Management System Manual, Bruce Power, June 23, 2014.
- [4] BP-MSM-1 Sheet 0001-R020, MSM - Bruce Power Program Matrix – Sheet 0001, January 23, 2015.
- [5] BP-PROG-01.02-R009, Bruce Power Management System (BPMS) Management, December 15, 2015.
- [6] BP-MSM-1 SHEET 0002-R015, MSM - Approved Reference Chart Authorities and Responsibilities – Sheet 0002, January 20, 2015.
- [7] BP-PROG-10.03-R006, Configuration Management, Bruce Power, February 5, 2015.
- [8] BP-PROG-10.01-R009, Plant Design Basis Management, Bruce Power, December 4, 2014.
- [9] BP-PROG-10.02-R010, Engineering Change Control, Bruce Power, November 12, 2014.
- [10] BP-PROC-00542-R007, Configuration Information Change, Bruce Power, November 24, 2015.
- [11] BP-PROC-00539-R016, Design Change Package, Bruce Power, June 23, 2015.
- [12] BP-PROC-00363-R003, Nuclear Safety Assessment, Bruce Power, January 24, 2013.
- [13] DPT-NSAS-00011-R004, Configuration Management of Safety Analysis Software, Bruce Power, October 11, 2013.
- [14] DPT-NSAS-00012-R004, Preparation and Maintenance of Operational Safety Requirements, Bruce Power, October 28, 2014.
- [15] DPT-NSAS-00015-R004, Planning and Execution of Nuclear Safety Assessments, Bruce Power, October 16, 2013.
- [16] DIV-ENG-00009-R005, Design Authority, Bruce Power, November 1, 2013.
- [17] BP-PROC-00169-R002, Safety-Related System List, Bruce Power, September 28, 2007.
- [18] DPT-RS-00012-R001, Systems Important to Safety (SIS) Decision Methodology, Bruce Power, September 24, 2013.
- [19] BP-PROC-00335-R007, Design Management, Bruce Power, July 30, 2015.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- [20] DPT-PDE-00025-R007, Engineering Change Paper Management, Bruce Power, June 14, 2013.
- [21] DPT-PDE-00034-R002, Preparation and Revision of System Design Manuals, Design Requirements and Design Description, Bruce Power, January 26, 2015.
- [22] DPT-RS-00015-R000, Safe Operating Envelope Gap Assessment, Bruce Power, May 31, 2011.
- [23] B-LIST-08133-00001-R012, Controlled Document Numbering List for PassPort, January 15, 2015.
- [24] BP-PROC-00898-R000, Equipment Codes, Bruce Power, June 19, 2013.
- [25] BP-PROC-00320-R004, Management of System/Subject Classification Indexes, Bruce Power, June 2, 2010.
- [26] NK29-CORR-00531-12932, Bruce B Periodic Safety Review Basis Document, Bruce Power Letter, F. Saunders to K. Lafrenière, January 25, 2016.
- [27] B-REP-09701-18AUG2016, Review of Bruce A and B Licence Concessions, August 18, 2016.
- [28] BP-PROC-00786-R003, Margin Management, Bruce Power, August 5, 2014.
- [29] DPT-PDE-00006-R013, Design Plan, Bruce Power, June 26, 2014.
- [30] BP-PROC-00972-R000, Records Retrieval and Secure Storage, Bruce Power, November 21, 2014.
- [31] BP-PROC-00098-R015, Records Management, Bruce Power, November 27, 2014.
- [32] BP-PROC-00238-R012, Retention Process for Bruce Power Records, Bruce Power, November 26, 2014.
- [33] BP-PROC-00068-R023, Controlled Document Life Cycle Management, Bruce Power, December 11, 2015.
- [34] BP-PROC-00584-R008, PassPort Equipment Data Management, Bruce Power, October 19, 2015.
- [35] BP-PROG-03.02-R004, Information Technology, Bruce Power, June 2, 2014.
- [36] BP-PROG-12.01-R007, Conduct of Plant Operations, Bruce Power, August 13, 2013.
- [37] BP-PROG-03.01-R016, Document Management, Bruce Power, August 31, 2015.
- [38] BP-PROC-00743-R003, Site Services Engineering Change Control, Bruce Power, November 28, 2012.
- [39] BP-PROC-00877-R000, Modification Installation Quality Assurance, Bruce Power, October 29, 2012.
- [40] BP-PROC-00615-R001, Commissioning of Modifications and Projects, Bruce Power, September 20, 2013.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- [41] BP-PROC-00638-R012, Temporary Configuration Change Management, Bruce Power, May 7, 2014.
- [42] BP-PROC-00703-R001, Change Management Guidance, Bruce Power, December 1, 2010.
- [43] BP-PROG-15.01-R004, Nuclear Oversight Management Program, Bruce Power, December 18, 2013.
- [44] BP-PROC-00295-SHT0001-R003, Audit Basis and Approach, Bruce Power, December 19, 2013.
- [45] BP-PROG-01.07-R010, Corrective Action, Bruce Power, August 30, 2013.
- [46] BP-PROC-00060-R028, Station Condition Record Process, Bruce Power, November 5, 2015.
- [47] BP-PROC-00019-R010, Action Tracking, Bruce Power, May 12, 2015.
- [48] BP-PROG-11.01-R005, Equipment Reliability, Bruce Power, December 16, 2015.
- [49] BP-PROC-00470-R004, Configuration Management Program Oversight and Trending, Bruce Power, October 1, 2012.
- [50] BP-PROC-00137-R015, Focus Area Self-Assessment, Bruce Power, March 10, 2015.
- [51] BP-PROC-00412-R006, Trend Identification and Reporting of SCRs, Bruce Power, August 18, 2014.
- [52] TQD-00082-R001, Configuration Management and Support, Training and Qualification Description, Bruce Power, November 16, 2011.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## **A.7. ASME BPVC Section III, Rules for Construction of Nuclear Power Plant Components**

Significant changes to ASME Section III are summarized in ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components [1][2] Appendix 6, with changes to the material requirements in Appendix 9 (there were no changes listed after 2007 in Appendix 9). Only significant changes that could imply that safety margins of existing equipment could possibly be lower than originally intended are of concern. Hence, changes related to the following, are not required for consideration:

- Changes relating to Quality Assurance (QA) provisions
- Changes allowing new or alternative materials
- Changes that incorporate alternative rules or calculation methods
- Changes allowing alternative test methods.

### **Summary of previous review findings**

#### **Bruce A Units 1 to 4 ISR findings [3]**

The design, materials, fabrication, inspection, testing and examination of the original Bruce A pressure retaining components complied with 1968, winter 1970 addenda of Section III of the ASME code. The requirements were further supplemented by the AECL design guides and specifications.

In the 2008 Safety Factor 1: Plant Design report [4], a review was conducted for Bruce A (Units 1 to 4) from the basis of the Bruce 1&2 Integrated Safety Review (ISR), expanding the review to cover the ASME III 2007 code and extend to Units 3 and 4. The review concluded that Bruce A (Units 1 to 4) would be safe to operate. Deviations to ASME Code Section III were identified but were determined to not have an impact on the structural integrity of the pressure retaining systems and components. The clauses pertained to aging effects, such as radiation embrittlement and to new requirements for supports, containment penetrations and expansion bellows.

These are outlined below:

- Non-Ductile Failure  
ASME Section III Sub-article NB-3211(d) and NF-3131(e) for Class 1 components and Class 1 supports mandate an assessment to demonstrate that the components and supports are protected from non-ductile fracture for all service levels A, B, C and D. This was not a requirement in the original design code. This requirement applies to pressure vessels, pumps, valves, piping, and supports. The stress and fatigue analysis methods in the modern code are more extensive and detailed, but the original code design meets the intent. All future Class 1 modifications including feeders and boiler tube bundles, etc., are to comply with new codes and standards. Any Class 1 non-identical component replacement will also consider fracture mechanics analysis if required.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- Piping and Component Supports

Pressure retaining components and pressure retaining containment barriers require support design to Subsection NE. This applies to Class 1, 2, 3, and 4 piping and components. This was not a requirement of the original code. The supports for the original designs were designed based on the best available industry practices including Building Construction Code and Steel Construction Manual supplemented by the AECL technical specifications. It is judged that the design of supports for mechanical loads and static seismic loads, where applicable, meets the intent of Subsection NE. Also, it is expected that the Life Assessment Inspection Program will ensure the adequacy of supports.

The loads due to steady state and transient temperature differences between the component and support, and high cycle fatigue considerations may need to be addressed. High cycle fatigue analysis as per NF-3330, and limit load analysis in accordance with NF-3340 are to be used in design of Class 1 linear supports that are subjected to high cycle fatigue. Class 2 and MC supports are designed by analysis. Class 3 supports may be designed by rules. Application of Subsection NE to nuclear code class systems and component supports was not a requirement of the original code and can be considered as non-compliant regarding design and analysis methodology for supports.


Bruce Power had committed to review and assess the design calculations for typical component supports, and typical standard supports and the Fuelling Machine supports to determine whether the design of supports meet the intent of the modern ASME Section III codes and CSA N285.0-95 Clause 14. Components will be registered as part of the registration of the system and this issue was addressed as Issue SF1-14 in the 2008 Safety Factor Report. At that time, progress was underway to update the system registration and to register previously unregistered systems in accordance with the N285.0 standard.

This issue is included in the Bruce A, Bruce B, and Centre of Site Integrated Implementation Plan from the SBR [5] as Global Improvement Opportunity (GIO), GIO-001, "Improve documented design basis". The Bruce B Legacy Registration project is on track for completion December 2017 [6]. It will continue to be tracked in the Integrated Implementation Plan (IIP) under global improvement opportunity GIO-001.

- Cyclic loading for containment penetrations

The modern code for Class 4 components (Subsection NE, article NE-3200) requires fatigue analysis for cyclic operating transients and loads. This was not a requirement in the Bruce A original design code. Bruce Power committed in the 2008 Safety Factor Report 1 [7] in Issue SF1-11 to evaluate cyclic loads on a sample number of typical Class 4 penetrations for each penetration type to determine the standards they were designed to, and determine whether there is a significant deviation from present codes and standards that would affect their function. The designs for all future Class 4 modifications are to comply with modern codes and standards.

This issue is included in the Bruce A, Bruce B, and Centre of Site Integrated Implementation Plan from the SBR [5] as GIO-005, "Assess cyclic loads of pressure

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

retaining components designed per ASME III and VIII." Work is expect to start on Bruce B in 2016 [5]. It will continue to be tracked in the IIP under global improvement opportunity GIO-005.

- **Fatigue Assessment for Bellows Expansion Joints**

The modern codes require fatigue assessment for Class 2, Class 3 and Class 4 (NC-3649,ND-3649 and NE-3600) bellows expansion joints. This was not a requirement in the Bruce A original design codes. Bruce Power committed in the Bruce 3 and 4 ISR Integration Implementation Plan [8] to evaluate a sample number of typical Class 2,3 and 4 bellows expansion joints to gain experience, develop screening criteria, and further evaluate as required.

This issue is included in the Bruce A, Bruce B, and Centre of Site Integrated Implementation Plan from the SBR [5] as GIO-005, "Assess cyclic loads of pressure retaining components designed per ASME III and VIII." Work is expected to start on Bruce B in 2016 [5]. It will continue to be tracked in the IIP under global improvement opportunity GIO-005.

### **Summary of SBR findings - changes to ASME III from 2007 to 2011**

This section presents findings of a review against changes made to ASME III Division 1 in the period from 2007 to 2011. An Updated Code Reconciliation Report, ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components [1] was issued to Bruce Power on 2012 December 7, which reviewed and assessed the changes to several codes.

The report [1] verified that ASME Section III Division 1 has not made any significant changes that change the original design basis of any equipment.

### **Summary of current review findings**

#### **Changes to ASME Section III from 2011 to 2015**

Significant changes to ASME Section III up to the 2015 edition are summarized in ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components [2] Appendix 6, with changes to the material requirements in Appendix 9.

The following items noted in the Code Reconciliation Report ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components of 2015 September 16, [2] Appendix 6, are changes identified in ASME Section III since 2011, introduced in the 2013 and 2015 Editions. There is no documentation available indicating that these changes have been reviewed for impact on safety margins.

- NC-3324.11(b)(5)(-a), NC-3324.11(b)(5)(-b), ND-3324.11(b)(5)(-a), ND-3324.11(b)(5)(-b) Stress Limits

This revision changes the stress limit for "membrane longitudinal stress plus discontinuity longitudinal stress" from 4S to 3S in Subsection NC and from 4SE to 3SE in Subsection ND. This change was made in Section VIII, Division 1 in 2002 and should have been made in Section III at the same time. The change became necessary when the design factor was reduced from 4 to 3.5.



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- NB-3231(a), NB-3232.1, NB-3232.2, NB-3232.3(b)(1), NB-3236, Appendix III-2000, Appendix XIII-1182, Appendix XIV-1322(b)  
Bolting  $S_m$  Values

This revision modifies the allowable stresses for bolting to be consistent with the changes to Section II, Part D, Appendix 2, "Basis for Establishing Design Stress Intensity Values for Bolting." In implementing this change, the suggested approach is that design stresses (such as pressure stresses) will continue to use  $S_m$  based allowable stresses, but service stresses that include actual bolt loads, will utilize  $S_y$  based allowable stresses.

- Table NB-3681(a)-1  
Stress Indices for Straight Pipe

This revision provides a new stress index  $C_3'$  and a revised stress index for  $C_3$ , both for straight pipe. The stress index  $C_3'$  for straight pipe remote from welds or other discontinuities was not listed in Table NB-3681(a)-1. The note under the table states, "For indices not listed, see the note referenced at the end of the applicable line." So, according to note (5), NB-3683.3 should be used to calculate this value. But, as documented in NB-3683.3, stress indices of straight pipe should be taken from Table NB-3681(a)-1. So, NB-3683.3 points back to Table NB-3681(a)-1, and the value of  $C_3'$  cannot be found in the Code. This change provides both a new stress index  $C_3'$  for straight pipe remote from welds and other discontinuities, and proposes a change in the  $C_3$  index to be consistent with the current  $C_3$  index for flush girth butt welds between nominally identical wall thickness items.

- NB-3683.8(a)(5), NB-3683.8(b), NB-3683.8(c), NB-3683.8(d), Table NC-3673.2(b)-1 & General Note (a) with last sentence of Note (9), Table ND-3673.2(b)-1 & General Note (a)

#### Branch Connections

This revision was made to improve stress indices  $C_{2r}$ ,  $K_{2r}$  and stress intensification factors (SIFs) for branch connections with  $r/R \leq 0.5$ .


- Table NF-3312.1(b)-1, NF-3313.1, NF-3322.1(a)(1), NF-3322.1(a)(2), NF-3322.1(b)(1), NF-3322.1(c)(3)(-a), NF-3322.1(c)(3)(-b), NF-3322.1(d)(1)(-a), NF-3322.1(d)(3), NF-3322.1(d)(4), NF-3370, F-1334.3(b)(1), F-1332.7

#### Load Limits

This revision modifies load limits to be consistent with USNRC Regulatory Guide 1.124, "Service Limits and Loading Combinations for Class 1 Linear-Type Supports," Revision 2, which was issued in February 2007 and presented regulatory positions on design of Linear Supports.


These changes may impose more conservative requirements, and have not been assessed for impact on pressure boundary design governance documentation. This is identified as gap SF1-17 in Table 8.

No other changes noted in Reference [2], Appendix 6, should have any impact on safety margins as they pertain to clarifications, additional exemptions, or other issues that do not pertain to changes in design requirements.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## A.7 References

- [1] Reedy Engineering, ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components, Revision 8, May 21, 2012.
- [2] Reedy Engineering, ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components, Revision 10, Reedy Engineering, September 16, 2015.
- [3] NK21-CORR-00531-11005/NK29-CORR-00531-11397, Submission of Safety Basis Report, Bruce Power Letter, F. Saunders to R. Lojk, December 30, 2013.
- [4] NK21-CORR-00531-05976, Bruce A Units 3 and 4 Refurbishment for Life Extension and Continued Operation: ISR Safety Factor Reports, Bruce Power Letter, F. Saunders to P. Elder, June 2, 2008.
- [5] NK21-CORR-00531-12288/NK29-CORR-00531-12719, Integrated Implementation Plan for Bruce A, Bruce B, and Centre of Site, Bruce Power Letter, F. Saunders to K. Lafrenière, December 18, 2015.
- [6] NK29-CORR-00531-12884, Action Item 091413: Bruce B Legacy Registration Project Update, Bruce Power Letter, F. Saunders to K. Lafrenière, November 23, 2015.
- [7] NK21-CORR-00531-06596, Bruce A Units 3 and 4 Refurbishment for Life Extension and Continued Operation: ISR Safety Factor Reports 1, 2, 3 and 4, Bruce Power Letter, F. Saunders to K. Lafrenière, December 18, 2008.
- [8] NK21-REP-03600-00025-R001, Bruce NGS A Units 3 and 4 Global Assessment Report and Integrated Implementation Plan, Bruce Power, May 2009.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## **A.8. ASME BPVC Section VIII, Design and Fabrication of Pressure Vessels**

Significant changes to ASME Section VIII Division 1 up to the 2011 annual addenda are summarized in ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components [1][2] Appendix 7, with changes to the material requirements in Appendix 9 (there were no changes listed after 2007 in Appendix 9). Only significant changes that could imply that safety margins of existing equipment could possibly be lower than originally intended are of concern. Hence, changes related to the following are not required for consideration:

- Changes relating to QA provisions
- Changes allowing new or alternative materials
- Changes that incorporate alternative rules or calculation methods
- Changes allowing alternative test methods.


### **Summary of previous review findings (Appendix H of [3])**

#### **Bruce A Units 1 to 4 ISR findings to 2007 version of ASME VIII Division I [3]**

The original design for Class 6 pressure vessels for Bruce A was based on ASME Code Section VIII 1968, winter 1970 addenda. The existing designs for Class 6 pressure vessels have been assessed to the requirements of ASME Section VIII, Division 1, 2007 and were included in 2008 Bruce 3 and 4 Safety Factor 1: Plant Design [4]. The review found that the design complies with or meets the intent of 72 of 73 clauses of the code. The original requirements of the code were very similar to that of the modern code, except that there are additional details to elaborate on the requirements provided in the modern code, and hence it was determined that Bruce A Class 6 pressure vessel designs generally meet the intent of the modern code except for the consideration of dynamic loading as discussed below.

Article UG-22(e) of the modern code requires consideration of cyclic and dynamic reactions due to pressure, temperature and mechanical loads. This load was not specifically stated in the original Bruce A design code, and hence cyclic loads were not considered for Bruce A Class 6 components. Although the inherent conservatism in the code is adequate to cater for the cyclic and dynamic reactions at the vessel, Bruce Power is committed to evaluate Class 6 safety-related systems for cyclic and dynamic reactions (SF1-12 in Table 13 of Safety Factor 1 [3]) for steam and waterhammer loads and initiate appropriate actions if warranted. This work will include a summary of the assessments already performed to demonstrate that waterhammer loads have been consistently and continuously monitored and acted on. This issue is included in the Bruce A, Bruce B, and Centre of Site Integrated Implementation Plan from the SBR [5] as GIO-005, "Assess cyclic loads of pressure retaining components designed per ASME III and VIII." Work is expected to start on Bruce B in 2016 [5]. It will continue to be tracked in the Integrated Implementation Plan (IIP) under global improvement opportunity GIO-005.

Bruce Power has a program to review all pressure vessel registrations and submit design packages to TSSA (Technical Standards and Safety Authority) for registration of pressure vessels if required. This issue is included in the Bruce A, Bruce B, and Centre of Site Integrated Implementation Plan from the SBR [5] as GIO-001, "Improve documented design basis". The

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Bruce B Legacy Registration project is on track for completion December 2017 [6]. It will continue to be tracked in the IIP under global improvement opportunity GIO-001.

### **Summary of SBR findings - changes to ASME VIII Division I from 2007 to 2011 [3]**

This section presents findings of a review against changes made to ASME VIII Division 1 in the period from 2007 to 2011. An Updated Code Reconciliation Report "ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components" [1] was issued to Bruce Power on 2012 December 7, which reviewed and assessed the changes to several codes.

The report [1] verified that ASME Section III Division 1 has not made any significant changes that change the original design basis of any equipment.

### **Summary of current review findings**

#### **Changes to ASME Section VIII from 2011 to 2015**

Significant changes to ASME Section VIII up to the 2015 edition are summarized in ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components [2] Appendix 7, with changes to the material requirements in Appendix 9.

The following items noted in the Code Reconciliation Report ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components of 2015 September 16 [2], Appendix 7, are changes identified in ASME Section VIII since 2011, introduced in the 2013 and 2015 Editions. There is no documentation available indicating that these changes have been reviewed for potential impact on safety margins.

- Appendix 26 - 26-2(g)  
Bellows Design

The rules for bellows were developed assuming no influence from the pipe other than the axial end effect due to pressure. This assumption may not be justified in the vicinity of a major structural discontinuity where local bending or stress concentration can occur. This revision added a requirement for a minimum length of shell on each side of the bellows.

- UHX-1(b), UHX-10(h), UHX-16, UHX-17, Appendix 5 - 5-1(c), 5-1(d), 5-1(e), 5-1(f), Appendix 26 - 26-1, 26-2(e), 26-4.1(f), 26-4.1(g), 26-4.1(h)  
Heat Exchanger Rules

This revision modifies the rules for heat exchangers to assure consistency with the changes made to U-2(g) and the rules of Section VIII, Division 2.

- UHX-13.3, Table UHX-13.4-2, Table UHX-13.8.4-1, UHX-14.3, Table UHX-14.6-1  
Operating Load Cases

This revision was necessary to accommodate operating loading cases where the operating pressure range limits are negative to positive. Currently the tables assume that the range of operating pressure is from zero to a positive pressure. The zero assumption was removed to address more realistic cases, such as negative (vacuum) operating pressures.

- Appendix 26 - 26-3, 26-4.1(d), 26-4.3, Form 26-1, Form 26-1M  
Shear Stress in Bellows Under Torsion Load

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


Torsional loads usually generate high shear stresses that can be detrimental to the bellow's life. An Expansion Joint Manufacturers Association (EJMA) Standard proposed a rule limiting the shear stress due to torsion to 0.25 times the allowable stress and gave formulas for calculating this shear stress. These formulas have been validated by finite element analyses on U-shaped bellows and on one toroidal bellows. This revision added the rules in Section 4 of the EJMA Standard (Circular Expansion Joint Design) to address torsional loads in bellows.

These changes may impose more conservative requirements, and have not been assessed for impact on pressure boundary design governance documentation. This is identified as gap SFR1-18 in Table 8.

No other changes noted in Reference [2], Appendix 7, should have any impact on safety margins as they pertain to clarifications, reduced conservatisms, or other issues that do not pertain to changes in design requirements.

#### **A.8 References**

- [1] Reedy Engineering, ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components, Revision 8, May 21, 2012.
- [2] Reedy Engineering, ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components, Revision 10, September 16, 2015.
- [3] NK21-CORR-00531-11005/NK29-CORR-00531-11397, Submission of Safety Basis Report, Bruce Power Letter, F. Saunders to R. Lojk, December 30, 2013.
- [4] NK21-CORR-00531-06596, Bruce A Units 3 and 4 Refurbishment for Life Extension and Continued Operation: ISR Safety Factor Reports 1, 2, 3 and 4, Bruce Power Letter, F. Saunders to K. Lafrenière, December 18, 2008.
- [5] NK21-CORR-00531-12288/NK29-CORR-00531-12719, Integrated Implementation Plan for Bruce A, Bruce B, and Centre of Site, Bruce Power Letter, F. Saunders to K. Lafreniere, December 18, 2015.
- [6] NK29-CORR-00531-12884, Action Item 091413: Bruce B Legacy Registration Project Update, Bruce Power Letter, F. Saunders to K. Lafrenière, November 23, 2015.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## A.9. ASME B31.1, Code for Power Piping

Significant changes to ASME B31.1 are summarized in ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components [1][2] Appendix 8. Only changes that could imply that design margins of existing equipment could be significantly lower than those that would be based on a new requirement need to be considered. Hence, changes related to the following, are not required for consideration:

- Changes relating to Quality Assurance (QA) provisions
- Changes allowing new or alternative materials
- Changes that incorporate alternative rules or calculation methods
- Changes allowing alternative test methods.

### Summary of previous review findings

#### **Bruce Units 3 and 4 ISR findings [3]**

A review of the 2004 version of B31.1, Power Piping [4], was performed as part of the Bruce Units 3 and 4 Integrated Safety Review [3]. This review identified a single issue applicable to all Bruce A units, which was captured in gap SF1-12, "Cyclic loads were not considered for Bruce NGS Class 6 piping components as they were not specified in the Bruce NGS initial design codes". This item was captured in the Bruce 3 and 4 Integrated Implementation Plan [5] as part of item #IIP-70, "Evaluate Class 6 piping components for cyclic and dynamic reactions".

This finding was identified for Bruce A and is applicable to Bruce B. It is tracked in the Integrated Implementation Plan (IIP) under global improvement opportunity GIO-005.

#### **Summary of SBR findings - changes to ASME B31.1 from 2007 to 2011**

The Safety Basis Report (SBR) presents findings of a review against changes made to ASME B31.1 in the period from 2004 to 2011 [6]. An Updated Code Reconciliation Report, ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components [1] was issued to Bruce Power on 2012 December 7, which reviewed and assessed the changes to several codes, including ASME B31.1, during that period. The following is a quotation from the SBR findings

"The following items noted in Reference [1], Appendix 8, should be reviewed further to assess the potential impact on safety margins:

- 121.7.2 (A), Table 121.7.2(A) Carrying Capacity of Threaded Hanger Rods - This revision increases the carrying capacity of threaded hanger rods based on 50 ksi, and a design factor of 3.5, reduced by 25%. The previous capacities were based on an allowable stress of 12,000 psi reduced by 25%.
- 107.1(F) MSS SP-88, "Diaphragm Valves" - This revision required the designer to specify the proper pressure-temperature ratings for the system design conditions and to consider the in-service and shelf life of the diaphragm material.
- 102.3.2(C), 102.3.2(D), 104.7.2(D), 104.8.1, 104.8.2, 104.8.3, 119.10.1, 123.1.1 (E), Table A-1, Table A-2, Table A-3, Table A-4, Table A-6, Table A-7, Table A-B, Table A-9,



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Table 126.1, Appendix F Allowable Stresses - This revision updates all of the allowable stresses except for A 254 copper brazed tubing, to reduce the design factor from 4 to 3.5, for consistency with B&PVC Section II, Part D. It incorporates the provisions of Case 173-1, Alternative Maximum Allowable Stresses Based on a Factor of Safety 3.5 on Tensile Strength for ASME B31.1 Construction. This change revised the allowable stresses for almost all materials.

The last bullet above relaxes the requirement so is less conservative. Therefore, there is no impact on safety margins. No other changes noted in Reference [1], Appendix 8, should have any impact on safety margins as they pertain to clarifications, additional exemptions, or other issues that do not pertain to changes in design requirements.”

### **Summary of current review findings**

#### **Changes to ASME B31.1 from 2011 to 2015**

Significant changes to ASME B31.1 up to the 2015 edition are summarized in ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components [2] Appendix 8, with changes to the material requirements in Appendix 9.

The following item noted in Reference [2], Appendix 8, is the only change in ASME B31.1 since 2011, introduced in the 2012 Edition:

- 101.7.2, 122.1.1(I)  
Expansion Joints

This revision added exclusions for all types of bellows in Boiler External Piping (BEP).

This change noted in Reference [2] Appendix 8, will not have any impact on safety margins as it addresses an exclusion that will not result in more stringent design requirements.

#### **A.9 References**

- [1] Reedy Engineering, ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components, Revision 8, May 21, 2012.
- [2] Reedy Engineering, ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components, Revision 10, September 16, 2015.
- [3] NK21-CORR-00531-06596, Bruce A Units 3 and 4 Refurbishment for Life Extension and Continued Operation: ISR Safety Factor Reports 1, 2, 3 and 4, Bruce Power Letter, F. Saunders to K. Lafrenière, December 18, 2008.
- [4] ASME B31.1, ASME Code for Power Piping, 2010.
- [5] NK21-REP-03600-00025-R001, Bruce NGS A Units 3 and 4 Global Assessment Report and Integrated Implementation Plan, May 29, 2009.
- [6] NK21-CORR-00531-11005/NK29-CORR-00531- 11397, Submission of Safety Basis Report, Bruce Power Letter, F. Saunders to R. Lojk, December 30, 2013.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## **A.10. CSA N290.0-11, General Requirements for Safety Systems of Nuclear Power Plants**

This standard establishes the general requirements for the design, qualification, installation, operation, maintenance, inspection, and documentation of the safety systems for a water cooled nuclear power plant.

One informative Annex is part of the standard. Annex A provides guidance on plant life maintenance. The guidance covers different aspects of the program, plant baseline data, component lifetimes as well as interfaces with other plant programs. The high level review of Annex A is already included in the compliance statements associated with the corresponding clauses of the standard. It should also be noted that plant life maintenance aspects of safety systems are addressed more comprehensively in SF-2 and SF-4.

The CSA N290 series of standards includes requirements on equipment qualification, human factors, system health monitoring, maintenance program and testing in addition to those associated with the design of safety systems. The high level review of this standard focuses on those associated with design. Those requirements related to equipment qualification, human factors, system health monitoring, maintenance program and testing are addressed more comprehensively in SF-2, SF-3, SF-4 and SF-12.


The approach used is to perform an initial review against the requirements of the CNSC REGDOC-2.5.2 [1] to identify any additional requirements related to design. Subsequently a high level review of the Bruce Power safety systems design against those clauses of N290.0 that contain additional requirements is carried out. It is noted that in general the requirements established in N290.0 remain largely aligned with the REGDOC-2.5.2 requirements for safety systems design. The assessment concludes that the design of Bruce B special safety systems meets the intent of the requirements with the exceptions indicated in the text.

**Sections 1 to 3** present the scope of the standard, the reference publications and relevant definitions and abbreviations used in the standard. These are introductory sections and no assessment is deemed necessary.

**Sections 4.1 to 4.4** define general requirements related to the plant states and system operating states. As described in Section 6 of Part 2 of the Safety Report [2], there are four special safety systems designed to mitigate the consequences of both a single failure and a dual failure. The single failure constitutes a failure in a process system whereas a dual failure is a failure consisting of a single failure in a process system combined with the coincident unavailability of one of the special safety systems. The four special safety systems are:

- Shutdown System 1 (SDS1)
- Shutdown System 2 (SDS2)
- Negative Pressure Containment (NPC) system
- Emergency Coolant Injection (ECI) system

These systems are independent of each other and are in the poised state during plant operation.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

The original design envelope and design basis were documented in the system design manuals and in the Safety Reports (along with important assumptions which included capabilities that are necessary for the plant in operational states, Structures, Systems, and Components (SSCs) failure modes, event progression leading to accident conditions and methods of analyses) submitted in the application for the original operating licence. Similarly, the basis for each modification, assumptions and methods of analysis since that time were documented.

The Plant Design Basis Management Program [3] ensures that the plant design meets safety, reliability and regulatory requirements, including pressure boundary quality assurance requirements as defined in Pressure Boundary Quality Assurance Program [4]. There are no systems at Bruce Power that were specifically designed for severe accidents. As a result of Fukushima Related Action Items, Bruce Power initiated design and programmatic evaluation and subsequent changes to improve plants severe accident response. Design modifications and alternative means are being incorporated based on the results of extensive reviews and assessments of the effectiveness of existing design provisions for severe accidents. Bruce Power reports the progress and schedule for Fukushima-related enhancement activities to CNSC twice a year [5].


Bruce Power is implementing design changes to improve severe accident response. Passive Autocatalytic Recombiners (PARs) have been installed in Bruce B as described in [5], to provide mitigation of the potential buildup of hydrogen gas in the Reactor Vaults or other areas of Containment during a severe accident scenario since buildup of hydrogen in the containment system has the potential to cause an explosion, if not properly mitigated. The Severe Accident Management Guideline (SAMG) updates related to multi-unit events and irradiated fuel bay events have been completed as described in [5].

The plant states defined in clause 4.2 of N290.0-11 are not explicitly covered in the existing design documentation. A summary of the acceptance criteria applied to Bruce Power accident analysis is provided in Section 1.5 of Part 3 of the Safety Report [6]. However, the current requirements deal only with the single process system failures (Design Basis Accidents (DBAs)) and the dual failure limits, some of which would be considered as BDBAs. Severe accidents were not considered in the original design of the plant but are now being dealt with through SAMG, which is in the process of being updated via the CANDU Owners Group (COG) SAMG program. Bruce Power has committed to upgrade the Safety Report and associated safety analysis in compliance with CSA N286.7-99, to address BDBAs in deterministic safety analysis. This gap is being addressed under CNSC Action Item 090739: Safety Report Improvement Plan [7] for Bruce A and Bruce B. This is identified as gap (SF1-1) in Table 8.

The safety analyses documented in Part 3 of the Safety Report [6] conservatively assume that the safety systems and associated major components are at their minimum allowable performance standards at the time of the accident.

**Sections 4.5 to 4.8** present the requirements related to reliability, separation and independence, single failure criteria application and fail-safe design concept.

Implementing and maintaining a reliability program in accordance with RD/GD-98 is provided for in licence condition 6.1 (Fitness for Service) in PROL 18.00/2020 [8]. Bruce B uses the reliability program described in BP-PROG-11.01 [9] and in the hierarchy of its implementing procedures (listed in Appendix B of BP-PROG-11.01). Under the Equipment Reliability Program BP-PROG-11.01[9], life cycle management integrates ageing management and asset life

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

planning to optimize the service life of SSCs and maintain an acceptable level of performance and safety over the life of the plant. The implementing procedures deal with scoping and identification of critical SSCs, continuing equipment reliability improvement, preventive maintenance implementation, performance monitoring, equipment reliability problem identification and resolution, long-term planning and life-cycle management.

As presented in Section 6.1.1 of Part 2 of the Safety Report [6] each of the special safety systems is designed for an unavailability of less than  $10^{-3}$  yr/yr. The Bruce B Annual Reliability Reports over the last few years show that Bruce B special safety systems had consistently met the probability of failure on demand from all causes below  $10^{-3}$  yr/yr [10]. Changes in equipment performance data and relevant OPEX are incorporated in the update of the Annual Reliability Reports and PRA models.

Per Section 6.1.1 of the Bruce Safety Report Part 2 [2], the four special safety systems are designed to mitigate the consequences of both a single failure in a process system and a (much less frequent) dual failure consisting of a single failure in a process system combined with the coincident unavailability of one of the special safety systems. These systems are independent of each other. They also are, as much as possible, independent of any of the process systems, including the reactor regulating system.

As discussed in Part 2, Section 6.1.4.1 of the Safety Report [2], to provide protection against postulated common mode incidents, such as local fires or missiles, plant systems are separated into two groups, Group 1 and Group 2. This is to ensure that sufficient systems remain available from at least one group to provide the following safety functions:

- Shut down the reactor
- Ensure that the reactor remains shutdown
- Remove the decay heat
- Monitor the plant status

Clause 4.7 specifies the requirements related to single failure criteria. A review of similar clauses in REGDOC-2.5.2 [1] indicated that the application of the single failure criterion for the Bruce B design does not follow the newer, more restrictive, interpretations of the single failure criterion; therefore, is assessed as a gap in Table 8 (SF1-5) against clause 7.6.2 of REGDOC-2.5.2.

Clause 4.8 requires that, as far as practical, the safety system components be designed to be fail-safe for credible failure modes. As discussed in Section 1.3.2.3 of Part 2 of the Safety Report [2], diversity of functions (e.g., process and neutronic measurements) for important control and safety systems is used such that a common fault in one type of component cannot cause complete failure of the function. In addition, to the extent possible, equipment is designed to fail safe on loss of electrical power (e.g., shutoff rods drop when power to their clutches is lost). Similarly, pneumatic instruments and components such as air-operated valves are designed to be fail-safe to the extent possible. Self-actuating devices are employed where possible. Where such choice is available, special safety system components are designed such that the most likely failure modes are in the fail-safe direction. It is recognized that in the original design this approach has been followed to the extent practicable. Since there are exceptions to this design rule (e.g., as documented in Design Guide Supplements) this is

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

assessed as a gap in Table 8 (SF1-20). The same gap was identified in the review against a very similar requirement in clause 7.6.3 of REGDOC-2.5.2.

**Sections 4.9 to 4.13** address the requirements related to safety support systems, pressure-retaining SSCs, instrumentation, control and monitoring, equipment qualification and dynamic piping effects. Human factors and fire protection requirements are presented in **Sections 4.14 and 4.15**, respectively. Bruce B support systems meet the intent of these requirements, except as indicated in the text below.

Operational Safety Requirements for Bruce B Electrical System [11] present the safety limits, applicable analysis and surveillance requirements for Bruce B Electrical Power Systems.

The instrument air system was designed on a unit basis, with one complete system per reactor unit. The individual air systems are provided with air receivers with a large enough capacity to supply air during a Class IV power failure until Class III power is available (Section 11.2.1.2 of the Bruce B Safety Report Part 2 [2]).

Licence condition handbook for Licence condition 5.2 (Pressure Boundary) [12] requires the licensee to implement and maintain a pressure boundary program to ensure compliance with CSA N285.0 [13].

The Bruce B instrumentation and control design philosophy is summarized in the Safety Report (Part 2, Section 7.1.6) [2]. The instrumentation and control systems are designed to a large variety of detailed requirements, depending on their function, importance and physical environment. Each process and nuclear measurement loop that is essential for the operation of a special safety system is redundantly designed (duplicated or triplicated), such that a single loop component or power supply failure will not incapacitate or spuriously invoke operation of the special safety system (Section 6.1.2 of Part 2 of the Safety Report [2]). The Operational Safety Requirements for special safety systems, i.e., shutdown systems [14], containment [15], and emergency coolant injection system [16] specify the testing and monitoring requirements required to verify that the system meets its performance and reliability requirements.

Clause 4.11.2.13 requires the design to minimize unavailability due to calibration and the time during which an instrument loop is unavailable due to calibration to be included in the unavailability of the loop. Bruce B design documentation does not explicitly reflect this requirement; therefore, it is assessed as a gap under SF1-5 in Table 8.

As described in Section 6.6 of Part 2 of the Safety Report [2], a computer system is used to monitor the state of the special safety systems.

The systems subjected to a harsh environment following some design basis accidents are protected through environmental qualification of essential equipment. The environmentally harsh conditions have been evaluated for all DBA categories considered and have been documented in the Room Conditions Manual [17]. The results of this program are documented in the Bruce B Design Guide for Environmental Qualification of Safety Related Equipment [19], which contains the detailed requirements for each of the systems subject to environmental qualifications.

Per the Bruce B Design Guide on Seismic Qualification of Safety Related Equipment [20] (see Section 6), Bruce B follows the requirements from the N289 series of standards.



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Bruce B design meets the aging requirement, as documented in the Equipment Reliability Program [9]. The program is to ensure that all systems important to safety meet their design intent and performance criteria. Current SSC life cycle and ageing management governance and processes meet the current regulatory requirements. Bruce Power is utilizing an Asset Management approach to ensure safe plant operations throughout its life cycle. Under the Equipment Reliability Program [9], life cycle management integrates ageing management and economic planning to optimize the service life of SSCs and maintain an acceptable level of performance and safety over the life of the plant.

Clauses 4.12.4 and 4.12.5 require the SSCs credited to perform their functions during AOOs, DBAs and BDBAs are protected against debris and contaminants initiated by that event and are assessed for their potential to perform under the expected environmental conditions. Since the current design documentation does not consider internal events as leading to AOOs, DBAs and BDBA this is assessed as a gap. The same gap was identified in the review against similar requirement in clause 7.4.1 of REGDOC-2.5.2. This gap is included under SF1-1 in Table 8.

The Bruce B design includes protection against common mode events as described in Section 2.5 of Part 2 of the Safety Report [2]. This covers the following:

- Earthquakes
- Seismic Design
- Missile Protection
- Protection Against Dynamic Effects Associated with the Rupture of Piping

Bruce B complies with the human factors related requirements. Bruce Power has a Human Factors Engineering Program Plan, DPT-PDE-00013 [18], which outlines the procedure for applying Human Factors site wide.

Bruce Power's reviews of the updated version of CSA N293-12 (Fire Protection for Nuclear Power Plants) concluded that the existing fire protection plans, programs, procedures and response capabilities are generally in full compliance with the standard. Administrative and editorial updates to documentation will be required to change references to the revised standard and, in some cases, to add the new terminology it contains. These actions will be completed in a timely manner in accordance with Bruce Power's document change control procedures. No transition plan is required. The administrative and editorial documentation updates to Fire Protection plans, programs and procedures to address the requirements of the 2012 edition of this standard are targeted for the end of November 2017 [20].

**Sections 4.16 to 4.20** cover the requirements related to System Health Monitoring, operability, maintainability, maintenance program and testing.

Bruce B has extensive testing programs to demonstrate that the special safety systems meet their ongoing reliability requirements. Section 03.5 of the Bruce B Operating Policies & Principles (OP&P) [22] specifies that the testing program is required on any system which is not normally operating but is required to function, in the event of a system failure, to control reactor power, cool the fuel, or contain radioactivity. The testing programs for these systems are consistent with reliability objectives established in system design.



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

The process for development of Life Cycle Management Plans for Structures, Systems and Components is outlined in Life Cycle Management for Critical SSCs [23]. The relevant technical information (e.g., age-related degradation mechanisms, replacement and major overhaul tasks/frequencies, current conditions, etc.) from the Technical Basis Assessments (TBA), Performance Monitoring Plans (PMP), Health Reports and other data sources and use this information to document the recommended long-term mitigation options for the SSCs. The recommended options are then included in the Asset Life Projections & Options document (ALP&O). The ALP&O process adds to the recommended long-term options key information needed in business strategy decisions. Critical components are listed on the Performance Monitoring Equipment List within the approved Performance Monitoring Plan [24][25][26] and meet the criteria specified in Component Categorization [28]. Life Cycle Management is one of the key elements of BP-PROG-11.01, Equipment Reliability Program [9]. System health monitoring, reporting and management processes are extensively discussed in Safety Factor 2.

Bruce B safety system instrumentation provides for clear and unambiguous indication of the necessity for operator action which are described in operating manuals and supporting documentation. As described in Section 7.1.6 of Part 2 of the Safety Report [2], the instrumentation and control systems are designed to a large variety of detailed requirements, depending on their function, importance and physical environment. However, all the systems are designed to the following general criteria:

- The maximum practical amount of automatic control is incorporated in the design to allow the station to be operated safely with a minimum staff and to leave operators free for higher level monitoring of overall unit status. The operator can readily intervene in the operation of the automatic control systems.
- Adequate, comprehensive information is designed to be readily available at all times to allow the operator to assess the status of the unit quickly and to intervene with manual actions if necessary.
- Equipment is designed for a minimum of regular maintenance. Any necessary maintenance operations are kept as simple and speedy as possible.
- The instrumentation and control systems are designed for a very high reliability and availability, both to maximize plant availability and for safety. This reliability is achieved through a combination of component selection and design and through redundancy.
- The control systems are designed to make the unit as tolerant as possible to expected and unexpected transients, in order to prevent unnecessary unit outages.
- Where possible, the control systems are designed to prevent or minimize damage to equipment.

Bruce B meets the intent of the operability requirements as described in the Operational Safety Requirements (OSRs) for each of the special safety systems. The conditions of operability are defined and explained for each category of mechanical equipment and related instrumentation. The system/component level testing and monitoring required to verify that the subsystem/component meets its performance and reliability requirements are specified in surveillance requirements. These requirements specify minimum hardware operability, parameter values, and automatic initiation setpoints consistent with the Safety Analysis Limits.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

In addition, Safety Related System Impairments Manual describes the provisions in place and action(s) to be taken when such systems or their components are found to be inoperable or impaired.

In general, safety system design allows for maintenance to ensure compliance with their design basis and performance requirements. Section 03.5 of the Bruce B Operating Policies and Principles (OP&P) [22] specifies that the testing program is required on any system which is not normally operating but is required to function, in the event of a system failure, to control reactor power, cool the fuel, or contain radioactivity. The testing programs for these systems are consistent with reliability objectives established in system design as required in clause 4.18.1.


All systems considered to have significant radiological implications for station personnel during operation or maintenance were reviewed in the design phase. Design provisions are also implemented to minimise the radiation doses to workers as well as access to components and systems that require periodic inspections per N285.4, N285.5 and N287.7. As much of the equipment (both safety and process) as possible was placed outside containment to allow on-power maintenance and testing. All safety system equipment that requires testing or maintenance is accessible on-power from outside containment (e.g., SDS1 and SDS2 instrumentation, poison tank sampling, shutoff rod drives, etc.). In general, for systems or structures that cannot be tested, inspection or monitoring programs are in place. Surveillance, maintenance and testing of safety systems are addressed through BP-PROG-11.01 Equipment Reliability [9], BP-PROG-11.04 Plant Maintenance [27] and BP-PROG-00.04 Pressure Boundary Quality Assurance Program [4] and their supporting procedures. These programs are addressed extensively under SF-2.

The special safety systems and standby safety support systems are tested on a regular basis to ensure that they will be available to operate if called upon. The systems are designed to facilitate testing of all components, either as a system or in a series of overlapping component tests. Test frequencies are established to ensure that the systems meet defined reliability requirements. By testing the components of these systems at known frequencies, the actual availability can be monitored and compared against the expectation.

The Bruce B design meets the requirement for periodic testing of the entire channel of instrumentation logic. The channelized logic at Bruce B allows for testing of the instrumentation all the way from the sensing device to the actuating device. The majority of the systems are such that the physical equipment being actuated cannot be tested on line. For example, the SDS1 shutoff rods can, and are, dropped partially into the core to demonstrate that they are physically capable of moving. They are caught before actually entering the core to any significant degree so as not to induce unnecessary flux tilts. On the other hand, it is not possible to inject poison from SDS2 into the core during on-power testing. Similarly, Emergency Coolant Injection (ECI) is tested up to the point of actually injecting water into the core. Full testing of the shutdown system capability is periodically carried out when entering planned shutdown.

Each shutdown system was designed to allow on-power testing to demonstrate that it will meet its unavailability targets. Furthermore, Bruce Power is committed to a maintenance and testing program as specified in the OP&P Section 63.1 Shutdown System Availability [22].

With respect to commissioning requirements in clause 4.20.4, Bruce B Safety Report, Bruce Power Design Manuals (DMs) and OSR do not explicitly state tests should be done prior to first

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

criticality of the reactor. With regards to systems modifications, the requirements for commissioning planning, commissioning specification, execution and reporting are defined in Commissioning Modifications and Projects [29].

**Sections 4.21 and 4.22** presents the requirements related to sharing within a unit and between units. Bruce B meets the intent of these requirements.

Special safety systems are physically separated from process systems and there is no instrumentation sharing between safety and process systems. Special safety systems are independent of the process systems and perform no process functions. As described in Section 6.1.2 of Part 2 of the Safety Report [2] each process and nuclear measurement loop that is essential for the operation of a special safety system is redundantly designed (duplicated or triplicated), such that a single loop component of power supply failure will not incapacitate or spuriously invoke operation of the special safety system.


With respect to sharing between units, Bruce B design does not fully meet the requirements as documented in [30]. The early design philosophy used for the multi-unit stations in Canada was to share some of the systems that were important to safety. For example, the containment systems are shared among the four units as well as the Emergency Water System (EWS) is common to all four units. The accident analyses and the PRA recognize the shared functions and have shown that the design is adequate to meet Bruce Power's safety goals and all of the regulatory requirements in Canada. Therefore, Bruce B design meets the intent of this requirement.

**Section 4.23** presents the requirements for design documentation, SOE documents, operational documents, history dockets and operational history.

A general design description of the plant is provided in Parts 1 and 2 of the Bruce B Safety Report [2]. The system Design Requirements were originally specified as part of the System Design Manuals and were provided to the AECB. Design Requirements for modifications are prepared according to BP-PROG-10.02 Engineering Change Control [31].

The design documentation follows well established processes and procedures as described in Design Management [32]. This procedure specifies the design activities and outputs that define and manage the Plant Design Basis such that the nuclear operating stations can operate safely and reliably for the duration of their design life. Design Management relies upon the implementing procedures of BP-PROC-00363, Nuclear Safety Assessment [33] to ensure nuclear safety requirements are incorporated into the design. Under the Equipment Reliability Program [9], life cycle management integrates ageing management and economic planning to optimize the service life of SSCs and maintain an acceptable level of performance and safety over the life of the plant. As described in [23] the author of a Life Cycle Management Plan (LCMP) reviews relevant documentation including design requirements and design descriptions when preparing or revising the LCMP. In addition, design changes described in design documentation can trigger a review of LCMPs.

Part 1 of the Safety Report provides an introduction and general description of the plant and site, including environmental conditions [2]. Plant components and systems are described in Part 2 of the Safety Report [2]. The deterministic safety analysis is documented in Part 3 of the Safety Report [6]. The Safety Report has been updated periodically, with the latest update performed in 2011. The Bruce B Probabilistic Risk Assessment (PRA) includes Level 1 and

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Level 2 analyses. The Bruce B PRA model, abbreviated as BBRA, is the result of a continuing process of updates and improvements that began in 1999 with the development of the original BBRA model by Ontario Hydro. Since then, the Bruce B PRA and models have been updated to reflect the plant as built and operated and as required. A full summary of the changes made to the BBRA model since its inception is provided in Appendix F of the latest Bruce B Risk Assessment (BBRA) Level 1 At Power Model Integration Report including Emergency Mitigation Equipment (EME) (report B1401/RP/004 R01, July 18, 2014) [34]. The list of current Bruce PRA analyses and corresponding guides is presented in Safety Factor 6. The Bruce B design documentation also includes Hazard Assessments as documented in Safety Factor 7.

Issues relevant to the adequacy of design documentation are considered gaps and identified as SF1-8 to SF1-11, SF1-13, SF1-14, SF1-16 through SF1-21, and SF1-23 as presented in Table 8. Therefore, these gaps are not repeated.

Bruce Power has introduced Operational Safety Requirements (OSRs), which essentially provide the same functions as Operational Limits and Conditions (OLCs). These limits are based upon the up to date safety analysis and also incorporated in OP&Ps and operating manuals.

Bruce Power is implementing an SOE program which will provide the comprehensive identification of all operating limits and conditions in compliance with the requirements of CSA N290.15. As described in Safety Factor 5, Bruce B has completed its baseline SOE project which consisted of documenting the limits and conditions derived from the safety analysis in OSRs, completing the corresponding Instrument Uncertainty Calculations (IUCs), and performing Gap Assessments to verify that the requirements are completely and accurately reflected in the station operating documentation. Any outstanding issues will be transferred to the maintenance phase of SOE sustainability, which is currently under development. Bruce Power is moving from Operating Policies and Principles (OP&P) towards the implementation of a Safe Operating Envelope (SOE) program, which will provide the comprehensive identification of all operating limits and conditions in compliance with the requirements of CSA N290.15. Further details are given in Safety Factor 5.


#### **A.10           References**

- [1]    CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants, May 2014.
- [2]    NK29-SR-01320-00001-R005, Bruce B 2012 Safety Report – Part 1: Plant and Site Description and Part 2: Plant Components and Systems, Bruce Power, August 2012.
- [3]    BP-PROG-10.01-R009, Plant Design Basis Management, Bruce Power, December 4, 2014.
- [4]    BP-PROG-00.04-R022, Pressure Boundary Quality Assurance Program, Bruce Power, May 27, 2015.
- [5]    NK29-CORR-00531-12635, Bruce Power Progress Report No. 7 on CNSC Action Plan – Fukushima Action Items, Bruce Power Letter, F. Saunders to K. Lafrenière, August 7, 2015.
- [6]    NK29-SR-01320-00002-R005, Bruce B 2011 Safety Report, Part 3: Accident Analysis, Bruce Power, November 2011.

 <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- [7] NK21-CORR-00531-10774/NK29-CORR-00531-11155, Action Item 090739: Safety Report Improvement Plan for Bruce A and B, Bruce Power Letter, F. Saunders to R. Lojk, November 20, 2013.
- [8] NK21-CORR-00531-12136/NK29-CORR-00531-12546/E-DOC 4723908, Nuclear Power Reactor Operating Licence, Bruce Nuclear Generating Stations A and B, PROL 18.00/2020, Canadian Nuclear Safety Commission, May 27, 2015.
- [9] BP-PROG-11.01-R005, Equipment Reliability, Bruce Power, December 16, 2015.
- [10] NK29-CORR-00531-13197, Bruce B Annual Reliability Report - 2015, Bruce Power Letter, F. Saunders to K. Lafrenière, April 28, 2016.
- [11] NK29-OSR-53000/55000-0001-R000, Operational Safety Requirements for Bruce B Electrical System, June 2009.
- [12] NK21-CORR-00531-12135/NK29-CORR-00531-12545/E-DOC 4659316, Licence Conditions Handbook, LCH-BNGS-R000, Bruce Nuclear Generating Station A and Bruce Nuclear Generating Station B Nuclear Reactor Operating Licence, PROL 18.00/2020 (Effective: June 1, 2015), Canadian Nuclear Safety Commission, May 27, 2015.
- [13] CAN/CSA N285.0-12, General Requirements for Pressure-Retaining Systems and Components in CANDU Nuclear Power Plants, 2012 (Update 1, 2013).
- [14] NK29-OSR-63720-63730-00001-R001, Operational Safety Requirements for Bruce B Shutdown and Maintenance Cooling Systems, November 2013.
- [15] NK29-OSR-34200-00001-R001, Operational Safety Requirements for Bruce B Containment System, November 2013.
- [16] NK29-OSR-34340-00001-R002, Operational Safety Requirements for Bruce B Emergency Coolant Injection System, May 2013.
- [17] B-STQ-03651-10001-R001, Environmental Qualification Room Conditions Manual, Bruce Power, November 15, 2001.
- [18] DPT-PDE-00013-R008, Human Factors Engineering Program Plan, Bruce Power, June 16, 2014.
- [19] NK29-DG-03650-003-R007, Environmental Qualification of Safety Related Equipment, Units 05678.
- [20] NK29-DG-03650-002-R007, Seismic Qualification of Safety Related Systems, Units 5678.
- [21] B-REP-00701-29NOV2013-059-R000, Assessment of Fire Protection at Bruce Power, Bruce Power, November 29, 2013.
- [22] BP-OPP-00001-R019, Operating Policies and Principles – Bruce B, Bruce Power, July 14, 2015.
- [23] BP-PROC-00400-R002, Life Cycle Management for Critical SSCs, Bruce Power, July 5, 2013.



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- [24] DPT-PE-00008-R006, System and Component Performance Monitoring Plans, Bruce Power, September 11, 2015.
- [25] DPT-PE-00009-R002, System and Component Performance Monitoring Walkdowns, Bruce Power, September 30, 2015.
- [26] DPT-PE-00010-R006, System Health Reporting, Bruce Power, August 27, 2013.
- [27] BP-PROG-11.04-R006, Plant Maintenance, Bruce Power, November 27, 2013.
- [28] BP-PROC-00666-R004, Component Categorization, Bruce Power, October 1, 2015.
- [29] BP-PROC-00615-R001, Commissioning Modifications and Projects, Bruce Power, September 20, 2013.
- [30] NK21-CORR-00531-11005/NK29-CORR-00531-11397, Submission of Safety Basis Report, Bruce Power Letter, F. Saunders to R. Lojk, December 30, 2013.
- [31] BP-PROG-10.02-R010, Engineering Change Control, Bruce Power, November 12, 2014.
- [32] BP-PROC-00335-R007, Design Management, Bruce Power, July 30, 2015.
- [33] BP-PROC-00363-R003, Nuclear Safety Assessment, Bruce Power, January 24, 2013.
- [34] B1401/RP/004-R01, 2014 Bruce B Risk Assessment (BBRA) Level 1 At-Power PRA Model Integration Report (including Emergency Mitigating Equipment (EME)), Bruce Power, July 18, 2014.



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## **A.11. CSA N290.2-11, Requirements for emergency core cooling systems of nuclear plants**

This standard covers the design, qualification, installation, operation, maintenance, inspection, and documentation of the emergency core cooling (ECC) system for a water cooled nuclear power plant.

A high level review of the Bruce Power design against the requirements in this standard is performed. This high level review is focused on the applicable requirements for the Emergency Coolant Injection System, which performs the emergency core cooling function for Bruce B reactors. The assessment concludes that the design of Emergency Coolant Injection System meets the intent of the requirements with the exceptions indicated in the text.

**Sections 1 to 3** present the scope of the standard, the reference publications and relevant definitions and abbreviations used in the standard. These are introductory sections and no assessment is deemed necessary.

**Section 4** lists the functional requirements for emergency cooling systems. The Emergency Coolant Injection (ECI) System is a special safety system. Its purpose is to adequately refill the primary heat transport (PHT) system and keep it filled after a loss-of-coolant accident (LOCA), thus establishing emergency core cooling. The system provides one of the long term heat sinks for emergency core cooling.

The system meets the functional and design requirements as defined in the system design manual [1] and as summarized in Section 6.4.2 of Part 2 of the Safety Report [2]. Its functional requirements are specified in Sections 1.0 and 2.1 of [1].

In summary [1], the system establishes conditions for heat rejection from the PHT system following a LOCA by:

- A timely response to a loss of coolant inventory in the PHT: detection of significant loss of inventory and “automatic” initiation of mitigating actions in a timely fashion.
- Ensuring a coolable geometry: pressure tube integrity (pressure/temperature characteristics). For large breaks this requires moderator subcooling during tube sagging.
- Providing an adequate inventory of coolant medium with sufficient subcooling.
- Providing a means of transporting heat from the fuel to a heat sink.
- Providing a means of heat rejection for a large LOCA where the primary heat sinks are ineffective.

The ECI is designed to initiate automatically for all postulated breaks down to a size when the make-up from the D<sub>2</sub>O feed system allows sufficient time for manual initiation by the operator. As a design requirement, no operator actions need to be credited within the first 15 minutes of a clear signal indicating the required action.

Heat transfer to the steam generators, the moderator, etc., may be credited as part of the assurance of adequate heat sinks [1]. In conjunction with reactor shutdown and the moderator system the ECI system ensures that:

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- with an unimpaired containment, the single failure release limits are not exceeded for all postulated LOCAs.
- with a coincident containment impairment, the dual failure release limits are not exceeded for all postulated LOCAs.

The required duration of the long term recovery stage of ECI operation is assumed to be three months. Per [1] the systems and components needed to ensure long term continuous ECI operation are adequately seismically qualified.

**Section 5** defines the ECC System Requirements. The specifics of system automatic and manual operation, instrumentation and control, service loads, containment boundary, chemistry and inventory control, loop isolation, core reactivity, venting, draining and leakage collection are addressed below.

#### **Section 5.1 General & Section 5.2 System Operation**

As described in Section 6.4.4 of Part 2 of the Safety Report [2], the ECI system is poised during normal operation of the station and is activated automatically when a loss of coolant accident is detected in any unit.

Bruce B meets the requirement for crediting the least effective shutdown system by using accident analyses assumptions that assume the negative reactivity insertion characteristics of the slowest of the shutdown systems. Section 3.2.3.1.1 of Part 3 of the Safety Report [3] indicates that the shutdown action by the least effective SDS is credited in the safety analysis of LOCA.


Towards the end of the high pressure injection operation mode, as accumulator injection proceeds, the levels in the water tanks drop and the gas expands and decreases in pressure. When the water tanks are close to empty, the downstream isolation valves close, preventing any gas from entering the HT system.

The ECI system design takes into account the potential sources of gas intrusion. Air volume limits are specified for various components of the system (e.g., H<sub>2</sub>O/D<sub>2</sub>O separator) and air injected into the system and into the heat transport system is minimized (e.g., by delay in closing of the drain and vent valves in the H<sub>2</sub>O/D<sub>2</sub>O separator). For details see Reference [4].

Regarding the manual blocking requirements, per Section 2.1.1.3 of [1], under the blocked state, the ECI will not act automatically but can be manually initiated from the main control room. The ECI is required to be blocked for a unit to prevent spurious injection of light water into the heat transport system when the unit is shutdown for maintenance. The ECI is blocked only when the primary heat transport temperature of the particular unit is 90 °C or less. Only the unitized portion of the ECI corresponding to the unit needs to be blocked, while the rest of the system will remain in the poised state.

Also per Section 2.1.1.3 of [1], the ECI system is capable of being recalled within the required recall time to refill the heat transport inventory in the event that the PHT coolant inventory cannot be maintained or on loss of maintenance cooling capability.

The system's reliability requirements and I&C requirements specified in Sections 2.12 and 2.15, respectively, of the ECI design manual [1] ensure ECC detection is reliable and diverse to ensure timely initiation of the ECC system injection.

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Many ECI system actions are automated (see Section 3.2.2 of [1]). For example, coolant injection (see Section 3.1.2.1 of [1]), depressurizing the reactor coolant system (see Sections 2.12, 3.1.1.1 and 3.1.2.7(2) of [1]), operation of equipment required for the recovery mode (see Section 3.1.2.5 of [1]).

Design measures (e.g., conditioning signals, selection of trip setpoints) are in place to prevent spurious operation in all operational states; see reference [1] for details. Post LOCA design requirements are in place (Section 2.9.6 of [1]) to prevent unacceptable releases outside containment after a LOCA.

Controls are also provided to allow manual initiation of the ECI (see Sections 2.15, 2.16, and 3.1.2.1 of [1]).

Sections 3.2.2.3 and 3.2.2.4 of [1] provide information in support of meeting the short-term and long term requirements of clauses 5.2.5 and 5.2.6 of the N290.2-11 standard with respect to the conditions (e.g., temperature, flow rate, pressure) needed to ensure adequate cooling and performance of the system.

Per Section 3.3.6.9 of [1], travelling screens have been provided to remove debris from water entering the service water pump intakes to prevent heat exchanger blockages.

Clause 5.2.6.4 of N290.2-11 requires the ECI system to be designed in such a way that credit for maintenance is not required during its mission time. Although not explicitly reflected in the design documentation, the design provisions ensure the system meets the intent of this requirement. As a special safety system, it is a licensing requirement to periodically demonstrate the ECI system availability of 99.9% (or unavailability be no more than  $1 \times 10^{-3}$ ). Therefore, every component required for automatic response to a LOCA has to be tested including the initiating logic. During testing, the ECI system remains available, although a temporary reduction in redundancy and an increase in susceptibility for spurious initiation may occur for the duration of the test.


### **Section 5.3 Instrumentation and Control**

The ECI system extends over three areas of control – coolant injection area (each unit), ECI supply tanks area and ECI recovery sump and pumps area as described in the Emergency Coolant Injection System Instrumentation and Control Design Manual [5].

Per Section 2.2.1.1 of [1], the ECI system monitors sufficient heat transport system conditions and other parameters to detect a loss of PHT liquid inventory or a shrinkage of PHT coolant that is beyond the make-up capability of the PHT Pressure and Inventory Control System. PHT System Pressure setpoint chosen had to be high enough to provide a considerable margin of assurance that there will be negligible fuel and pressure tube damage, but low enough to decrease the risk of spurious injection. In addition, conditioning signals are required to minimize the probability of a spurious injection, but must also cover all break sizes and break locations. Conditioning parameters are reactor vault high pressure and temperature, moderator high level, PHT system sustained low pressure.

### **Section 5.4 Usability Requirements Specific to Manual Operation**

As with all safety systems, once initiated their automatic functions, no single operator action can stop the ECI system operation. It is noted in that once an initiation signal comes in to the

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

initiation logic, the system will automatically activate unless the ECI blocking signal is also in. However, for such a signal to be in, there would be a violation of the Operating Policies and Principles since the reactors are not allowed to operate with the heat transport system to be above 90°C unless the ECI is available. Compliance with the OP&Ps is mandatory and is an essential part of operator's training. In order to inappropriately or unintentionally defeat the ECI function, the blocking signal would have to be put in place between the time of first indication of a problem and the initiation of the ECI. This time period is very short for those accidents with the highest fission product releases, so the probability is so small that the requirement can be considered as met.

Once a LOCA has been detected and the injection has occurred and the need for decay heat removal has passed, the ECI system equipment may be returned to normal by operator action only. Per direct interfacing system requirements (Section 2.3.2.1 of [1]) the Safety System Monitoring Computers provides ECI information to the operator.

### **Section 5.5 Service Loads and Water Hammer Loads**

Implementation and maintaining a pressure boundary program is a licence condition 5.2 of the current Bruce Power licence [1]. As part of the licence renewal application process, an Implementation strategy for N285.0 (2012 Updates 1 and 2) is detailed in Licence Condition 5.2 of the LCH for Bruce B [6].

Specific water hammer analyses demonstrating that pressures in, and pressure differentials across, the system piping do not exceed design values when the system is employed, are performed. The maximum limits in ECI OSRs [4] are determined by the results of water hammer analysis that ensures the integrity of the ECI system piping.

### **Section 5.6 Containment Boundary**

The containment envelope surrounds the four reactor vaults, the fuelling duct, the central fuelling area, the east service area, the two pressure relief ducts and the pressure relief valve manifold (Section 2.0 of Containment OSRs [7]). Per Section 4.0 of [7] various pipes and ducts penetrate the containment envelope or vacuum building boundary and communicate with the protected volumes. The portions of these flow paths up to and including the redundant isolation device are called the containment extensions. Most of the extensions are closed and are simply a part of the overall containment envelope or vacuum building boundary. Some extensions are (or may be) open during normal operation and these are isolated after the accident. Potentially open flow paths communicating with the containment atmosphere are provided with automatic isolation on high pressure or high activity. Potentially open flow paths communicating with water in the vacuum building are isolated by the operator-initiated signal to the motorized valves (i.e., the vacuum building active drainage lines). The isolation of penetrations that do not communicate with the containment free volumes (e.g., piping of a system located within containment) is addressed in the OSR for that system.

Per Section 1.2.5 of [4], there is a Leakage Mitigation Subsystem that includes provisions which ensure that there is no significant additional public dose resulting from leaks from equipment located in the ECIS equipment room during post-LOCA operation. The subsystem also prevents flooding the ECIS pumps should a significant leak develop during the ECIS mission time. Post-accident, the Leakage Mitigation Subsystem collects any leakage into the ECIS

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

equipment room and returns it to containment. The operability of this subsystem is defined by mechanical hardware characteristics only (e.g., valve positions).

Per Section 2.9.3 (Containment Boundary Requirements) of [1], the ECI system penetrates the containment envelope and therefore forms an extension to the containment envelope. The portions of the system that form an extension to containment may contain radioactivity after a LOCA. Leakage from the ECI system is monitored. Process parameters which signify leakage are alarmed to verify the integrity of the ECI pressure boundary in the poised mode and to prevent unacceptable releases outside containment after a LOCA.

### **Section 5.7** Chemistry, Water Quality, and Inventory Management

Bruce B meets the requirements related to water chemistry, quality and inventory management. A chemistry control program for the Emergency Coolant Injection (ECI) System and the Emergency Storage System (ESS) is employed with the objective to minimize the corrosion of the carbon steel and aluminum components. The chemistry control is achieved by maintaining an alkaline environment and a low dissolved oxygen concentration for the carbon steel components and maintaining neutral pH and low chloride levels for the aluminum components. The ESS vacuum building storage tank is included in ECI chemistry control, as it is connected with the low pressure ECI loop. The chemistry control regime takes into account the different types of makeup water for ECI (demineralized water) and ES systems (lake water). The ECI system chemistry control regime is subdivided further to two different chemistry control specifications based on the difference in its construction material (carbon steel and aluminum). Hydrazine is added to the system to inhibit carbon steel corrosion by scavenging dissolved oxygen from the water and to promote the formation of magnetite. For aluminum components, chemistry is controlled by maintaining the pH in the specified range and low chloride levels by draining and refilling the tank as required to minimize pitting corrosion, and by monitoring water quality by grab sampling and chemical analysis. For more details see reference [8].

Water inventory in the ECI recovery sump ensures adequate supply for the recovery phase. The ECI pumps are located in a room next to the recovery sump (the recovery sump is inside containment on the south side of the east service area duct). The four pumps are also connected to the recovery sump by a common suction line with branch pipes for each recovery pump. A motorized valve at the suction of each pump normally isolates the pump from the recovery sump. The pumps receive electric power from the Class III buses. The pumps discharge to the common supply header through two of three heat exchangers and a heat exchanger bypass line. A check valve station prevents reverse flow into this part of the system and overpressurization during high pressure injection from the accumulator tanks. The heat exchangers cool the injected water when the pumps are in the recovery mode. They are supplied with cooling water from the Unit Low Pressure Service Water Systems. Unit Low Pressure Service Water System is described in Section 11.1.3.1 of Part 2 of the Safety Report. As discussed in Section 11.5.4 of Part 2 of the Safety Report [2] chlorination is used to provide protection against zebra mussels. It prevents the mussels from attaching themselves to water intake pipes, thereby restricting the water flow. The service water systems, low pressure water, and common service water systems are usually chlorinated when the presence of zebra mussels is established within 80 km (50 miles) of the Bruce site and the lake water temperature exceeds 12°C (53.2°F). As presented in Section 11.1.1 of Part 2 of the Safety Report, water for all purposes is drawn from Lake Huron through a common intake channel. Screens are provided at pump intakes to remove debris.



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## Section 5.8 Reactor Coolant System Depressurization

The crash cooldown reduces the stored heat in the secondary side and further accelerates the Heat Transport System depressurization, thereby increasing the rate of injection. Per Section 3.1.2.7 of [1], the safety relief valve (crash cooldown) logic includes both manual initiation and automatic actuation.

## Section 5.9 Heat Sink for Small Breaks

For small breaks, the injection flow rate into the PHT system may be as low as 68 l/s. Extended operation of the pumps at such low flow rates are not recommended. In order to cope with these situations, recirculation loops have been provided which guarantee a minimum recommended flow through each operating pump and provide cooling during pump operation near the shutoff head. For more details, see Section 3.1.1.5 (Common Low Pressure Injection and Recovery Subsystem) of [1]. For small breaks the predominant heat sink is the steam generators.

## Section 5.10 Loop Isolation

The Bruce B Heat Transport System consists of a single coolant loop with concurrent east-to-west and west-to-east flow through alternating fuel channels via four reactor inlet headers and two reactor outlet headers. As shown in Figure 6-5 of Part 2 of the Safety Report [2] the ECI system is connected to two inlet headers (one east and one west) and both outlet headers. By design, the Emergency Coolant Injection (ECI) system does not require loop isolation to ensure successful operation; therefore the requirements for loop isolation in this clause are not applicable to Bruce B reactors.

## Section 5.11 Core Reactivity

Due to the specifics of CANDU reactor design the impact of light water addition to the reactor coolant will decrease the core reactivity during ECI initiation (downgrading the coolant isotopic purity). This will act to increase core subcriticality due to the negative reactivity effect of downgrading the coolant isotopic purity once light water from the ECI system enters the HT system and subsequently the moderator. Per [1], for in-core breaks the negative reactivity insertion effect of light water from ECIS displacing D<sub>2</sub>O moderator is credited in the safety analysis.

## Section 5.12 Venting and Draining

In general, Bruce B meets the intent of the requirement that the ECC system be provided with properly sized high-point vents and low-point drains, which are described in the ECI Design Manual [1]. Since the requirements in clause 5.12.5 for providing a drain between isolation and check valves where hazardous fluids could be trapped is not explicitly reflected in the design documentation, this is assessed as gap in SF1-14 in Table 8.

The high pressure ECI system piping is well vented through vents added at significant high points. Vents are provided at significant high points of the common supply header and the accumulator discharge line. Before Unit 6 criticality a level survey was taken of the common supply header and new vents were added at significant high points. Vents are also provided on testable check valves 3434 NV155 to NV158 and NV340, NV341 and the unit gate valves 3433 MV2, MV3, MV101 and MV102 to vent the valve bonnets. The amount of air remaining in the high pressure piping after venting or after maintenance can be determined by a compressibility



 <div style="font-size: small;">Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

test. Furthermore, conditioning logic is provided for opening the emergency storage tank isolation valves (34340 MV387, MV388) to avoid formation of vapour pockets in the system high points and subsequent water hammer on pump restart as described in ECI Design Manual [1].

### Section 5.13 Leakage Collection

The Leakage Mitigation Subsystem refers to ECI design provisions, which ensure that there is no significant additional public dose resulting from leaks from equipment located in the ECIS equipment room during post-LOCA operation. The subsystem also prevents flooding the ECIS pumps should a significant leak develop during the ECIS mission time. The sump pump design flow exceeds the maximum expected leakage from the anticipated leak sources (pump seals, relief valves). Post-accident, the Leakage Mitigation Subsystem collects any leakage into the ECIS equipment room and returns it to containment.

The portion of the ECI system that is located in a harsh environment following a LOCA is environmentally qualified. The environmental qualification requirements related to ECI are presented in Appendix B1 of DG-29-03650-003 [9]. The ECI system is designed in accordance with the seismic requirements of DG-29-03650-002 [10].

There are interfacing systems that support addressing potential leakages. Per Section 2.3.2.1 of [1], for the D<sub>2</sub>O Recovery System (33330), the ECI logic provides a signal to isolate the system to prevent the spread of contamination outside containment. For the D<sub>2</sub>O Collection System (33810), the ECI logic provides a coincident LOCA signal to vent the collection tanks to containment in order to prevent the spread of contamination outside containment. For the Unit and ECI Area Active Drainage System (71720), the ECI logic provides a LOCA signal to the Recovery Room Sump Pump Diverting Valves to keep potentially radioactive fluid inside containment.


### Section 5.14 Debris Interceptors

Section 5.14 indicates that existing plants demonstrate that their existing debris interceptors meet minimum allowable standards.


Per Section 3.1.1.5 of [1], during the long term injection stage, the ECI pumps take suction from the bottom of the steel lined recovery sump via four lines (one line for each pump). Vortex breakers are provided in all four pump intakes at the sump. A strainer above the vortex breakers and grating above the strainer in the sump prevent foreign objects from entering the pump suction. Each suction of the four individual lines contains a normally closed valve (34340 MV103, MV104, MV113, MV114), which prevents the system water from draining back into the sump and provide containment isolation during normal reactor operation. Per Section 3.3.6.9 of [1], travelling screens have been provided to remove debris from water entering the service water pump intakes to prevent heat exchanger blockages.

## A.11 References

- [1] NK29-DM-34330/34340-003-R001, Emergency Coolant Injection System Design Manual, August 2006.
- [2] NK29-SR-01320-00001-R005, Bruce B 2012 Safety Report – Part 2: Plant Components and Systems, Bruce Power, August 2012.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- [3] NK29-SR-01320-00002-R004, Bruce B 2011 Safety Report, Part 3: Accident Analysis, Bruce Power, November 2011.
- [4] NK29-OSR-34340-00001-R002, Operational Safety Requirements for Bruce B Emergency Coolant Injection System, Bruce Power, May 2013.
- [5] NK29-DM-63433/63434-R020, Emergency Coolant Injection System Instrumentation and Control, Units 05678, March 2015.
- [6] NK21-CORR-00531-12135/NK29-CORR-00531-12545/E-DOC 4659316, Licence Conditions Handbook, LCH-BNGS-R000, Bruce Nuclear Generating Station A and Bruce Nuclear Generating Station B Nuclear Reactor Operating Licence, PROL 18.00/2020 (Effective: June 1, 2015), Canadian Nuclear Safety Commission, May 27, 2015.
- [7] NK29-OSR-34200-00001-R001, Operational Safety Requirements for Bruce B Containment System, November 2013.
- [8] B-CYS-34340-00001-R005, Chemistry Specification Emergency Coolant Injection System, November 2, 2010.
- [9] NK29-DG-03650-003-R007, Environmental Qualification of Safety Related Equipment, Units 05678.
- [10] NK29-DG-03650-002-R007, Seismic Qualification of Safety Related Systems, Units 05678, June 2012.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## **A.12. CSA N290.3-11, Requirements for the containment system of nuclear plants**

This standard presents the requirements for the design, qualification, installation, operation, maintenance, inspection, and documentation of a containment system. A high level review of the Bruce B design against the requirements in this standard is performed with the conclusion that the design meets the intent of the requirements with the exceptions indicated in the text.

Two normative Annexes are part of the standard. These Annexes present the requirements for overpressure protection for piping systems penetrating the containment as well as for piping systems connected to the containment atmosphere and to the reactor coolant system. Specific requirements related to closed piping systems and for small ductile lines are provided together with examples of acceptable configurations to meet the barrier requirements. The requirements in Annex A: Containment Piping Barrier Requirements for Existing Plants are applicable to Bruce B, whereas Annex B: Containment Piping Barrier Requirements For New Builds is intended for new reactor designs only. The high level review of Annex A is already included in the compliance statements associated with the corresponding clauses of the standard.


**Sections 1 to 3** present the scope of the standard, the reference publications and relevant definitions and abbreviations used in the standard. These are introductory clauses and no assessment is deemed necessary.

**Section 4** lists the containment system safety functions.

As described in Section 6.5.1 of Part 2 of the Safety Report [1], the containment is a special safety system, which forms an envelope around the nuclear components of the reactor and the reactor coolant system. It consists of a number of systems and subsystems whose collective purpose is to prevent any significant release of radionuclides, which may be present in the containment atmosphere following certain postulated accident conditions, to the outside environment.

The physical barrier, which minimizes the outflow of radionuclides is called the containment envelope. An important criterion for determining the effectiveness of the containment envelope is the integrated leakage rate for the period of the pressure excursion. To meet the design leakage requirements, two measures are employed. The first involves stringent design requirements to minimize the leakage rate. The second is to reduce the pressure within the containment envelope following a LOCA. The containment system quickly reduces the containment pressure pulse to sub-atmospheric level following a large energy release within the containment envelope and hence minimizes uncontrolled releases to the outside environment.

Deterministic analyses of containment behaviour are performed for all accidents that can release mass and energy and/or radioactivity into the containment envelope. Analyses are performed for an intact containment (i.e., all components and subsystems function as designed) as well as for various containment impairments (i.e., component and subsystem failures). Relevant analyses that define the Safety Analysis Limits are for the intact containment because this is the intended state of this Special Safety System [2]. Design Basis Accidents that employ containment to mitigate the effects of the mass and energy discharge as well as radioactivity release are evaluated and documented in Part 3 of the Safety Report [3].

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

With regard to severe accidents, it is recognized that originally Bruce B was not designed to cope with these, other than the dual failure LOCA plus Loss of Emergency Core Injection (LOECI) which is considered to be a BDBA. The capability of containment to cope with other BDBAs including severe accident conditions is being addressed as part of Fukushima related actions items to enhance the existing understanding of severe accident phenomena and SAMG capabilities [4]. Bruce Power is providing bi-annual progress updates to CNSC until completion.

**Section 5** presents the general requirements and containment design features. Section 6.5.2 of [1] provides a description of all the main containment system, including its envelope, energy management (pressure relief, dousing system), radionuclide management system (Emergency Filtered Air Discharge System – EFADS), combustible gas management (Hydrogen Igniter System).

Per Section 3.2.1.6 of [5], in the event of high pressure within the envelope or high activity conditions being detected in any reactor vault, fuelling machine room or the Vacuum Building, the Bruce B containment envelope will be automatically isolated.

There are four pressure measurements in the pressure relief valve manifold and sixteen activity measurements. There are two activity measurements in the vapour recovery system for each reactor vault and each half, north and south, of the central fuelling area.

There are two on the discharge line from the Vacuum Building vacuum pumps and two in the exhaust line from the east service area to the vapour recovery system upstream of the dryer. As containment is a two channel special safety system (Channel N and P) there are two pressure measurements and eight activity measurements per channel. One of the high pressure signals or any one high activity signal in either channel will initiate automatic containment isolation, as will manual operation of any of the four auxiliary pressure relief valves. Per the design requirements in Section 2.2 of [5], the containment system is required to limit radiological releases to the environment under normal operating conditions and in the event of accidents resulting in discharge of radioactive materials into containment. The design basis events, which require analysis, are listed in the Bruce B Safety Report [3]. The scope of the analysis is agreed upon and reviewed by the CNSC.

Bruce B containment has been shown capable of withstanding the conditions of severe accidents such that the leakage requirements are met. The results of Level 2 PRA showed that containment integrity can be challenged during a multi-unit severe accident if no mitigating measures are available. Bruce Power has completed analysis and assessment activities to evaluate options for ensuring containment integrity and filtered venting in the event of a multi-unit severe accident. The analysis examined the effectiveness of various Containment Filtered Venting System (CFVS) designs as well as the effectiveness of other options for protecting containment integrity and limiting fission product release during a multi-unit severe accident. A final report summarizing the results of the analysis is provided in [6].

**Section 6** describes the general design principles of a containment system.

The containment system is considered to be effective if timely activation of containment isolation and pressure suppression takes place. These will ensure that releases of radioactivity from the containment boundary to the outside environment are mitigated.

Per Section 1.5.3 of [3], timely activation of containment isolation is demonstrated by comparing conservatively calculated doses to Siting Guide dose limits. The criterion that is applied to demonstrate effective pressure suppression is that the peak containment pressure remains

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

below its design pressure (82.7 kPa[g]). This derived effectiveness criterion, while applied for all design basis accidents, is most relevant for large break LOCAs and steam supply system failures.

External event and conditions are taken into account in the design of the plant, including containment and its structures. Meteorology, hydrology, seismology, geology and climate change conditions are described in Section 2 of [1].

From the severe accident viewpoint, the current Bruce B plant design capabilities and features are taken into consideration to supplement containment features and functions. In support of Fukushima action items additional safety features supplement the existing containment envelope and systems providing substantial benefit in mitigating the consequences of such events [6].

The selection of materials used inside containment considers post-accident conditions; the Bruce Environmental Qualification (EQ) program follows the requirements of [7]. As part of the EQ program, Bruce Power has upgraded the cables to feed selected in-containment equipment - ECI valves, SDS2 ion chamber cabling, SDS2 flux detectors, and wall mounted vault coolers (i.e., all equipment credited for harsh environment that resides in the vault).

**Section 7** discusses the leakage criteria applicable to the containment boundary.

The maximum allowable leakage rate is based on the analyses documented in Part 3 of the Safety Report [3] (Section 5.6.4). The safety limits related to leakage are presented in the Containment OSR [2]. The design leakage rates are presented in the Design Manual Negative Pressure Containment System Part 1 [5].

The containment OSR [2] states that the OP&P requires the overall leakage rate of the containment envelope to be  $\leq 2.0$  percent of the free, enclosed volume per hour at the positive design pressure of 82.7 kPa(g) (see also Table A.21.2.2 of [8]). The design target is one percent per hour at the design pressure and the measured leakage is below this target.

As described in Section 6.5 of Part 2 of the Safety Report [1], an important criterion for determining the effectiveness of the containment envelope is the integrated leak rate for the period of the pressure excursion. To meet the design leakage requirements, two measures are employed. The first involves stringent design requirements to minimize the leak rate. The second is to prevent the design pressure within the containment envelope from being exceeded following a LOCA.

Quantitative leakage criteria are discussed in [2] for the components of the containments systems. Justification is provided for the components for which quantitative values are not provided (e.g., for the vacuum building since its operability is continuously verified by maintaining the pressures within the specified limits).

Bruce Power Nuclear Emergency Response Plan (NERP) [9] outlines the command, control, and coordination structure and activities, activation, site integration, external agency coordination, deployment of emergency resources, and emergency facilities through the use Emergency Response Procedures developed to guide effectively trained emergency response staff in emergency response and mitigation techniques. In addition to design basis events, this plan takes into account requirements to support a sustained response to a beyond design basis multi-unit event resulting in an extended loss of off-site power for up to 72 hours without



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

assistance. Since beyond design basis event response is not addressed in BP-PLAN-00001 [9], for those events where accident consequences indicate that the design basis response has not been effective, the ERO will activate Severe Accident Management Procedure [10]. The Severe Accident Management Procedure [10] is implemented by station specific SAMG documentation. The Bruce B specific Severe Accident Guides applicable to containment are listed in Section 5.3 of [10].

**Section 8** describes the requirements related to identification and location of containment penetrations and the associated extensions of the containment boundary. These requirements are reflected in the Bruce B containment design guide [11].

**Section 9** describes the design requirements for containment subsystems such as containment structures, barriers for containment penetrations, energy management, radionuclide management and combustible gas management systems.

**Section 9.1 Containment Structure** requires that the containment structure be in accordance with the requirements of CSA N285.0/N285.6 and the CSA N287 Series of Standards.

Compliance with, as well as guidance from, these standards is provided in the Licence Conditions 5.1, 5.2, and 6.1 of the Licence conditions handbook [12] in support of the PROL [13].

**Section 9.2 Barriers for Containment Penetrations:** Bruce B design meets the intent of the requirements in this clause. The containment penetrations are described in Section 6.5.2.7 of Part 2 of the Safety Report [1]. Allowable leakage through penetrations is specified in the Design Manual [5].

Per Section 6.1.8.3.4 of [5], complex extensions of containment (piping systems, transfer chambers or facilities), or those using mechanical or working Type A barriers and Type B barriers, may be required to be testable for leak tightness on a routine basis.

Annex A provides containment piping barriers requirements for existing plants. While in general Bruce B meets these requirements, the safety significance of identified differences has not been assessed and therefore is considered a gap (SF1-19 in Table 8). The main differences between the requirements from Annex A2 and A3 of N290.3 and the containment design guide are as follows:

- N290.3 Clause A.2.3 requires pipes open to containment less than 1 hour per year to have two means of isolation (i.e., one of two normally closed manual isolation barriers in series, or two automatic isolation valves, or a combination of a manual and an automatic barrier. Bruce B containment Design Guide (DG) [11] Section 6.2.1.1.8 allows a single closed valve.
- N290.3 Clause A.2.5 provides the conditions for having at least one barrier, one condition being pipes with less than 50 mm nominal diameter. Bruce B DG [11] specifies these conditions for pipes with less than 1 inch nominal diameter.
- N290.3 Clause A.3.1 requires that, for pipes connected to HTS (reactor coolant system) with nominal diameter greater than 25 mm, two isolation barriers be provided, one inside and one outside the containment. Bruce B DG [11] (Section 6.2.2.3.1) specifies the requirement for pipes with nominal diameter greater than 1 inch. It also allows both valves to be on only one side of the containment in certain circumstances.



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- N290.3 Clause A.3.4 requires that, for pipes connected to HTS (reactor coolant system) with nominal diameter less than 25 mm, at least one barrier be provided. Bruce B DG [11] (Section 6.2.2.3.4) specifies this condition for pipes with less than 1 inch nominal diameter.

The design requirements for the airlocks are reflected in the Bruce B DG [11] Section 6.2.1.2.3. The design manual [5] (Section 2.10.1.1) also includes a requirement that the personnel airlocks should be manually operable to facilitate personnel evacuation.

### **Section 9.3 Energy Management Systems:**

The energy management systems comprise 12 main pressure relief valves, four auxiliary and four instrumented pressure relief valves, vacuum building dousing system, vacuum system, vault coolers. They are described in detail in Sections 1.2.2, 2.4.2, and 3.2.2 of the containment design manual [5].

**Section 9.4 Radionuclide management system:** The Emergency Filtered Air Discharge System (EFADS) provides the means for long-term, post-LOCA pressure control after the containment vacuum reserve is exhausted. The function of EFADS is to maintain containment pressure at -0.1 kPa(g) or less, and to filter, control, and monitor the discharge flow from containment to limit releases of radioactivity. It is manually connected to the vacuum building and/or PRV manifold during the containment repressurization phase following a LOCA. The Design Manual for EFADS [13] provides additional details.

### **Section 9.5 Combustible gas management:**

Hydrogen igniters are used for short term hydrogen mitigation at the Bruce B station. The hydrogen ignition system consists of 64 igniters distributed in pairs within the reactor vaults and the fueling machine duct (16 igniters per unit). These are divided into two channels for redundancy. The igniters are energized by the containment isolation signal. The system is inactive during normal operation. The only system function is that the igniter coils reach and maintain a sufficiently high temperature when the system is activated. For more details see [2].

Passive Autocatalytic Recombiners (PARs) have been installed in Bruce B as described in [15], to provide mitigation of the potential buildup of hydrogen gas in the Reactor Vaults or other areas of Containment during a severe accident scenario since buildup of hydrogen in the containment system has the potential to cause an explosion, if not properly mitigated.

There are no design provisions to sample the containment atmosphere and monitor the concentration of hydrogen during BDBA as required in clause 9.5.4. This is addressed by the implementation of Severe Accident Management Guidelines where a computational aid will be used to determine hydrogen concentration based on an estimated percentage of core Zirconium oxidation (see Section 7.2 of [16]).

**Section 10 Instrumentation:** addresses the instrumentation and monitoring requirements. Following the completion of the COG generic methodology for performing survivability assessments in CANDU reactors, Bruce Power completed the Instrument and Equipment (I&E) survivability assessment as documented in Enclosure 2 of reference [6]. The assessment demonstrated that the vast majority of the BDBA and SAMG High Value I&E that could be used to maintain basic safety functions (i.e., fuel cooling, containment integrity and control of radioactive release) have a reasonable chance of survivability [4]. The identified opportunities for improvement are being addressed. Also as part of Fukushima Action Items, Bruce Power

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

performed assessment of site-specific external hazards. The assessment of Review Level Condition for high winds and seismic events and a review of the potential impacts of seismically induced internal fires and internal floods identified several recommendations that are being investigated [4].


Clause 10.1 requires the effect of atmospheric pressure fluctuations due to extreme weather (e.g., tornados) to be considered in the design of instrumentation. Since the design documentation does not reflect this requirement, it is assessed as a gap in SF1-3 in Table 8.

Clause 10.2.2 requires a list of containment conditions (e.g., pressure, temperature, and hydrogen concentration inside containment) that need monitoring for BDBAs to be developed. The SAM parameters and setpoints are presented in BP-SAM-20017 [17].

**Section 11 Shielding:** presents the shielding design requirements. The containment structure itself provides shielding from fission products following an accident. The only portion of the system which is external to the containment structure and which might require access following a LOCA is the EFADS system. Under normal station operation, there will be no radioactivity present on or released from the filters. Following a LOCA with subsequent EFAD system operation, there may be a significant level of activity in the filter unit; therefore, the following provisions are made [13]:

- EFADS filter units are provided with shielding suitable for the activity levels present;
- For occupational doses, construction material and thickness are compatible with maximum radiation fields of 3 rem/hr and maximum integrated radiation doses of 2.5 rem based on intermittent access;
- The blowers are shielded from the filters to permit post-accident access and maintenance;
- All instruments, except primary elements, are located outside the shielded filter rooms in an area with low radiation dose rate;
- Valves associated with the filters are located outside the shielded filter rooms wherever possible;
- The discharge stack is designed and located such as to minimize radioactive exposure of operating staff.

**Section 12 Support Systems** lists the design requirements related to containment support systems. During normal operation, there is a continuous inflow of gas from the instrument air system and other sources. As described in the Containment OSRs [2], this "compressed gas ingress" is removed by venting a portion of the containment atmosphere through the Vault Vapour Recovery System (VVRS). The gas inflow has a detrimental effect on the consequences of accidents, since it shortens the sub-atmospheric hold-up period and increases controlled venting flows through the Emergency Filtered Air Discharge System. Unlike the structural leakage, the compressed gas ingress is not sensitive to the pressure differential between inside and outside of the containment. The reference large break LOCA containment response analysis assumed a compressed gas ingress rate of 400 kg/h (corresponding to about 90 L/s). The accident consequences are affected by the post-accident air-ingress rate.

 <div style="font-size: small;">Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


Following a LOCA, operators will isolate all unnecessary sources of compressed air into containment [2].

**Section 13 Operational requirements:** discusses the operational requirements related to containment atmosphere. The requirement for maintaining the containment atmosphere at sub-atmospheric pressure in normal operation is reflected in Section 2.3 item a) of the containment design manual [5].

**Section 14 Maintenance of isolation barriers:** describes the requirements applicable to maintenance of isolation barriers. The requirements of this section of the standard are fully reflected in Section 6.1.8.2 of the containment design guide [11].

## A.12 References

- [1] NK29-SR-01320-00001-R005, Bruce B 2012 Safety Report – Part 2: Plant Components and Systems, Bruce Power, August 2012.
- [2] NK29-OSR-34200-00001, Operational Safety Requirements for Bruce B Containment System, R001, November 2013.
- [3] NK29-SR-01320-00002-R005, Bruce B 2011 Safety Report, Part 3: Accident Analysis, Bruce Power, November 2011.
- [4] NK21-CORR-00531-12209/NK29-CORR-00531-12635, Bruce Power Progress Report No. 7 on CNSC Action Plan – Fukushima Action Items, Bruce Power Letter, F. Saunders to K. Lafrenière, August 7, 2015.
- [5] NK29-DM-34200-001-R003, Negative Pressure Containment System, Units 5-8, December 1983.
- [6] NK21-CORR-00531-11801/NK29-CORR-00531-12195, Bruce Power Progress Report No. 6 on CNSC Action Plan – Fukushima Action Items, Letter, F. Sanders to K. Lafreniere, January 30, 2015.
- [7] NK29-DG-03650-003-R007, Environmental Qualification of Safety Related Equipment, Units 05678.
- [8] BP-OPP-00001-R019, Operating Policies and Principles – Bruce B, Bruce Power, July 14, 2015.
- [9] BP-PLAN-00001-R005, Bruce Power Nuclear Emergency Plan, Bruce Power, December 2, 2014.
- [10] BP-PROC-00659-R002, Severe Accident Management, Bruce Power, February 3, 2014.
- [11] NK29-DG-03650-006-R004, Containment Provisions for Extensions of the Containment Envelope, Units 05678, December 2005.
- [12] NK21-CORR-00531-12135/NK29-CORR-00531-12545/E-DOC 4659316, Licence Conditions Handbook, LCH-BNGS-R000, Bruce Nuclear Generating Station A and Bruce Nuclear Generating Station B Nuclear Reactor Operating Licence, PROL 18.00/2020 (Effective: June 1, 2015), Canadian Nuclear Safety Commission, May 27, 2015.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

- [13] NK21-CORR-00531-12136/NK29-CORR-00531-12546/E-DOC 4723908 , Nuclear Power Reactor Operating Licence, Bruce Nuclear Generating Stations A and B, PROL 18.00/2020, Canadian Nuclear Safety Commission, May 27, 2015.
- [14] NK29-DM-34310-001-R004, Emergency Filtered Air Discharge Systems (EFADS), December 1984.
- [15] NK21-CORR-00531-12209/NK29-CORR-00531-12635, Bruce Power Progress Report No. 7 on CNSC Action Plan – Fukushima Action Items, Bruce Power Letter, F. Saunders to K. Lafrenière, August 7, 2015.
- [16] BP-SAM-0001-R000, Technical Support Group User's Guide, Bruce Power, October 15, 2009.
- [17] BP-SAM-20017-R000, Bruce B – SAM Parameters and Setpoints, September 24, 2011.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

### **A.13. CSA N290.11-13, Requirements for reactor heat removal capability during outage of nuclear power plants**


This is a relatively new standard (issued in 2013) presenting the requirements for the design, qualification, installation, commissioning, operation, maintenance, testing, inspection, and documentation for systems providing heat removal from the reactor core to the ultimate sink(s) for water-cooled nuclear power plants during outages. The scope of the standard is limited to fuel cooling within the reactor core.

Sections 1 to 3 present the scope of the standard, the reference publications and relevant definitions and abbreviations used in the standard. These are introductory clauses and no assessment is deemed necessary. Section 4 describes the general functional requirements and success criteria for process and emergency heat sinks. Further requirements related to heat sink operation, instrumentation and control, containment boundary, loop isolation, reliability, independence and separation, pressure-retaining SSCs, equipment qualification, dynamic piping effects, maintenance and testing, documentation and support systems are presented in Section 5. The relationship of heat sinks to design and engineering aspects of safety and to operation is also explained in Section 5.

Decay heat is removed in a staged manner during a reactor outage. As presented in [1], during normal cooldown from the zero power hot state with Class IV power available, the main HT pumps circulate the coolant and heat is rejected through the Condenser Steam Discharge Valves (CSDVs) or the Atmospheric Steam Discharge Valves (ASDVs) to cool the HT system to 177°C (350°F). Further cooldown is then achieved using the shutdown cooling system. The shutdown cooling circuit cools the HT system from 165°C (329°F) to 90°C (194°F) or less by circulating demineralized cooling feed water through the shell side of the preheaters. Heat absorbed through the preheaters is transferred to the Low Pressure Service Water System (LPSW) via two SDCS Heat Exchangers (HX). The SDCS is isolated from the Feedwater and Condensate system under normal operating conditions and is poised to be used when required. The Shutdown Cooling System is required to depressurize the HTS and partially drain it, so the Maintenance Cooling System can be employed if needed. The SDC system is capable of cooling the HT system to 59°C (138°F) and can be used to hold it at that temperature for an indefinite period. The shutdown cooling system is capable of cooling the HT system from the zero power hot temperature (260°C) under emergency conditions.

The shutdown cooling system consists of two (50%) heat exchangers and two 100% recirculation pumps. Operation of the shutdown cooling system requires that the feedwater system be pressurized. The shutdown cooling system is part of the feedwater circuit and is designed and constructed in accordance with ASME B31.1, as is the feedwater system.

The Maintenance Cooling System (MCS) is a process system that provides the long-term heat sink for the HTS following a reactor shutdown. It circulates primary coolant through the reactor core to remove fuel decay heat and maintain the coolant temperature in the reactor outlet header. The MCS is the safety analysis-credited engineered heat sink for the HTS when it is in its fully depressurized and drained state. During normal operation, the MCS is poised and isolated from the HTS. It is normally placed in service no sooner than 24 hours after a reactor shutdown and when the primary coolant temperature has been reduced to below 90°C using the SDCS.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

As presented in reference [1], the maintenance cooling system is normally used for cooling the HT system to 59°C or less after the shutdown cooling system has reduced the HT system temperature to less than 90°C (194°F). It can be used to cool down the HT system from 160°C (326°F) if the shutdown cooling system is unavailable. Maintenance of some components (steam generators, pumps, valves) requires that the HT system be depressurized and drained to the header level. Following depressurization, the HT system can be drained to any level above the reactor headers with the decay heat being removed by the maintenance cooling heat exchanger. All heavy water drained from the HT circuit is purified before being stored.

The system consists of a one-loop circuit containing a heat exchanger and two pumps connected between the reactor outlet headers and the corresponding inlet headers. The system bypasses the steam generators and main pumps. Core cooling is achieved by pumping water from the outlet headers, through the heat exchanger, with the pressure at the inlet headers being sufficient to force water through the core to the opposite outlet header.

The system is entirely below header level. The piping is routed through the containment wall to the pumps and heat exchanger located outside containment. Isolating valves are located just inside and outside the containment structure and are always closed when the reactor is operating.

Following Design Basis Accidents, the MCS system may be used as a heat sink, similar to its normal use. However, it may have to be employed sooner if the accident requires that the HTS be cooled as soon as possible to mitigate accident consequences. It may also be activated for an emergency cooldown of the HTS, should the SDCS be unavailable. In this mode of application the MCS can be used at more elevated HTS temperatures, attainable by cooldown via boiler steam relief to the atmosphere.

Per [2], the safety-related functions performed by the SDCS are:

- Serve as emergency shutdown heat sink in the range of HTS temperatures from 260°C to below 100°C;
- Maintain a pressure boundary between the Feedwater and Condensate System and the SDCS piping when not in service (i.e., the isolation function);
- Provide an emergency isolation of the Feedwater and Condensate System following a break in the SDCS when in service.

The safety-related functions performed by the MCS are:

- Serve as a heat sink over the full range of HTS pressures with reactor outlet header (ROH) temperatures  $\leq 90^{\circ}\text{C}$  (i.e., the post-accident heat sink function);
- Serve as an emergency shutdown heat sink when the HTS is pressurized, SDC is unavailable, and ROH temperatures  $\leq 177^{\circ}\text{C}$  (i.e., the emergency HTS cooldown function);
- Maintain a leak-tight boundary of the Containment extension formed by the MCS when in use (i.e., the containment function);
- Be able to restore the pressure boundary of the HTS should failures occur in the MCS when in use (i.e., the isolation function).



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

The N290.11-13 success criteria are reflected in the safety criteria provided in the Operational Safety Requirements safety criteria (Section 1.4 of [2]). Specifically, safety analyses use derived criteria that stipulate that an accident is successfully mitigated when:

- Fuel sheath failures are avoided,
- Fuel channel integrity is maintained, and
- Public doses are below the siting guide limits.

For failures of the SDCS and MCS, dose limits are met if fuel failures are prevented. For HTS breaks outside containment and spurious opening of boiler SRVs, public doses are due to pre-existing iodine and tritium in the HTS rather than fuel failures.

The systems associated with outage heat sinks are identified and listed in Bruce B Outage Heat Sinks Operating Manual [3]. The Operating Manual outlines the selection criteria for various combinations of primary and backup heat sinks. The operating states, standard and specific outage conditions are defined in the Operating Manual. Non-standard operating conditions are listed as well as the associated operational constraints and requirements. For each state, the primary, the backup and the emergency heat sinks are described. Outage Heat Sink Checklists and emergency checklists are prepared.

The requirement in clause 5.2.2.4 for the staff credited with performing contingency activities to support the heat sink not to be credited with availability for other activities has not been demonstrated to be met; therefore it is assessed as a gap and is noted as SF1-7 in Table 8.

Maintenance activities are carried out according to the specific procedures. The Outage Work Management Program [4] specifies the controls associated with planning, implementation, and control of work performed on a reactor unit when the unit is shutdown such that maintenance, inspections, and modifications are performed safely and on the basis of value to maintaining safe, reliable and lowest cost operation. This includes selecting and controlling the scope of work, planning, scheduling, coordinating work execution, and closing out the outage. BP-PROG-11.02 [5] covers the approval of new Work Requests and decides if the work is performed during On-Line plant operations or during outage conditions. The Outage Work Management Program [4] is designed to satisfy and exceed the intent of CSA Standards N286-05, Management System Requirements for Nuclear Power Plants as they pertain to managing outage work. The Program is implemented by BP-PROC-00342 Planned Outage Management [6] and BP-PROC-00343 Forced Outage Management [7].

As presented in Shutdown and Maintenance Cooling Systems OSRs [2], following design basis accidents for which SDCS is credited, the MCS can be credited as an acceptable alternative in case SDCS is not available (Section 1.6 Overview of Limiting Accidents of OSRs and Appendix 6, Heat Transport Auxiliary System Pipe Breaks Outside Containment, Part 3 of the Safety Report). For this reason, the SDCS heat sink function can be considered to be a defence-in-depth provision that is credited in the safety analysis to assure a highly reliable emergency heat sink capability. As a consequence, unavailability of SDCS represents a loss of redundancy with respect to the credited heat removal function of the Shutdown and Maintenance Cooling Systems, provided MCS is available. The operability conditions have been defined accordingly in this OSR. It is noted that the SDCS cannot be credited as an alternative for MCS since there

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

are design basis accidents for which MCS must be credited (e.g., events that require draining of the HTS to terminate releases).

Clause 5.2.2.10 requires an assessment of the consequences of the delay or error during the execution of manual actions required to recall a heat sink to be completed with respect to meeting the success criteria defined in Clause 4.2. The list of internal initiating events is presented in Table 2-1 (Shutdown Cooling and Maintenance Cooling System Failures) of Part 3 of the Safety Report [8]; however events initiated as a result of human errors in operation and maintenance are not explicitly identified, although initiating event frequencies implicitly include any relevant operator error that may cause the initiating event. This is identified as a gap (SF1-3) in Table 8, and is also identified as a gap against clause 6.1.1 of REGDOC-2.5.2.


A review of outage heat sinks under natural circulation has been performed to define the configurations and conditions under which natural circulation could be credited as an effective heat transport mechanism for use in shutdown heat sink management. The objective of the review was to establish the conditions under which thermosyphoning and Channel Cooling in the Absence of Forced Flow (CCAFF) can be credited as effective heat removal mechanisms. The most limiting restrictions were then identified and presented as waiting times after shutdown to perform various maintenance activities [9]. Further series of analyses have been carried out and historical operating data analysed to refine the methodology for deriving operating restrictions during outage [10].

Part 3 of the Safety Report [8], Sections 3.3.4 and 3.3.5 present a summary of Shutdown Cooling System failures and Maintenance Cooling System (MCS) failures, respectively. The analyses demonstrate that failures during operation of SDC system or MCS do not cause fuel failures due to overheating, the fuel channel integrity is maintained and radiological doses to the public do not exceed applicable limits. The details of these analyses are presented in Appendix 8 of [8], Shutdown Cooling and Maintenance Cooling System Failures.


Based on this assessment, gaps SF1-3 and SF1-7 have been identified and are listed in Table 8.

### **A.13           References**

- [1] NK29-SR-01320-00001-R005, Bruce B 2012 Safety Report, Part 2: Plant Components and Systems, August 2012.
- [2] NK29-OSR-34700-00001-R000, Operational Safety Requirements for Bruce B Shutdown and Maintenance Cooling Systems, September 2008.
- [3] NK29-OM-03500.2-R019, Bruce Nuclear Generating Station B Operating Manual, Outage Heat Sinks, Units 05678, September 2011.
- [4] BP-PROG-11.03-R005, Outage Work Management, Bruce Power, July 26, 2011.
- [5] BP-PROG-11.02-R006, On-Line Work Management Program, Bruce Power, October 23, 2012.
- [6] BP-PROC-00342-R006, Planned Outage Management, Bruce Power, February 11, 2015.
- [7] BP-PROC-00343-R006, Forced Outage Management, Bruce Power, March 4, 2015.

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


- [8] NK29-SR-01320-00002-R005, Bruce B 2011 Safety Report, Part 3: Accident Analysis, November 2011.
- [9] N-REP-03500.2-10002-R000, Corporate Review of Outage Heat Sinks Management – Guidelines and Principles of Crediting Natural Circulation in Outage Heat Sinks, July 31, 2000.
- [10] NK29-REP-03500-00007-R000, Corporate Review of Outage Heat Sinks Decay Heat Curve Documentation and Confirmatory Analysis, June 30, 2004.

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## Appendix B – Clause-by-Clause Assessments Against Relevant Codes and Standards

This appendix presents the clause-by-clause assessments that are performed for this Safety Factor. The PSR Basis Document provides the following compliance categories and definitions for clause-by-clause assessments:

- Compliant (C) – compliance has been demonstrated with the applicable clause;
- Indirect Compliance (IC) – Compliance has been demonstrated with the intent of the applicable clause;
- Acceptable Deviation (AD) – Compliance with the applicable clause cannot be demonstrated; however, a technical assessment has determined that the deviation is acceptable. For this case a detailed discussion and explanation shall be included in the PSR documentation;
- Gap – system design and/or operational improvements may be necessary;
- Guidance: A potential programmatic, engineering, analytical or effectiveness gap found against non-mandatory guidance;
- Relevant but not Assessed (RNA) – The particular clause provides requirements that are less strenuous than clauses of another standard that has already been assessed. The definition also includes the guidance portion of clauses in which a gap has already been identified against the requirement;
- Not Relevant (NR) – The topic addressed in the specific clause is not relevant to the safety factor under consideration but may well be assessed under a different Safety Factor; and
- Not Applicable (NA) – The text is not a clause that provides requirements or guidance. Also used if the clause does not apply to the specific facility.

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## B.1. CSA N290.1-13, Requirements for the Shutdown Systems of Nuclear Power Plants

In support of the review tasks listed in Section 5, a detailed assessment of CSA N290.1-13 has been performed in Table B1.

**Table B1: CSA N290.1-13, Requirements for the Shutdown Systems of Nuclear Power Plants**


Article No.	Clause Requirement	Assessment	Compliance Category
4		This is not a requirement/guidance clause (this is a title only).	NA
4.1		This is not a requirement/guidance clause (this is a title only).	NA
4.1.1	<p>The NPP shall include SDS capability for the following design safety functions. Acting automatically, the SDS shall</p> <p>a) shut down the reactor to mitigate the consequences of postulated initiating events (PIEs); and</p> <p>b) prevent any foreseeable increase in reactivity leading to unintentional criticality during the shutdown state.</p>	<p>SDS1 and SDS2 are incorporated in the NPP special safety systems that are designed to mitigate consequences of a single failure in the process system and a dual failure involving a failure in the process system combined with coincident unavailability of one of the special safety systems.</p> <p>To effectively reduce the risk presented by a postulated process system failure, special safety systems are independent of process systems, including the reactor regulating system, whose failure might require the subsequent action of the special safety system. To the greatest extent practicable, the special safety systems are also independent of each other in design and operation. This requirement evolves from the Canadian reactor safety principle of analyzing each postulated process system failure in conjunction with a failure of each of the special safety systems in turn.</p> <p>Section 6.1.1 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001, Revision 05].</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
4.1.2		This is not a requirement/guidance clause (this is a title only).	NA
4.1.2.1	<p>The SDS shall terminate the chain fission reaction when a failure of a reactor process system occurs that could fail fuel sheaths or other barriers, to prevent a significant release of radioactivity.</p> <p>Notes:</p> <ol style="list-style-type: none"> <li>1) Termination of the chain fission reaction is generally accomplished by inserting rods or liquids that absorb neutrons.</li> <li>2) In CANDU reactors, SDS is credited for overpressure protection.</li> </ol>	<p>Bruce B reactor incorporates these common CANDU design features. SDS1 and SDS2 can both be used to terminate reactor operation when parameters reach an unacceptable range.</p> <p>Section 6 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev.5].</p>	C
4.1.2.2		This is not a requirement/guidance clause (this is a title only).	NA
4.1.2.2.1	<p>At least two separate, independent, and diverse MSD shall be provided.</p> <p>Notes:</p> <ol style="list-style-type: none"> <li>1) "Independence" and "diversity" are defined in CSA N290.0, Clause 3.1.</li> <li>2) For CANDU reactors, two separate, independent, and diverse shutdown systems are generally provided.</li> </ol>	<p>SDS1 and SDS2 are functionally and physically independent and employ two diverse shutdown principles (means of shutdown). SDS1 is the primary shutdown system which releases 32 neutron absorbing spring-assisted gravity drop shutoff rods. Section 6.2 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev.5].</p> <p>SDS2 uses rapid injection of concentrated gadolinium nitrate solution into the bulk moderator through eight horizontally distributed nozzles. Section 6.3 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev.5].</p>	C
4.1.2.2.2	<p>During normal operation, in AOOs and in DBAs, at least one means shall be independently capable of quickly rendering the reactor subcritical by an</p>	<p>For single process failures (identified in Part 3 of the Safety Report), SDS1 is demonstrated by analysis to have sufficient reactivity depth and act with sufficient speed that the reactor</p>	IC




Article No.	Clause Requirement	Assessment	Compliance Category
	adequate margin on the assumption of a single failure.	<p>siting criteria are met. See Section 6.2.2 of Part 2 of the Bruce B Safety Report [NK29-SR-01320-00001 Rev.5]</p> <p>For the accident conditions (identified in Part 3 of the Safety Report), SDS2 is demonstrated by analysis to have sufficient depth and to act with sufficient speed that the reactor siting criteria are met. See Section 6.3.2 of Part 2 of the Bruce B Safety Report [NK29-SR-01320-00001 Rev.5]</p> <p>Part 3 of the Bruce B Safety Report [NK29-SR-01320-00002 Rev.5] does not specifically categorize the single failure events into AOO, DBA or BDBA categories.</p> <p>The systematic identification and classification in accordance with REGDOC-2.4.1 is part of an ongoing commitment per action Item 090739 (Safety Improvement Project) as described in Section 1.1 of Attachment A of the November 2015 letter [NK29-CORR-00531-12767]. Therefore, Bruce B indirectly complies with the requirements of this clause.</p>	
4.1.2.2.3	At least one means shall be independently capable of rendering the reactor subcritical and maintaining it subcritical by an adequate margin for even the most reactive conditions of the core.	<p>For all single process failures identified in Part 3, each shut down system (SDS1 and SDS2) is demonstrated by analysis to have sufficient speed that the reactor siting criteria are met.</p> <p>Section 6 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev.5].</p>	C
4.1.2.3	If the credited SDS fails or is unavailable when required and the inherent reactor core characteristics are unable to maintain the reactor within specified limits for that event, a second, fast-acting SDS shall be provided to assure shutdown.	Bruce B design incorporates two shutdown systems, SDS1 and SDS2, are functionally and physically independent of each other and functionally independent of the reactor regulating systems. The systems are geographically separated. Each system is independently demonstrated by analysis to have sufficient speed that the reactor siting	C

Article No.	Clause Requirement	Assessment	Compliance Category
	Note: The safety analysis determines the maximum time allowed for detection of the unsafe condition, for actuation of the MSD, and for its deployment to shut down the reactor.	criteria are met.  Each system is designed for an unavailability of less than 1E-3 yr/yr, shutdown system reliability is monitored and reported regularly and has usually been substantially better than the 1E-3 yr/yr unavailability requirement as noted in Section 1.1.3 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev.5].	
4.1.3	Any number of redundant instrumentation channels, or a mixture of various numbers of channels, may be employed to meet the reliability and single failure requirements.  Note: Past practice on CANDU reactors has indicated that both safety and spurious trip requirements can be met by a three-channel SDS in which the coincidence of two out of three channels initiates reactor shutdown.	Separation of the instrumentation channels of the two systems is achieved by channelization. Each of the three channels on a specific special safety system follows a separate route. Section 6.1.5 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev.5].  Each process and nuclear measurement loop that is essential for the operation of special safety system is designed to be redundant (duplicated or triplicated), such that a single loop component or power supply failure cannot incapacitate or spuriously invoke its operation. Section 6.1.2 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev.5].	C
4.1.4		This is not a requirement/guidance clause (this is a title only).	NA
4.1.4.1	Diverse methods or concepts of the MSD (e.g., rods and poison) shall be used to avoid common-cause failures and cross-link effects.	The means of shutdown (MSD) has diverse methods, as SDS1 uses shutoff rods and SDS2 uses injection of a neutron absorbing solution into the moderator. Section 6 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev. 5].	C
4.1.4.2	When more than one SDS is used, the system components involved in trip initiation shall not be	SDS 1 uses independent triplicated logic, which senses the requirement for a reactor trip and de-energizes DC-operated	C

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	shared between SDS.	<p>clutches to release the shutoff rods. Section 6.2.1 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev.5].</p> <p>SDS2 employs an independent triplicated logic system, which senses the requirement for emergency shutdown and opens fast acting valves to inject the gadolinium poison into the moderator using high pressure helium. Section 6.3.1 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev. 5].</p>	
4.1.4.3	<p>Principles shall be prepared for preventing failures in more than one SDS when common equipment, procedures, or personnel are used in design, construction, commissioning, or operation.</p> <p>Note: An example of common equipment is calibration tools.</p>	<p>As stated in the Design Manuals for SDS1 and SDS2 the two shutdown systems shall be independent of each other physically, functionally and conceptually per Section 2.9.4.1 of the Bruce B Shutdown System 1 Design Manual [NK29-DM-63720-001 Rev.7] and Bruce B Shutdown System 2 [NK29-DM-63730-001 Rev.11].</p> <p>There are common personnel used in the design of SDS1 and SDS2, per the revision history of the respective design manuals [NK29-DM-63720-001] [NK29-DM-63730-001]. Principles have been prepared in the SDS1 and SDS2 Design Manual (see section 2.12.2 of [NK29-DM-63720-001 Rev.7] and [NK29-DM-63730-001 Rev.11]) which requires: "The system shall tolerate any plausible, single personnel-induced fault".</p> <p>Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p> <p>There is a comprehensive system of monitoring, inspection, and testing to ensure the integrity of mechanical components</p>	C

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>and reliability of equipment. Section 1.3.2.2 of the Bruce B Safety Report Part 2 [NK29-SR-01320-001 Rev. 5].</p> <p>The development of detailed operating procedures and extensive training of the plant personnel contribute to the prevention of failures in more than one SDS.</p>	
4.1.4.4	<p>If common electrical power and instrument air systems are employed for the redundant SDSs, their designs shall be demonstrated to be free from the adverse consequences of failures in the support service.</p> <p>Note: See CSA N290.5 for requirements on electrical power and instrument air systems.</p>	<p>Each shutdown system has a separately channelized Class I power supplies per Sections 6.2.8 and 6.3.7 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev. 5].</p> <p>The instrument air system was designed on a unit basis, with one complete system per reactor unit. The individual air systems are provided with air receivers with a large enough capacity to supply air during a Class IV power failure until Class III power is available. Section 11 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev. 5].</p>	C
4.1.5		This is not a requirement/guidance clause (this is a title only).	NA
4.1.5.1		This is not a requirement/guidance clause (this is a title only).	NA
4.1.5.1.1	<p>If an SDS and a process system share physical space, then the associated shutdown function shall also be provided by another SDS to counter the possibility of failures in the process system.</p> <p>Note: "Physical space" refers to an area where a process failure can disable the SDS.</p>	<p>The Bruce B shutdown systems (SDS1, SDS2) are as much as possible independent of any of the process systems. A single plausible fault in the process system shall not adversely affect the other shutdown system.</p> <p>Requirements between shutdown systems and process systems physical facilities (e.g., racks, panels, etc.) are provided in Section 2.9.4.2(b) of the Bruce B Design Manual for SDS1 [NK29-DM-63720-001] and Section 2.9.4.2(b) of Bruce B Design Manual for SDS2 [NK29-DM-63730-001].</p> <p>Each system is independently demonstrated by analysis to</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
		have sufficient speed that the reactor siting criteria are met per Section 6 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev. 5].	
4.1.5.1.2	<p>Any process equipment performing an SDS function shall be designed to be consistent with SDS requirements.</p> <p>Note: Existing CANDU plants may use SUI where agreed to by the authority having jurisdiction (AHJ).</p>	<p>The SDS is independent of each other and also are, as much as possible independent of any process systems, including the reactor regulating system. Per Section 6 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev. 5].</p> <p>Requirements between shutdown systems and process systems sharing of components (e.g., pipes) in the specific process system are prescribed in the respective design manuals for SDS1 and SDS2. Where such sharing is used it shall be shown that a fault associated with that element does not constitute an unsafe cross-link between a process system and the shutdown system as required in Section 2.9.4.2(a) of the Bruce B Design Manual for SDS1 [NK29-DM-63720-001 Rev.7] and Section 2.9.4.2(a) of Bruce B Design Manual for SDS2 [NK29-DM-63730-001 Rev.11].</p> <p>Additionally, any interlocks between the shutdown system and a process system that are provided to ensure the necessary effectiveness of the shutdown system shall be designed to the shutdown system standards as required in in Section 2.9.4.2(d) of the Bruce B Design Manual for SDS1 [NK29-DM-63720-001 Rev.7] and Section 2.9.4.2(d) of Bruce B Design Manual for SDS2 [NK29-DM-63730-001 Rev.11].</p> <p>Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p>	C


Article No.	Clause Requirement	Assessment	Compliance Category
4.1.5.2	<p>If an SDS is also required to perform a process function, the following design requirements shall apply:</p> <p>a) Function sharing:</p> <p>i) The process functions and the SDS functions shall not be credited at the same time.</p> <p>ii) If the process system is operating, and a PIE in that system is postulated, it shall be shown that all essential functions of the SDS required to mitigate a PIE shall be unaffected.</p> <p>iii) The process function shall be designed to the same standard as the SDS.</p> <p>iv) If the process function is used intermittently, then the SDS availability shall be demonstrated, after each use of the process function, by testing the SDS.</p> <p>b) Equipment sharing:</p> <p>i) Sharing of instrumentation, where necessary, shall be limited to the sensing devices and their associated pre-amplifiers or amplifiers to get the signal to the point of processing.</p> <p>ii) Signals past the pre-amplifiers or amplifiers, on the process side, shall be electrically isolated so that failures cannot be propagated from the process system to the SDS.</p> <p>iii) Isolation devices or interlocks between SDS and process systems shall be classified and</p>	<p>Special safety systems are independent and do not perform process functions.</p> <p>Section 6 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev. 5].</p>	NA



Article No.	Clause Requirement	Assessment	Compliance Category
	qualified as SDS devices.		
4.1.6		This is not a requirement/guidance clause (this is a title only).	NA
4.1.6.1	The SDS should be separated from other safety systems; however, a grouping of systems could be acceptable provided that the impact of the particular grouping arrangement is evaluated through safety analysis.	<p>Per Section 6.1.1 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev. 5], the four special safety systems are:</p> <ul style="list-style-type: none"> <li>(1) Shutdown System 1 (SDS1)</li> <li>(2) Shutdown System 2 (SDS2)</li> <li>(3) Negative Pressure Containment (NPC) System</li> <li>(4) Emergency Coolant Injection (ECI) System.</li> </ul> <p>The four special safety systems are independent of each other and to the extent possible the reactor regulating system.</p> <p>Per Section 6.1.4.1 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev.5] to provide protection against postulated common mode incidents, such as local fires or missiles, plant systems are separated into two groups, Group 1 and Group 2. SDS1 belongs to Group 1 and SDS2 to Group 2.</p>	C
4.1.6.2	<p>As a minimum, the SDS shall be physically and functionally separated and electrically isolated from other safety systems as follows:</p> <ul style="list-style-type: none"> <li>a) Sharing of components:</li> </ul> <p>Sharing shall be restricted to passive components in a specific system. Where such sharing is used,</p>	<p>Bruce B Safety Report Part 2, Section 6 identifies four special safety systems (SDS1, SDS2, NPC and ECI) [NK29-SR-01320-0001]. SDS1 and SDS2 are functionally and physically independent of each other and from the NPC and ECI systems.</p> <p>Due to physical constraints imposed on the plant itself it may</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>it shall be shown that any credible fault associated with those components does not constitute an unsafe cross-link between two safety systems. However, as a minimum, separate pressure taps and impulse lines shall be provided for each system. Safety systems may also feed common information-reporting components in the plant process systems (e.g., monitoring devices, annunciation systems), provided that suitable isolation devices are supplied that preclude the possibility of an adverse effect being fed into the safety systems from the common components and the possibility of a fault in one safety system being propagated into other safety systems.</p> <p>b) Sharing of physical facility:</p> <p>An SDS may share physical facilities and routes with other safety systems. However, adequate grouping of the components of such systems shall be provided to permit commissioning, operational, and maintenance control to be satisfactorily administered. A single credible fault in one system should not adversely affect the other system.</p> <p>c) Sharing of power:</p> <p>At the final utilization level, the power distribution arrangements to the safety systems shall contain separate protective devices and disconnects for each system. If common power sources (e.g., electric, pneumatic, hydraulic) are employed, then the system designs shall be demonstrated to be free from the adverse consequences of failures in</p>	<p>be difficult to achieve complete separation of equipment location and inter-connection routing for each shutdown system from every other Special Safety System. This limitation let two group separation approach where SDS1 belongs to Group 1 and SDS 2 grouped with Group 2.</p> <p>The requirements from this clause (4.1.6.2) are a required minimum for each shutdown system from other Special Safety Systems as stated in 2.9.4.3 of the SDS1 Design Manual [NK29-DM-63720-001 Rev.7] and the SDS2 Design Manual [NK29-DM-63730-001 Rev.11].</p> <p>Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0]. Therefore, the design is deemed in compliance.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	those sources (e.g., decreasing or increasing potential levels, superimposed noise, dirty fluid, changing fluid characteristics).		
4.1.7	A failure in support power (electrical or compressed air) shall not prevent the SDS from performing its function.	<p>Per Section 2.12.3 of the Bruce B Design Manual for SDS1 [NK29-DM-63720-001 Rev. 7] and Section 2.12.3 of the Bruce B Design Manual for SDS2 [NK29-DM-63720-001 Rev. 11] redundancy requirement states that the shutdown system shall incorporate sufficient redundancy to ensure that no single failure results in the loss of its protective action.</p> <p>Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p>	C
4.1.8		This is not a requirement/guidance clause (this is a title only).	NA
4.1.8.1	The SDS shall have provision for the operator to trip the reactor manually in the main control room and in the secondary control room.	<p>Established in the Design Manual for Bruce B SDS1 [NK29-DM-63720-001 Rev. 7], Section 2.15(b): "The trip logic shall incorporate provisions for manually initiating an SDS1 reactor trip and they shall be located in the Main Control Room". To minimize the possibility of common mode effects or cross-links from disabling both shutdown systems per Section 2.9.4.1(e) "Spaces in the Secondary Control Area (SCA) shall be provided for SDS2 control equipment including a trip button and parameter display. No SDS1 equipment shall be located in the SCA" [NK29-DM-63720-001 Rev.7].</p> <p>Established in the Design Manual for Bruce B SDS2 [NK29-CM-63730-001 Rev.11] Section 2.1.4.3(b): "The trip logic shall incorporate provisions for manually initiating shutdown action. The pushbutton shall be located in the main control</p>	C

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>room. An additional means for manually actuating SDS2 shall be provided in the secondary control area remote from the main control room."</p> <p>Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p>	
4.1.8.2	<p>The manual trip facility shall allow the operator to trip each channel individually or to trip all of the channels together in one action. The means for manual actuation and for monitoring shutdown status shall be provided in the main control room for each SDS. For new plants, manual actuation and monitoring for each SDS shall be provided in the secondary control room.</p> <p>Note: For some existing CANDU plants, manual actuation and monitoring for one SDS is provided in the secondary control room.</p>	<p>The design manual for SDS1 [NK29-DM-63720-001 Rev.7] requires in section 2.1.4.3(b) that, "The trip logic shall incorporate provisions such as a pushbutton, for manually initiating a shutdown. The manual trip shall allow an individual channel to be put in a tripped state." Per Section 2.1.4.1(b), "Manual actuation is acceptable as a 'trip parameter'..." and per Section 2.1.4.4 (a), "continuous displays of the trip variables and their trip set points shall be presented to the operator on the main control panels as part of the shutdown system itself."</p> <p>The design manual for SDS2 [NK29-DM-63730-001 Rev.11] requires in Section 2.1.4.3(b) that, "the manual trip facility shall also allow an individual channel to be put in a tripped state." Per Section 2.1.4.1(b), "Manual actuation is acceptable as a 'trip parameter'..." and per Section 3.1.3.1.2 "Information on the trip parameters, plus status and operation of the system is displayed on the SDS2 panel". A SDS2 panel is located in the main control room per Section 3.1.2.2.</p> <p>The SDS2 logic processing for the two manual trip push buttons and one test trip push button are shown in Figure 6-7 (see Part 2 of the Bruce Power Safety Report [NK29-SR-01320-00001 Rev.5]).</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
4.2		This is not a requirement/guidance clause (this is a title only).	NA
4.2.1		This is not a requirement/guidance clause (this is a title only).	NA
4.2.1.1	<p>The reliability evaluation shall demonstrate that the reliability of the shutdown function from all credited means is such that the cumulative probability of failure to shutdown on demand can be shown to meet its requirement. The contribution of all sequences, involving failure to shutdown, to the large release frequency shall be less than the target stated in regulatory requirements.</p> <p>Notes:</p> <ol style="list-style-type: none"> <li>General requirements on reliability and reliability analysis for safety systems can be found in CSA N290.0, Clause 4.5.</li> <li>The probability of an SDS failure on demand for existing CANDU plants is typically lower than 1E-3.</li> <li>CNSC RD/GD-98 requires a licensee who constructs or operates an NPP to develop and implement a reliability program that assures that the systems important to safety can and will meet their defined design and performance specifications at acceptable levels of reliability throughout the lifetime of the NPP.</li> </ol>	<p>Implementing and maintaining a reliability program in accordance with RD/GD-98 [Reliability Programs for Nuclear Power Plants] is a licence condition as specified in PROL 18.00/2020 (see Section 6.1 of the LCH [NK29-CORR-00531-12545]).</p> <p>The reliability requirements for shutdown systems are to have an unavailability of less than <math>10^{-3}</math>. As presented in Section 6.1.1 of Part 2 of the Safety Report [NK29-SR-01320-00002, Rev. 005] to provide a high degree of assurance that a special safety system will perform as designed when called upon to do so, the unavailability target of each is limited to less than 1E-3 year/year.</p> <p>The reliability targets are specified in the design manuals. The annual reliability reports show that the predicted future unavailability for SDS1 and SDS2 are lower than <math>10^{-3}</math> for the period of 2011-2015 (see Enclosure 1 to NK29-CORR-00531-13197, Bruce Power Letter, F. Saunders to K. Lafreniere, April 28, 2016).</p> <p>Refer to assessment of clause 8.4.2 of CNSC REGDOC-2.5.2. The following information is extracted from Level 2 At-Power Summary Report, B0900/RP/055 R01, December 2013 (see NK21-CORR-00531-10958/NK29-CORR-00531-11342, Enclosure 4, Submission of S-294 Probabilistic Risk Assessment Deliverables, Bruce Power letter, F. Saunders to R. Lojk, December 24, 2013): from Level 1 PRA, Fuel Damage Category 1 (FDC1) represents all sequences</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
		involving rapid accident progression resulting from failures to shutdown the reactor when required. FDC1 is conservatively assumed to cause early consequential containment failure with a 0.5 probability and the failure sequence is assigned to a unique PDS, PDS1. Release Categories (RCs) are defined to bin the consequences associated with containment event tree end-states to facilitate comparison with safety goals. RC0 consists of single unit events (PDS1), two-unit events (PDS3A) and three- or four-unit events (PDS3). The contributions to RC0 of PDS3 and PDS3A are 94% and 4%, respectively, meaning that the contribution of PDS1 to RC0 is approximately 2%. The frequency of RC0 is included in the LRF calculation. RC0 frequency is 4.71E-6, which means that the contribution to it from PDS1 is 9.42E-8. This is below the target for the contribution of all sequences involving failure to shutdown to the large release frequency of the safety goals of 10-7/yr.	
4.2.1.2	Existing CANDU plants may meet reliability requirements by demonstrating SDS availability. If this approach is taken, each SDS shall have a demonstrated unavailability that meets its requirement. An SDS shall be considered to be available only when it meets all its minimum allowable performance standards. All the components in the trip chain shall be included in the SDS unavailability calculations.  Notes: 1) The SDS demonstrated unavailability requirement for existing CANDU plants has been	Each system is designed for an unavailability of less than 1E-3 yr/yr, shutdown system reliability is monitored and reported regularly and has usually been substantially better than the 1E-3 yr/yr unavailability requirement as noted in Section 1.1.3 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev.5].	C




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>1E-3 years per year due to all causes. (This is equivalent to a maximum of one failure out of 1000 demands for SDS action.)</p> <p>2) The unavailability is demonstrated by actual direct SDS experience or reasonable extrapolation from it, in conjunction with the test frequency. The causes to be included in the analysis are random component failures, operator disabling of the SDS, common-cause failures, and safety support system failure.</p>		
4.2.2	<p>The SDS should be designed to keep spurious actuation at a low frequency. The design target for inadvertent operation of an SDS due to random component failures should be specified.</p> <p>Note: A typical target for an existing CANDU plant is less than one sudden, unnecessary shutdown per year due to all causes.</p>	<p>Section 2.12.1, of SDS1 design manual [NK29-DM-63720-001 Rev.7] requires that, "the design target for inadvertent operation of a shutdown system due to random component failures shall be 1E-1 occurrences /year or less".</p> <p>Section 2.12.1 of SDS2 design manual [NK29-DM-63730-001 Rev.11] requires that, "The design target for inadvertent operation of a shutdown system due to random component failure shall be 1E-1 occurrences/year or less".</p> <p>Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p>	C
4.2.3	<p>The SDS design should be simple, conceptually and physically, to facilitate achievement of high performance reliability.</p>	<p>A design principle which applied to the design of a shutdown system fir SDS1 per Section 3.1 of [NK29-DM-63720-001 Rev.7] is to "keep the system simple. Use the minimum amount of equipment that will adequately do the job".</p> <p>Similarly, the design principles which should be applied to the design of a shutdown system for SDS2 per Section 2.23 of</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>[NK29-DM-63730-001 Rev.11] are to "keep the system simple and use the minimum amount of equipment that will do the job adequately."</p> <p>Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p> <p>This principle is also described in Section 1.1.1 of Part 2 of the Bruce Power Safety Report [NK29-SR-01320-00001 Rev.5].</p>	
4.2.4	<p>To improve reliability, stored energy should be employed to achieve the shutdown action.</p> <p>Note: Examples of the use of stored energy in shutdown are</p> <ul style="list-style-type: none"> <li>a) the use of gravity to move shutoff rods into the core;</li> <li>b) the acceleration of shutoff rod insertion by release of compressed springs (CANDU); and</li> <li>c) the injection of neutron-absorbing liquids by release of compressed gas or hydraulic fluid into the injection system.</li> </ul>	<p>Both shutdown systems employ stored energy to achieve their action:</p> <p>SDS1 uses 32 gravity-drop, spring assisted shutoff rods, when the rod is fully withdrawn a spring is compressed to 450N and held in compression by the clutch. This results in a drop time shorter than could be achieved by unassisted free fall.</p> <p>SDS2 opens fast acting valves to inject the gadolinium poison into the moderator using pressure helium.</p> <p>Section 6 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev. 5].</p>	C
4.2.5	<p>The effectiveness of the MSD (i.e., speed of action and shutdown reactivity margin) shall be such that specified limits are not exceeded and the possibility of re-criticality or reactivity</p>	<p>Acting alone, for the accident conditions identified in part 3, both SDS1 and SDS2 have sufficient reactivity depth and act with sufficient speed so that the reactor siting criteria is met.</p> <p>Section 6 of the Bruce B Safety Report Part 2 [NK29-SR-</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
	excursion following a PIE is minimized.	01320-00001 Rev. 5].	
4.2.6	<p>The design should aim for fail-safe operation of its SSCs where such an option exists, while maintaining a balance with simplicity.</p> <p>Note: The requirement for fail-safe operation appears in CSA N290.0, Clause 4.8.</p>	<p>Section 2.1.4.2 of SDS1 design manual [NK29-DM-63720-001 Rev.7] and SDS2 design manual [NK29-DM-63730-001 Rev.11] provide system functional safety considerations for a fail-safe design, particularly bullet (a) requires that "shutdown systems devices shall be fail-safe (i.e. failure of the device should cause a trip instead of inhibiting a trip) where such a choice is available".</p> <p>Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p> <p>However, there remain instances where the failure mode is unsafe and SDS reliability is dependent on panel monitoring or testing by the Operator. For example the ion chamber log N and log rate signals fail unsafe for loss of polarizing voltage (See section 5.17(5) of [CMT-60544-00003 Rev.002]). This is a gap.</p>	Gap
4.3		This is not a requirement/guidance clause (this is a title only).	NA
4.3.1		This is not a requirement/guidance clause (this is a title only).	NA
4.3.1.1	<p>SDS trip parameters shall be selected to sense the plant conditions of concern that result from the PIEs considered in the plant design.</p> <p>Notes:</p> <p>1) Examples of SDS trip parameters for a</p>	<p>As required by section 2.1.4.1(a) for SDS1 [NK29-DM-63720-001 Rev.7] and SDS2 [NK29-DM-63730-001 Rev.11] the trip parameters "shall be selected on the basis of appropriateness for the plant conditions of concern in response to the postulated process failures being considered in the design". Table 3-3 of the SDS1 design manual [NK29-DM-63720-001 Rev.7] provides a simplified trip coverage</p>	C


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>CANDU NPP are neutron overpower, high rate of change of neutron flux, high (or low) primary heat transport system (PHTS) pressure, PHTS low flow, and steam generator low level.</p> <p>2) Annex B provides a list of postulated failures for CANDU reactor</p>	<p>summary for design basis accidents. Table 3-2 of the SDS2 design manual [NK29-DM-63730-001 Rev.11] provides trip coverage for postulated serious process failures.</p> <p>Table 6-1 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev.5] provides a summary of the reactor trips for SDS1 and SDS2.</p>	
4.3.1.2	There shall be two diverse SDS trip parameters to protect against a PIE, unless it is impracticable or it can be shown that failure to trip when a single trip parameter is provided will not lead to unacceptable consequences.	Except for a few cases where limited windows of single trip coverage exist, at least two diverse trips are demonstrated to be effective for each analyzed event. The limited windows of single trip coverage are justified by the impracticality of closing them, as discussed in Section 1.6 of the Bruce B Safety Report Part 3 [NK29-SR-01320-00002 Rev.005].	IC
4.3.1.3	<p>Where the design allows to condition out (bypass) trip parameters manually or automatically, the design shall condition the trip parameter back in automatically whenever the process conditions change to make the trip effective.</p> <p>Note: These conditions normally occur at low reactor power.</p>	<p>Table 3-4 of SDS1 design manual [NK29-DM-63720-001 Rev.7] and Table 3-1 of SDS2 design manual [NK29-DM-63730-001 Rev.11] identify trip conditioned out on percentage of full power.</p> <p>Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p> <p>Some SDS process parameters are subject to conditioning. A parameter is allowed to be "conditioned out" if reactor power is sufficiently low that a trip is not required if a process failure for which the parameter is credited occurs. "Conditioning out" of process parameters often requires manual action in combination with an automatic permissive based on reactor power. Manual conditioning is provided to reduce the chance of a common mode failure across several parameters as a result of a problem with reactor power</p>	C

 <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


Article No.	Clause Requirement	Assessment	Compliance Category
		<p>measurement. However "conditioning in" of these parameters is typically automatic to improve reliability as per Bruce Power training manual [CMT-60544-00003]. The process trip parameters are described in SDS Design Manuals.</p> <p>As such, this meets the requirements of the clause and is deemed in compliance</p>	
4.3.1.4	<p>In order to credit (in the safety analysis) operator action to shut down (manually trip) the reactor, the design shall provide</p> <p>a) clear, well-defined, validated, and readily available operating procedures that identify the necessary actions;</p> <p>b) instrumentation in the control rooms to provide clear and unambiguous indication of the necessity for operator action;</p> <p>c) adequate time before operator action is required, following indication of the necessity for operator action inside the control rooms; and</p> <p>d) adequate time before operator action is required, following indication of the necessity for operator action outside the control rooms.</p> <p>Notes:</p> <p>1) For new plants, adequate time is at least 30 min for operator action inside the control room and 60 min for operator action outside the control room.</p>	<p>A summary of operator actions required as part of the safety analysis are summarized in Table 1-1 through Table 1-10 of the Bruce B Safety Report Part 3 [NK29-SR-01320-00002 Rev.5].</p> <p>(a) The plant has operating procedures that identify the necessary actions, operator training and reliable instrumentation designed to provide clear unambiguous indication of the need to take action, whether promptly or not. The procedures are clear, well-defined, and readily available in the Abnormal Incidents Manual [NK29-AIM-03600.1 Rev. 057].</p> <p>(b) The SDS1 MCR panel contains a separate alarm window system, which will indicate the state of trip parameters and trip channels, per section 3.6.3 of the design manual [NK29-DM-63720-001 Rev.7]. The SDS2 MCR panel contains a separate annunciation window system, which indicates the state of trip parameters, conditioning setpoints and trip channels per section 3.1.3.1.1 of the Bruce B SDS2 design manual [NK29-DM-63730-001 Rev.11].</p> <p>(c) Part 3 of the Bruce B Safety Report [NK29-SR-01320-00002 Rev.5] in Table 1-1 to Table 1-10 provides a summary of the operator actions credited for various accident categories, noting where an operator is required to manually</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	2) For existing CANDU plants, adequate time is 15 min for operator action inside the control room and 30 min for operator action outside the control room.	<p>trip the reactor.</p> <p>As identified in Table 1-3, analysis of HTS depressurization due to steam bleed valves open with pressurizer heaters off and multiple failures of the bleed condenser to isolate, operator action to manually trip the reactor was credited at 12 minutes in order to prevent sheath dryout (see Appendix 3, Section 3.5.4.2 of Part 3 of the Safety Report). Additionally, analysis of HTS depressurization due to spurious opening of the two pressurizer steam relief valves, operator action to manually trip the reactor was credited at &gt;12 minutes, steam relief valves have approximately one-fifth the capacity of the steam bleed valves and therefore the occurrence of automatic system actions, and the time available for operator actions are correspondingly longer (See Appendix 3, Section 3.5.4.3).</p> <p>Subsequent to that analysis, analysis of Breaks at the Top of the Pressurizer (see Appendix 4, Section 4.2.2.3.1.3 of Part 3 of the Safety Report), which have a similar system response, has shown that manual trip at 15 minutes is effective for discharge rates of less than 100 kg/s.</p> <p>For control failures which lead to sustained discharge from the pressurizer low pressure and low flow SDS1 trips (HTLP,HTLF) provide effective protection (see Section 3.2.1.2.1 of Part 3 of the Safety Report). However, the manual trip within 12 minutes ensures that no dryout occurs. Given that multiple failures of the bleed condenser to isolate must occur for the discharge to be sustained, manual action at 12 minutes is considered an acceptable in terms of providing backup trip coverage on SDS2 (see Section 3.5.7 item (b) of Part 3 of the Safety Report).</p>	



 <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>Although considered acceptable in terms of providing backup coverage on SDS2, in the current analysis, the credited 12 minutes is not considered adequate time (less than 15 minutes) and is therefore considered a gap.</p> <p>(d) Operator action to shutdown (manually trip) the reactor, outside the main control room is not credited in Part 3 of the Safety Report [NK29-SR-01320-00002 Rev.5].</p>	
4.3.2		This is not a requirement/guidance clause (this is a title only).	NA
4.3.2.1	A trip function may be initiated by either the state of a single parameter or the state of a combination of parameters, e.g., a conditioned trip parameter. All components used to generate such trip functions shall be considered part of the SDS and shall meet the requirements of this Standard.	<p>Each process and nuclear measurement loop that is essential for the operation of a special safety system is designed to be redundant (duplicated, or triplicated) such that a single loop component or power supply failure cannot incapacitate a special safety system or spuriously invoke its operation (see Section 6.1.2 of Part 2 of the Bruce B Safety Report [NK29-SR-01320-00001 Rev.5].</p> <p>Equipment design requirements define equipment operating characteristics to meet the system design requirements. The equipment design characteristics can be subdivided for three categories of equipment for SDS1 and SDS2, namely:</p> <p>For SDS1: (a) Sensing Instrumentation, (b) Trip Logic, and (c) Shutoff Rods. For SDS1 there are three neutronic trips in addition to the seven trip parameters (see Section 2.1.3.1.1 of the Bruce B SDS1 design manual [NK29-DM-63720-001 Rev.7]).</p> <p>For SDS2: (a) sensing instrumentation, (b) trip logic and (c) poison injection. For SDS2 there are three neutronic trips in addition to the six process trip parameters (stated in section 2.1.3.1.1 of the Bruce B SDS2 design manual [NK29-DM-</p>	C

 <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>63730-001 Rev.11].</p> <p>Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p>	
4.3.2.2	<p>All trip sensors and their associated instruments shall provide long-term, reliable service under all required operating conditions. The sensors shall be qualified to meet their performance requirements, including response time, for their mission times.</p> <p>Note: The accident analyses in the NPP safety report are based on the SDS performing as designed.</p>	<p>Instrumentation and control systems are designed for very high reliability and availability, both the maximize plant availability and for safety. The reliability is achieved through component selection, and redundancy. Equipment is designed for a minimum of regular maintenance (see Section 7.1.6 of the Bruce B Safety Report Part 3 [NK29-SR-01320-00001 Rev.005]).</p> <p>The design shall take into account the possible failure modes which could adversely affect the sensors (see Section 2.1.4.1 of the Bruce B design manual for SDS1 [NK29-DM-63720-001 Rev.7], and SDS2 [NK29-63730-001 Rev.11]). The accident analysis in Part 3 of the Safety Report is based on SDS1 and SDS2 performing as designed per Table 3-2 (Trip setpoints and time delays used in the analysis) [NK29-SR-01320-00002 Rev.5]. Surveillance verifies that the time response of the trip is within the limits specified in Table 4.1-4 of the Operational Safety Requirements for Bruce B Shutdown Systems [NK29-OSR-63720-63730-00001 Rev.1], which provides the Safety Analysis limits for delays and time constants.</p> <p>Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p>	C


Article No.	Clause Requirement	Assessment	Compliance Category
4.3.2.3	The sensors and their associated instruments shall have provisions for calibrating their signals to the required accuracy.	<p>SDS1 and SDS2 design principles require that the system be designed "such that it may be tested and calibrated at any time" (see the Section 3.1 of the Bruce B design manual for SDS1 [NK29-DM-63720-001 Rev.7], and SDS2 [NK29-DM-63730-001 Rev.11]). Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p> <p>Loop calibration is a complete check of the instrument loop, including the sensor. The surveillance verifies that the instrument loop responds to the measured parameter within the necessary range and accuracy (see section 4.3.3 of [NK29-SOR-63720-63730-00001 Rev.1].</p>	C
4.3.2.4	Neutron flux detectors and their associated instruments shall not be credited outside their operating range of sensitivity. When a single type of flux detector is not sensitive over the required operating range, additional detectors of a different type shall be employed. The operating ranges of the detectors selected shall overlap by an appropriate margin.	<p>Where a single type of detector does not cover the full operating range of concern, the detectors selected shall overlap their ranges by an appropriate margin (e.g., overlapping range for ion-chambers and in-core flux detectors) are required per section 2.1.4.1 of the design manual for SDS1 [NK29-DM-63720-001 Rev.7] and section 2.1.4.1 of the design manual for SDS2 [NK29-DM-63730-001 Rev.11]. Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p> <p>An Action Request (AR 28013605) was initiated to demonstrate that the design changes to SDS1 and SDS2 NOP Flux detector amplifiers in the design manuals to incorporate revised calculations for Amplifier gain settings.</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>This status of this action is complete as of July 27, 2001.</p> <p>Section 7 of the Bruce B safety report [NK29-SR-01320-00001 Rev.5] notes there are three boron coated uncompensated ion chambers in the regulating system for measuring neutron flux 1E-7 to 1.5 times full power. In the power range above 15% full power, self-powered in-core flux detectors are used to provide accurate power information that is not available from the ion chambers. The response of the ion chambers is affected by flux tilts and by the concentration of poison in the moderator. The flux detectors are distributed throughout the core and can provide more accurate information on the bulk power level and its spatial distribution.</p>	
4.3.3		This is not a requirement/guidance clause (this is a title only).	NA
4.3.3.1	<p>The SDS instrumentation shall have provision to set trip set points.</p> <p>Note: Trip set points are normally set at predefined fixed values. Certain trip parameters require the trip set point to be automatically adjusted based on the value of other plant variables. When a set point has to be varied based on plant status information that is not available to the SDS, provision may be made to allow the operator to select pre- defined set points.</p>	<p>As summarized in Table 6-1 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev.5] the shutdown system instrumentation has provision to set trip set points.</p> <p>For a particular trip function, there may be one or more trip setpoints dependent upon the nature of the trip function. The trip setpoints may be manually or automatically adjusted depending on the state of the other plant variables per section 2.1.4.6 of the SDS1 design manual [NK29-DM-63720-001 Rev.7] and 2.1.4.5 of the SDS2 design manual [NK29-DM-63730-001 Rev.11]. Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p>	C
4.3.3.2	Where automatically adjusted set points are incorporated, the design of the set point adjusting	Per section 2.1.4.6 of the SDS1 design manual [NK29-DM-63720-001 Rev.7] and the SDS2 design manual [NK29-DM-	C


Article No.	Clause Requirement	Assessment	Compliance Category
	instrumentation shall be to SDS standards. The design shall ensure that failure of the set point adjusting instrumentation is automatically detected and alarmed and does not put the SDS in an unsafe condition.	<p>63730-001 Rev.11], where automatically adjusted setpoints are incorporated, the design of the setpoint adjusting instrumentation shall be to shutdown system standards. Automatically adjusted setpoints are incorporated to protect systems, for example:</p> <p>SDS1 high neutron power trip is reduced automatically on low HT flow to provide protection in case of three HT pump operation 30 seconds after HT low flow (85%) is detected by feeder flow loops. Section 3.8 of the SDS1 design manual, part 5 Section A High Neutron Power Trip [NK29-DM-63720-005A Rev.6].</p> <p>The neutron overpower trip setpoint is automatically reduced on low heat transport differential pressure to assure trip coverage during three PHTS pump operation per Section 3.4 (q) of SDS2 design manual [NK29-DM-63730-001 Rev.11] and Section 7.3.3 of the SDS2 design manual part 5, Process Trips Information [NK29-DM-29-63730-005 Rev.10].</p> <p>Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p>	
4.3.3.3	Adjustment of trip set points shall be controlled physically or procedurally to prevent manual adjustment without proper authorization.	As prescribed in Section 63.4 in Operating Policies and Principles - Bruce B [BP-OPP-00001 Rev.19], manual adjustment of the trip setpoints shall only be made following procedures approved by the Senior Operation Authority.	C
4.3.3.4	Trip set points shall be selected to provide sufficient allowance between the set points and	Preparation of SOE Instrument uncertainty calculations was completed following the Bruce Power methodology	C

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>corresponding safety analysis limits to account for uncertainties. The uncertainties include but are not limited to</p> <ul style="list-style-type: none"> <li>a) instrument calibration uncertainties;</li> <li>b) instrument uncertainties during normal operation;</li> <li>c) instrument drift;</li> <li>d) instrument uncertainties caused by design basis events;</li> <li>e) process-dependent effects;</li> <li>f) calculation effects;</li> <li>g) dynamic effects; and</li> <li>h) calibration and installation bias accounting.</li> </ul> <p>Notes:</p> <ul style="list-style-type: none"> <li>1) Based on ANSI/ISA-67.04.01.</li> <li>2) Set point margins should accommodate normal operational transients to minimize spurious trips without compromising the safety margin.</li> </ul>	<p>documented in file [B-REP-03602-00001 Rev.0]. The methodology was based on ISA standard for nuclear Safety-Related System set-point determination (ANSI/ISA-S67.04.01) and the associated recommended practice ISA-RP67.04.02, per note 1 of this clause.</p> <p>For SDS1;</p> <p>Uncertainties and Allowable Values are calculated in the CALC note [NK29-CALC-63720-00001 Rev. 05] to provide design and operational information for Safe Operating Envelope parameters as required for the SOE compliance program. Which includes, in the respective sections, the following information :</p> <p>(a) As-found and as-left tolerances for instrument calibration purposes (Table 3-1b, Table 3-1c in [NK29-CALC-63720-00001 Rev. 05]).</p> <p>(b) Instrument uncertainty calculation tables (see Section 2.0 and Appendix A of [NK29-CALC-63720-00001 Rev. 05]).</p> <p>(c) Instrument Drift per (Appendix A of [NK29-CALC-63720-00001 Rev. 05]) noted as generally based on the EPRI Instrument Drift Study for the Bruce NGS.</p> <p>(d) Uncertainties caused by the limiting design basis accident including any systematic errors is considered as part of this assessment (see Section 1.0 of [NK29-CALC-63720-00001 Rev. 05])</p> <p>(e) process-dependent effects, as defined by ANSI/ISA-S.67.04.01 means "the determination of trip setpoint allowance shall account for the process variable. Examples are (but not limited to) the effect of fluid stratification on temperature measurement, the effect of changing fluid</p>	




 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>density on level measurements, and process oscillations or noise." Such process effects are included in the report with the exception of SOE uncertainties associated with instrument or process response times (note that time relays are not exceptions because the time is a component of the design function), and those related to an equipment characteristic that cannot be measured directly (see Section 1.1 of [NK29-CALC-63720-00001 Rev.5]).</p> <p>(f) calculation effects, "The safety analysis Limits defined in the OSR document for this system include any applicable simulation errors in the modeling and computer simulation of the limiting DBA" (per section 2.0 of [NK29-CALC-63720-00001 Rev.5]).</p> <p>(g) dynamic effects, as defined by ANSI/ISA-S.67.04.01 "behavior of a channel's output as a function of the input with respect to time shall be accounted for". This has been accounted for. For example, in the conditioning signal uncertainties "if power levels are changing, there will be detector signal delays and errors due to under or over compensation by the Dynamic Signal Conditions resulting in errors (uncertainty)" (see Appendix C of [NK29-CALC-63720-00001 Rev.5]).</p> <p>(h) Calibration and installation bias accounting- such biases are accounted for in the uncertainty calculations and are shown in Appendix A [NK29-CALC-63720-00001 Rev.5].</p> <p>For SDS2;</p> <p>Uncertainties and Allowable Values are calculated in the CALC note [NK29-CALC-63730-00001 Rev. 03] to provide</p>	

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>design and operational information for Safe Operating Envelope parameters as required for the SOE compliance program. Which includes, in the respective sections, the following information :</p> <p>(a) as-found and as-left tolerances for instrument calibration purposes (Table 3-1b, Table 3-1c in [NK29-CALC-63730-00001 Rev. 3])</p> <p>(b) instrument uncertainty: calculation tables (see Section 20 and Appendix A of [NK29-CALC-63730-00001 Rev. 3])</p> <p>(c) Instrument Drift: per (Appendix A of [NK29-CALC-63730-00001 Rev. 3]) noted as generally based on the EPRI Instrument Drift Study for the Bruce NGS.</p> <p>(d) Uncertainties caused by the limiting design basis accident including any systematic errors is considered as part of this assessment (see Section 1.0 of [NK29-CALC-63730-00001 Rev. 3])</p> <p>(e) process-dependent effects: Such process effects are included in the report with the exception of SOE uncertainties associated with instrument or process response times (note that time relays are not exceptions because the time is a component of the design function), and those related to an equipment characteristic that cannot be measured directly (see Section 1.1 of [NK29-CALC-63730-00001 Rev.3].</p> <p>(f) calculation effects: per section 2.0, "The safety analysis Limits defined in the OSR document for this system include any applicable simulation Errors in the modeling and computer simulation of the limiting DBA" [NK29-CALC-63730-00001 Rev.3].</p> <p>(g) dynamic effects: This has been accounted for. For</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>example, in the conditioning signal uncertainties "if power levels are changing, there will be detector signal delays and errors due to under or over compensation by the Dynamic Signal Conditions resulting in errors (uncertainty)" (see Appendix C of [NK29-CALC-63730-00001 Rev.3]).</p> <p>(h) Calibration and installation bias accounting: such biases are accounted for in the uncertainty calculations and are shown in Appendix A [NK29-CALC-63730-00001 Rev.3].</p> <p>Bruce A and B have completed their baseline SOE projects which consisted of documenting the limits and conditions derived from the safety analysis in OSRs, and completing the corresponding Instrument Uncertainty Calculations (IUCs) that are considered in setting the OLCs.</p>	
4.3.4		This is not a requirement/guidance clause (this is a title only).	NA
4.3.4.1	<p>The SDS design in a particular plant shall employ general or local coincidence, or both, to balance the required safety reliability, system testability, and the need to keep the frequency of spurious SDS action low. With local coincidence, adequate isolation techniques shall be employed to ensure that any credible, internally generated faults within one channel do not adversely affect the operation of the remaining channels.</p> <p>Note: Trip logic, which could be of the general coincidence or local coincidence type or, possibly, some combination of the two, is described as follows:</p>	<p>SDS1 uses local coincidence logic. Two out of three sensors in the same parameter must trip to initiate an SDS1 reactor trip. There are three independent channels from the sensor location to trip relays (see Section 6.2.5 of the Bruce B Safety Report [NK29-SR-01320-00001 Rev.5]).</p> <p>SDS2 uses general coincidence logic. There are three independent channels. They are independent from the sensor location through the trip relays to the solenoid trip valves. Any combination of parameter trips on two of three channels will initiate poison injection. A two-out-of-three poison valve configuration and the low wattage requirements of the solenoid valves permit a reliable design, with the parameter trip relays de-energizing the solenoids directly (see section 6.2.5 of the Bruce B Safety Report [NK29-SR-</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>a) With general coincidence logic, the final shutdown action is initiated by the actuation of any trip sensor in one instrumentation channel combined with the actuation of any trip sensors in the other instrumentation channels (e.g., in a three-channel CANDU system, high PHTS pressure in one channel, high neutron power in another channel). With local coincidence logic, the final shutdown action is initiated only by the actuation of trip sensors measuring the same parameter in each instrumentation channel (e.g., in a three-channel CANDU system, high PHTS pressure in each of two channels).</p> <p>b) General coincidence logic permits a greater degree of functional independence between the channels of a system. This is counterbalanced by a greater probability of spurious SDS action.</p> <p>c) Local coincidence logic gives a greater immunity to spurious SDS action. This is counterbalanced by possible decreases in channel functional independence and testing capabilities due to interconnections between channels, if appropriate design measures are not taken.</p> <p>d) Means should be provided for easily putting a given parameter into the tripped state. This is particularly important with local coincidence logic, when it might not be sufficient just to trip the logic channel manually.</p>	01320-00001 Rev.5)].	

Article No.	Clause Requirement	Assessment	Compliance Category
4.3.4.2	As the manual trip facility is an area of possible cross-linking between redundant instrumentation channels, suitable measures shall be taken in the design to ensure independence between channels.	Separation of the instrumentation channels of the two shutdown systems is achieved by channelization. Each of the three channels on a specific special safety system follows a separate route. Adequate separation is maintained by using associated channels. Separation is also achieved between channels following a common route by routing the channels in separate cable pans. Channelization ensures that the three cable routes are separated, that the equipment associated with the three sets of channels is located in three different rooms, and that power to the three sets of channels is supplied by three different buses. Consequently, any credible local common mode event can affect only one set of channels, leaving the other two unimpaired and thus the special safety systems remain functional. Section 6.1.5 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001 Rev. 5].	C
4.3.4.3	The manual shutdown logic shall be hard wired and should be made as direct as possible (i.e., by minimizing the amount of equipment common to both the automatic trip logic and manual trip logic).	<p>As required by the SDS1 and SDS2 design manuals the manual shutdown facility (logic) shall be as direct as possible, i.e., minimizing the amount of equipment common to both the automatic trip logic and manual trip logic, per section 2.1.4.3 [NK29-DM-63720-001 Rev.7] and [NK29-DM-63730-001 Rev.11].</p> <p>Manual shutdown logic for SDS1 is hardwired. A manual channel trip is initiated by depressing a pushbutton located the main control room panel (66100-PL7B). The pushbutton opens the series chain and causes the channel trip relays, open causing LEDs to illuminate. By depressing pushbuttons of any two channels or by depressing the common "trip bar" which activates all three pushbuttons will cause a complete reactor trip, shutoff rods drop. See the Manual Chanel Trip</p>	C


Article No.	Clause Requirement	Assessment	Compliance Category
		<p>requirements are 4.1.3(a) of [NK29-DM-29-63720-003 Rev.6].</p> <p>Manual shutdown logic for SDS2 is hardwired. A channel can be manually tripped by depressing a pushbutton located on the main control room panel (6610-PL8B) or secondary control area panel (PL 1902). A channel trip, de-energizes the solenoids for the two helium injection halves and the helium vent valve for that channel. See section 3.2 and section 4 channel trip logic operation from the Bruce B SDS2 design manual [NK29-DM-29-63730-003 Rev.10].</p> <p>Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p>	
4.3.4.4	The design of the trip logic and the system as a whole shall be such as to minimize any need for operator intervention or manual action during an accident.	<p>The respective SDS1 and SDS2 design manuals require that the design of the trip logic and the system as a whole shall be such as to minimize any need for operator intervention or manual action during an accident. See Section 2.1.4.3 of the design manual for SDS1 [NK29-DM-63720-001 Rev.7] and Section 2.1.4.3 of the design manual for SDS2 [NK29-DM-63730-001 Rev.11]. Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p> <p>Operator intervention or manual action required to shut-down the reactor is assessed under clause 4.3.1.4 of this standard.</p>	C
4.3.5		This is not a requirement/guidance clause (this is a title only).	NA




Article No.	Clause Requirement	Assessment	Compliance Category
4.3.5.1	When the intended shutdown action, as determined by the trip sensors is initiated, the action shall go through to completion automatically.	<p>For the design manual requires that for the SDS1 and SDS2 systems: when the intended shutdown action, as determined by the trip sensors, is initiated and sealed-in, the action shall go through to completion automatically.</p> <p>See Section 2.1.4.5 of the Bruce B: SDS1 Design Manual [NK29-DM-63720-001 Rev.7] and SDS2 Design Manual [NK29-DM-63730-001 Rev.11]. Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p>	C
4.3.5.2	For existing CANDU plants that have seal-in delay time, the final shutdown action shall be sealed-in before the action of the reactivity components starts to modify the values of the initiating trip parameters.	<p>The final shutdown action for SDS1 shall be sealed-in before the action of the reactivity components start to modify the values of the initiating trip parameters. For SDS1 a value of 150 ms is currently being used. See the Bruce B design manual for SDS1 [NK29-DM-63720-001 Rev.7].</p> <p>For SDS2, for Bruce 'B' a trip seal-in relay is provided with sufficient time delay such that beyond the specified time delay, the relay seals the trip logic and keeps the valves open. The time delay is set at 150 ms (see Section 3.1.2.2 of [NK29-DM-63730-001 Rev.11]. a channel trip seal-in feature with a delay of 150 ms shall be provided.</p> <p>Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p>	C
4.3.5.3	Resetting of the trip logic and repoising of the reactivity components subsequent to the trip	As required by the Bruce B design manual(s), resetting the trip action and recocking of the reactivity components	C

Article No.	Clause Requirement	Assessment	Compliance Category
	action shall be initiated only manually and shall not interrupt the completion of the shutdown action.	<p>subsequent to the trip seal-in shall only be initiated manually and shall not interrupt the completion of the shutdown action.</p> <p>See Section 2.1.4.5 item (c) of [NK29-DM-63720-001 Rev.7] for SDS1.</p> <p>See Section 2.1.4.5 item (c) of [NK29-DM-63730-001 Rev.11] for SDS2.</p> <p>Both systems are currently operating in accordance with the design basis, per the latest Condition Assessment Report for SDS1 [NK29-CAR-63720-0001 Rev.0], for SDS2 [NK29-CAR-63730-00001 Rev.0].</p> <p>Per Section 63.7 of the Operating Policies and Principles for Bruce B Shift Manager authorization is required prior to resetting all reactor trips [BP-OPP-00001 Rev.19].</p>	
4.3.5.4	The design shall be such that it is not readily possible for an operator to prevent actuation of an SDS when such actuation is required.	<p>All shutdown system actions that are required in the short term are automatic for all accidents considered at Bruce B. There are no requirements for operator action for trip initiation or any means of inhibiting the trip initiation, and once initiated the operator cannot stop such actions. The complete list of operator actions credited in the Safety Report is given in Tables 1-1 through 1-10 of Section 1.3 of Part 3 of the Safety Report [NK29-SR-01320-00002, Rev.005].</p> <p>Per clause 4.3.5.2 of this standard a seal-in time is provided for SDS1 and SDS2. For example for SDS1 for Bruce B when the intended shutdown action as determined by the trip sensors, is initiated and sealed-in, the action shall go through completion automatically. A seal-in feature shall be provided to ensure that, if a tripped condition exists for more than a</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
		preset time the trip will be completed even if the signal is subsequently cleared (see section 2.1.4.4 of [NK29-DM-63720-001 rev.7]).	
4.3.6		This is not a requirement/guidance clause (this is a title only).	NA
4.3.6.1	<p>When digital equipment is employed to read inputs, execute software programs, and activate SDS reactivity components, the digital equipment shall be of high reliability for nuclear safety systems. Its software programs shall be developed, reviewed, verified, and validated in compliance with a recognized software development standard that is appropriate for nuclear safety systems. The process to develop the digital (computer) system shall conform to appropriate standards and guidelines for SDSs.</p> <p>Notes:</p> <ol style="list-style-type: none"> <li>1) This Clause applies to both the pre-development software (includes operating system, application software, function block or ladder logic software, and firmware) and the custom-developed software of the computer system.</li> <li>2) Software for SDSs is considered as having high safety significance. See CSA N290.14.</li> <li>3) For qualification of pre-developed software, see CSA N290.14.</li> </ol>	<p>The Bruce B design does not incorporate digital equipment to read inputs, execute software programs and activate SDS components this requirement is not applicable.</p> <p>Note the Bruce B design does incorporate a monitoring computer (see clause 4.4.1).</p>	NA

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


Article No.	Clause Requirement	Assessment	Compliance Category
4.3.6.2	The computerized SDS trip shall be channelized with adequate separation and independence between the channels to be immune to unsafe cross-links and common-cause events.	Since Bruce B design does not incorporate computerized SDS trips and safety related software; this requirement is not applicable.	NA
4.4		This is not a requirement/guidance clause (this is a title only).	NA
4.4.1	Continuous display of the trip parameter signals (values) and their trip set points shall be presented to the operator in the main control room. Display of appropriate trip parameter information of at least one SDS shall be presented in the secondary control room. Display of one SDS shall be independent of the other SDS.	<p>The monitoring computer is an operator aid intended to reduce the spurious reactor trip frequency and reduce safety system unavailability by detecting instrument failures.</p> <p>For SDS1, see section 3.6.4 of the Bruce B design manual [NK29-DM-63720-001 Rev.7]. The shutdown system monitoring computer hardware is described in DM-29-66460/66560-1 and software in DM-29-66460/66560-2.</p> <p>Per section 6.2.9, of the Bruce B safety Report Part 2 the SDS1 alarm messages are also displayed in the main control room on the safety system monitoring computer screen. In addition the messages are printed out on the main control computer printer time stamped and in sequence of occurrence [NK29-SR-01320-00001 Rev.5].</p> <p>For SDS2, see section 3.1.3.4 of the Bruce B design manual [NK29-DM-63730-001 Rev.11]. The shutdown system monitoring computer hardware and software are described in DM-29-66460/66560-1 and DM-29-66460/66560-2, respectively.</p> <p>Per section 6.3.8, of the Bruce B Safety Report Part 2 alarm messages for SDS2 are also displayed in the main control room on the unit display terminals and printed by printers</p>	C

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


Article No.	Clause Requirement	Assessment	Compliance Category
		<p>driven by the main control room [NK29-SR-01320-00001 Rev.5].</p> <p>Per section 6.3.6 of the Bruce B Safety Report Part 2, the SDS2 panel in the secondary control area contains displays of all SDS2 parameters with the exception of the high-neutron-power and HT low-core-differential pressure trips (log-of-neutron power indication however is provided) [NK29-SR-01320-00001 Rev.5].</p>	
4.4.2	For certain trip parameters, such as those that originate from in-core flux detectors, display of the margins to trip should be provided in the control room.	Per Section 6.6 of the Bruce B Safety Report Part 2, the special safety system monitoring function displays the margin to trip on the in-core flux detectors and annunciates an alarm if the margin on the detector falls below a threshold [NK29-SR-01320-00001 Rev.5].	C
4.5		This is not a requirement/guidance clause (this is a title only).	NA
4.5.1	The test facility may incorporate digital equipment (computers) to achieve an improvement in human factors. Computerized testing equipment and software programs should be assessed for safety category and developed to the appropriate level of software quality assurance.	<p>Bruce B design has no SDS computer testing equipment in use.</p> <p>Therefore; this requirement is not applicable.</p>	NA
4.5.2	SDS tests that are possible when the reactor is subcritical shall be done prior to first criticality and with the reactor in an appropriate shutdown state.	<p>Bruce B Safety Report, Bruce Power DM for SDS1 and SDS2, and OSR do not explicitly state SDS tests should be done prior to first criticality in the appropriate shutdown state.</p> <p>The SDS Design Manuals require commissioning tests to be carried out to demonstrate that all parts and functions of the system meet their design requirements under normal conditions. In addition, tests also to be carried out as far as</p>	NA

Article No.	Clause Requirement	Assessment	Compliance Category
		practical to determine that the system acts in a predicted and acceptable manner for faulted conditions (e.g., transient or temporary loss of power).	
4.5.3	Complete operational tests to demonstrate the effectiveness of each SDS shall be carried out at a frequency consistent with the reliability requirements of the safety system.	Special Safety Systems are tested on a regular basis. The systems are designed to facilitate testing of all system components and test frequencies are established to ensure that the defined reliability requirements are met.  Section 6.2.10 for SDS1 and 6.3.9 for SDS2 of the Bruce B Safety Report Part 2 [NK29-SR-00001 Rev. 5].	C
4.6	Consideration shall be given to cyber security for the digital SDS equipment.  Notes: 1) The intent of this Clause is to cover all aspects of cyber security including hardware, software design, software development, and operating environments, including maintenance. 2) Further guidance on cyber security can be found in IEEE 7-4.3.2 and IEC 61513.	Cyber security is addressed separately due to the sensitivity of the information.	RNA
4.7		This is not a requirement/guidance clause (this is a title only).	NA
4.7.1	Equipment for the SDS should a) be of a proven design (industrial experience); b) have a predictable failure mode;	For points a) and b), all SSCs important to safety have been in place at Bruce B for 30 years. The SSCs are designed based on the design of earlier plants and design changes have been based on design improvements that have been tested and proven elsewhere.	C




 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>c) be designed to facilitate test, maintenance, and repair; and</p> <p>d) have an expected operating life that is equal to or greater than the life of the plant.</p>	<p>For points c) and d), all SSCs important to safety are calibrated, tested, maintained, repaired (or replaced), inspected, and monitored over the lifetime of the plant. Testing, maintenance and repair are described in the operational safety requirements for the Bruce B shutdown systems [NK29-OSR-63720-00001 Rev.1]. SDS are also monitored under the Equipment Reliability Program as Tier 1 Systems Important to Safety,</p> <p>Each shutdown system was designed to allow on-power testing to demonstrate that it will meet its unavailability targets. Furthermore Bruce Power is committed to a maintenance and testing program as specified in the OP&amp;Ps Section 63.1 Shutdown System Availability [BP-OPP-00001, R019]. As such, this meets the requirements of the clause and is deemed in compliance</p>	
4.7.2	To achieve high signal sensitivity and avoid spurious SDS actuation, the SSCs employed in the design of the SDS shall be qualified for electromagnetic noise disturbances (conducted and radiated, continuous and transient) and mechanical vibrations from normally operating plant equipment. Qualification tests shall be specified and performed to provide assurance that electromagnetic and mechanical disturbances cannot render the SDS ineffective.	<p>Bruce B design documentation (e.g., Safety Report, Bruce Power DM's, etc.) does not explicitly state the SSCs employed are qualified for electromagnetic noise disturbances and mechanical vibrations (Gap 1).</p> <p>Qualification against electromagnetic susceptibility for the installed equipment cannot be confirmed. As such, the requirement for the clause is deemed not in compliance. Bruce Power is implementing compensatory measures to avoid spurious trips.</p> <p>For example, rooms designed as 'radio-free' zones. Roll-outs to all control maintenance personnel and MCR operations staff have been completed to enforce the expectations on radio use in or around the instrument rooms, the vertical reactivity deck, gantry crane movement activities or any</p>	Gap

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>maintenance that takes place on SDS equipment in the vault.</p> <p>It is common practice for Bruce Power to request EMI/RF qualification for all new I&amp;C components, which is typically documented in the Technical Specifications.</p>	
4.8	The maintenance of instrumentation associated with the measurement of neutron power should be carried out when the reactor is at a power level at which the instrumentation gives sensible indications.	Section 03.1 item (3) of the Operating Policies and Principles - Bruce B [BP-OPP-00001 Rev. 19] states: " Maintenance of shutdown system neutron power instrumentation shall be done at a sufficiently high power such that the effect of the maintenance is immediately apparent before the component or channel is returned to service, unless Senior Operations Authority approval is given, on a case by case basis, for an alternative reactor state."	C


 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

## B.2. CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants


In support of the review tasks listed in Section 5, a detailed assessment of REGDOC-2.5.2 has been performed in Table B2.

**Table B2: CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plant**


Article No.	Clause Requirement	Assessment	Compliance Category
4.1.1	<p>The radiation protection objective is to provide that during normal operation, or during anticipated operational occurrences, radiation exposures within the NPP or due to any planned release of radioactive material from the NPP are kept below prescribed limits and as low as reasonably achievable (ALARA).</p> <p>Provisions shall be made for the mitigation of the radiological consequences of any accidents considered in the design.</p>	<p>The change introduced in the second paragraph is editorial in nature and does not affect the requirement.</p> <p>The design provisions for the accident prevention include highly reliable regulating, shutdown, and heat transport systems. The regulating system controls reactor power under all normal modes of operation to prevent power increases from overheating the fuel. The shutdown system contributes to the control function by reliably terminating any anticipated transients for the same reason.</p> <p>Reliable fuel cooling systems circulate water over the fuel at sufficient flow and suitable conditions to remove the heat being generated over the complete range of expected power levels and during transient conditions. In particular, a number of backup cooling systems are provided to perform this function during upset conditions such as loss of power from the electrical grid.</p> <p>Fuel and fuel sheath design are of high quality to contain radioactive material so as to prevent leakage into the heat transport system under normal operation and during transients.</p> <p>The heat transport pressure boundary provides reliable fuel cooling, maintain coolant inventory, and must be leak tight to contain any radioactive material that might leak from the fuel</p>	C

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>into the heat transport system. The heat transport pressure boundary is robust and of very high quality to minimize the likelihood of loss of coolant from the system.</p> <p>The adequacy and effectiveness of engineering and administrative measures to prevent and mitigate accidents is assessed in Safety Factor 5.</p>	
4.1.2	<p>The technical safety objectives are to provide all reasonably practicable measures to prevent accidents in the NPP, and to mitigate the consequences of accidents if they do occur. This takes into account all possible accidents considered in the design, including those of very low probability.</p> <p>When these objectives are achieved, any radiological consequences will be below prescribed limits, and the likelihood of accidents with serious radiological consequences will be extremely low.</p>	<p>The text in this clause is the same as in RD-337.</p> <p>In order to achieve the safety objectives in the design of the plant, a comprehensive safety analysis is carried out to identify all sources of exposure and to evaluate radiation doses that could be received by the workers and the public, as well as potential effects on the environment. The safety analysis examines: (1) all planned normal operational modes of the plant; (2) plant performance in anticipated operational occurrences; (3) design basis accidents; and (4) event sequences that may lead to a severe accident. On the basis of this analysis, the robustness of the engineering design in withstanding postulated initiating events and accidents can be established, the effectiveness of the safety systems demonstrated, and requirements for emergency response can be established.</p> <p>The Safety Report for Bruce B consists of three main parts and presents the following information:</p> <p>Part 1: Plant and Site Description [Bruce B 2012 Safety Report, NK29-SR-01320-00001, Rev 005, November 27, 2012] provides a general description of plant and site, including environmental considerations.</p> <p>Part 2: Plant Components and Systems [Bruce B 2012 Safety Report NK29-SR-01320-00001, Rev 005, November 27,</p>	C

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>2012] provides a description of major station systems and components in sufficient detail to enable the reader to understand the functions and interactions and to follow the accident analyses in Part 3.</p> <p>Part 3: Accident Analysis [Bruce B 2011 Safety Report. NK29-SR-01320-00002, R005, October 11, 2011] presents the analysis of all design basis accidents, to demonstrate that all safety design objectives for the station are met.</p>	
4.1.3	<p>The environmental protection objective is to provide all reasonably practical mitigation measures to protect the environment during the operation of an NPP and to mitigate the consequences of an accident.</p> <p>The design shall include provisions to control, treat and monitor releases to the environment and shall minimize the generation of radioactive and hazardous wastes.</p>	<p>This is a new clause.</p> <p>Emissions of each radionuclide group associated with each pathway are managed to As Low As Reasonably Achievable (ALARA) levels. Action Levels are specified for each radionuclide group. If emissions of a radionuclide group exceed defined Action Levels, prompt action to return emissions to normal levels is taken. In addition, emissions for all radionuclide groups from all facilities at Bruce Power are routinely evaluated with respect to an overall emission administrative limit. This is to promptly identify abnormal emissions for more than one radionuclide group and/or from more than one facility at Bruce Power. A measure of the radioactive emissions performance compared to the action levels is presented in the Quarterly Operations Report for Bruce B.</p> <p>BP-PROC-00888 [ R001, November 2015] Conventional and Hazardous Waste Management Program describes how Bruce Power complies with applicable federal, provincial, and local regulations and corporate requirements, including waste minimization affecting the generation, handling, storage, and disposal of hazardous waste (section 1.0).</p>	C

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		The design provisions for environmental protection are discussed in detail later on under Clause 10. The radiological impact of the nuclear power plant on the environment is discussed in more detail in Safety Factor 14.	
4.2	<p>The NSCA and the technical safety objectives provide the basis for the following criteria and goals:</p> <ol style="list-style-type: none"> <li>1. dose acceptance criteria</li> <li>2. safety goals</li> </ol> <p>Safety analyses shall be performed to confirm that these criteria and goals are met, to demonstrate effectiveness of measures for preventing accidents, and mitigating radiological consequences of accidents if they do occur.</p>	<p>The text in this clause is the same as in RD-337.</p> <p>Section 1.5 of Part 3 of Bruce B Safety Report describes the analysis acceptance criteria, including regulatory criteria and derived acceptance criteria. Meeting the derived acceptance criteria ensures that the regulatory criteria are met. Dose acceptance criteria for DBAs and the plant safety goals for BDBAs are met. Bruce Power makes use of the concept of safety goals as a means of determining the adequacy of overall plant safety as determined through the use of Probabilistic Safety Assessments. The Safety Report presents an introduction (Part 1), a detailed description (Part 2) and the Safety Analysis (Part 3) for Bruce B. Part 1 provides an introduction to the Safety Report and a general description of plant and site, including environmental considerations. Part 2 provides a description of major station systems and components in sufficient detail to enable the reader to understand the functions and interactions and to follow the accident analyses in Part 3. Part 3 presents the analysis of all design basis accidents, to demonstrate that all safety design objectives for the station are met.</p>	C
4.2.1	<p>The acceptance criteria for normal operations are provided in section 6.4.</p> <p>The committed whole-body dose for average members of the critical groups who are most at</p>	<p>The changes in this clause are provided for clarification and guidance; therefore they have no impact on the requirements.</p> <p>A review of the same clause in RD-337 as documented in [NK21-CORR-00531-11005 / NK29-CORR-00531-11397]</p>	Gap



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>risk, at or beyond the site boundary, shall be calculated in the deterministic safety analysis for a period of 30 days after the analyzed event.</p> <p>This dose shall be less than or equal to the dose acceptance criteria of:</p> <ol style="list-style-type: none"> <li>0.5 millisievert (mSv) for any AOO or</li> <li>20 mSv for any DBA</li> </ol> <p>The values adopted for the dose acceptance criteria for AOOs and DBAs are consistent with accepted international practices, and take into account the recommendations of the IAEA and the International Commission on Radiological Protection.</p>	<p>indicated that the B design does not fully meet this requirement. The Bruce B safety analysis covers a wide range of accident scenarios, demonstrating that the levels of defence-in-depth have been met, and that all of the regulatory reference dose limits of the current licence are not exceeded. However, the AOOs have not been analyzed explicitly to demonstrate that the specific dose acceptance criteria are met (Gap). It should be noted that although AOOs have not been directly addressed in the analysis, they have been shown to meet the current single failure limit, as required.</p> <p>As documented in supporting documentation for NK21-CORR-00531-11567/NK29-CORR-00531-11950, analysis of AOOs will be addressed as part of the Safety Report Improvement activities, as identified in the Safety Report Improvement Plan for Bruce A and Bruce B. The formal Regulatory Communication Plan is provided in Attachment A of [NK21-CORR-00531-12334 / NK29-CORR-00531-12767]. The Safety Report Improvement project is scheduled to be complete by 2017 with the submission of the revised Safety Report which implements REGDOC-2.4.1.</p> <p>The acceptance criteria for the radiological consequences of postulated events are specified in section 1.5 of Part 3 of f Bruce B Safety Report [NK29-SR-01320-00002, R005]. The reference dose limit for all DBAs (20 mSv) is met since the limit quoted is 4 times that of the single failure limit used as the current Bruce B reference dose limit. The limits for AOOs have not been treated separately but have been shown to meet the current single failure limit as required.</p>	
4.2.2	Qualitative safety goals	In comparison to RD-337, there are no changes to the	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>A limit is placed on the societal risks posed by NPP operation. For this purpose, the following two qualitative safety goals have been established:</p> <p>Individual members of the public shall be provided a level of protection from the consequences of NPP operation, such that there is no significant additional risk to the life and health of individuals.</p> <p>Societal risks to life and health from NPP operation shall be comparable to or less than the risks of generating electricity by viable competing technologies, and shall not significantly add to other societal risks.</p> <p>Quantitative application of the safety goals</p> <p>For practical application, quantitative safety goals have been established, so as to achieve the intent of the qualitative safety goals. The three quantitative safety goals are:</p> <p>1. core damage frequency</p>	<p>requirements in this clause.</p> <p>Bruce Power makes use of the concept of safety goals as a means of determining the adequacy of overall plant safety as determined through the use of Probabilistic Safety Assessments. Bruce Power has been reporting the results of PSA for the Bruce A and B plants against the Bruce Power nuclear public safety goals for Severe Core Damage Frequency (SCDF) and Large Release.</p> <p>The Probabilistic Risk Assessment Procedure [DIV-ENG-00010, R000] establishes the process for the evaluation of the safe operation of the station utilizing Probabilistic Risk Assessment and comparing the results against established industry safety goals and licensing targets.</p> <p>Bruce Power specified that the SCDF limit is 1E-4 per reactor year compared to the RD-337/REGDOC-2.5.2 quantitative safety goal of 1E-5 per reactor year. Bruce units meet the 1E-4 SCDF limit but the values are higher than the quantitative goal of CNSC REGDOC-2.5.2 (1E-5).</p> <p>Bruce Power specified safety goals include Large and Severe Release Limits. The Limits are defined as fractions of core inventory rather than absolute Becquerel value as specified in this clause. The Bruce Power Large Release Frequency is defined as the frequency of events with releases from containment that are &gt;1% fraction of Cs-137 inventory. The Bruce Power Severe Release Frequency is defined as the frequency of events with releases from containment &gt; 10% fraction of Cs-137 inventory. Bruce Power estimated releases meet their limits and goals.</p> <p>The quantitative safety goals calculated in the Bruce B PRA are defined in accordance with the requirement of this clause.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2. small release frequency</p> <p>3. large release frequency</p> <p>A core damage accident results from a postulated initiating event (PIE) followed by the failure of one or more safety system(s) or safety support system(s). Core damage frequency is a measure of the plant's accident prevention capabilities.</p> <p>Small release frequency and large release frequency are measures of the plant's accident mitigation capabilities. They also represent measures of risk to society and to the environment due to the operation of an NPP.</p> <p>Core damage frequency</p> <p>The sum of frequencies of all event sequences that can lead to significant core degradation shall be less than 1E-5 per reactor year.</p> <p>Small release frequency</p> <p>The sum of frequencies of all event sequences</p>	<p>However, the limiting values of the safety goals adopted in the Bruce B PRA are one order of magnitude larger than the corresponding limits required in the clause, i.e., Bruce B PRA uses the safety goal limits defined in the Level 2 PRA Guide B-REP-03611-00010:</p> <p>" for the severe core damage frequency to be less than 1E-4 per reactor year;</p> <p>" for the small release frequency to be less than 1E-4 per reactor year;</p> <p>" for the large release frequency to be less than 1E-5 per reactor year.</p> <p>The following results of the Bruce B PRAs are summarized in the letter NK21-CORR-00531-11324/NK29-CORR-00531-11729 submitted to the CNSC on July 31, 2014:</p> <p>Severe Core Damage Frequency (SCDF) for At-Power Internal Events:</p> <p>5.18E-6 per reactor year</p> <p>(if Emergency Mitigating Equipment (EME) installed for Fukushima-related improvements are credited) or</p> <p>1.48E-5 per reactor year</p> <p>(without crediting the Fukushima-related EME, as obtained in the Level 1 At-Power Internal Events 2013 [Enclosure 2 to NK21-CORR-00531-10958/NK29-CORR-00531-11342, Submission of S-294 Probabilistic Risk Assessment Deliverables, Bruce Power letter, F. Saunders to R. Lojk, December 24, 2013])</p> <p>SCDF for Outage Internal Events:</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>that can lead to a release to the environment of more than 1E15 becquerels of iodine-131 shall be less than 1E-5 per reactor year. A greater release may require temporary evacuation of the local population.</p> <p>Large release frequency</p> <p>The sum of frequencies of all event sequences that can lead to a release to the environment of more than 1E14 becquerels of cesium-137 shall be less than 1E-6 per reactor year. A greater release may require long term relocation of the local population</p> <p>Guidance</p> <p>A comprehensive probabilistic safety assessment (PSA) considers the probability, progression and consequences of equipment failures or transient conditions, to derive numerical estimates for the safety of the plant. Core damage frequency is determined by a Level 1 PSA, which identifies and quantifies the sequence of events that may lead to significant core degradation. The small release frequency and large release frequency are determined by a Level 2 PSA, which starts from the results of a Level 1 PSA, analyzes the</p>	<p>8.30E-6 per reactor year</p> <p>SCDF for Internal Flood:</p> <p>4.60E-7 per reactor year (with the Fukushima-related EME credited)</p> <p>SCDF for Fire Hazard:</p> <p>4.06E-6 per reactor year (with the Fukushima-related EME credited)</p> <p>SCDF for Seismic Hazard:</p> <p>7.20E-7 per reactor year (crediting the Fukushima-related EME)</p> <p>SCDF for High Wind Hazard:</p> <p>6.16E-6 per reactor year (crediting the Fukushima-related EME)</p> <p>Aggregated SCDF by adding the above SCDFs:</p> <p>2.49E-5 per reactor year (with the Fukushima-related EME credited)</p> <p>Large Release Frequency (LRF) for At-Power Internal Events:</p> <p>6.93E-7 per reactor year</p> <p>(if Emergency Mitigating Equipment (EME) installed for Fukushima-related improvements are credited , as reported in the document "RE: Bruce A and Bruce B Level 2 At-Power PRA Results Including Emergency Mitigating Equipment" B1538/005/000001, November 20, 2014) or</p> <p>5.49E-6 per reactor year</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>containment behaviour, evaluates the radionuclides released from the failed fuel, and quantifies the releases to the environment. An exemption for performing a Level 2 PSA is granted if it is shown that core damage frequency in the Level 1 PSA is sufficiently low (i.e., less than the large release frequency limit).</p> <p>Calculations of the safety goals include all internal and external events as per REGDOC-2.4.2, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants. However, aggregation of internal event and other hazard risk metrics performed through simple addition to demonstrate that the risk metrics (core damage frequency, small release frequency and large release frequency) are not exceeded might not be appropriate. It is recognized that when the risk metrics</p> <p>for external events are conservatively estimated, their summation with the risk metrics for internal events can lead to misinterpretation. Should the aggregated total exceed the safety goals, conclusions should not be derived from the aggregated total until the scope of the conservative bias in the other hazards is investigated.</p> <p>Further details on PSAs are contained in section 9.5 of this document and CNSC REGDOC-2.4.2,</p>	<p>(without crediting the Fukushima-related EME, as obtained in the Level 2 At-Power Summary Report, B0900/RP/055 R01, December 2013 [NK21-CORR-00531-10958/NK29-CORR-00531-11342, Enclosure 4, Submission of S-294 Probabilistic Risk Assessment Deliverables, Bruce Power letter, F. Saunders to R. Lojk, December 24, 2013])</p> <p>LRF for Fire Hazard:</p> <p>8.74E-7 per reactor year (with the Fukushima-related EME credited)</p> <p>LRF for Seismic Hazard:</p> <p>7.20E-7 per reactor year (with the Fukushima-related EME credited)</p> <p>LRF for High Wind Hazard:</p> <p>6.16E-6 per reactor year (crediting the Fukushima-related EME)</p> <p>Aggregated LRF by adding the above LRFs:</p> <p>8.45E-6 per reactor year (with the Fukushima-related EME credited)</p> <p>Small Release Frequency (SRF) for At-Power Internal Events:</p> <p>7.14E-7 per reactor year</p> <p>(without crediting the Fukushima-related EME, as obtained in the RE: Bruce A and Bruce B Level 2 At-Power PRA Results Including Emergency Mitigating Equipment" B1538/005/000001, November 20, 2014)) or</p> <p>5.67E-6 per reactor year</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	Probabilistic Safety Assessment (PSA) for Nuclear Power Plants.	<p>(without crediting the Fukushima-related EME, as obtained in the Level 2 At-Power Summary Report, B0900/RP/055 R01, December 2013 [see NK21-CORR-00531-10958/NK29-CORR-00531-11342, Enclosure 4, Submission of S-294 Probabilistic Risk Assessment Deliverables, Bruce Power letter, F. Saunders to R. Lojk, December 24, 2013])</p> <p>If Fukushima-related EMEs are credited, all SCDFs for individual events meet both the Bruce Power guide's (B-REP-03611-00010 Rev 1) safety goal limit of 1E-4 per reactor year and CNSC's REGDOC 2.5.2 clause 4.2.2 safety goal limit of 1E-5 per reactor year.</p> <p>The SRF for at-power internal events meets both the Bruce Power guide's (B-REP-03611-00010 Rev 1) safety goal limit of 1E-4 per reactor year and CNSC's REGDOC 2.5.2 clause 4.2.2 safety goal limit of 1E-5 per reactor year.</p> <p>If Fukushima-related EMEs are credited, all LRFs but for one of the events meet both the Bruce Power guide's (B-REP-03611-00010 Rev 1) safety goal limit of 1E-5 per reactor year and CNSC's REGDOC 2.5.2 clause 4.2.2 safety goal limit of 1E-6 per reactor year. The PRA for high wind events results in an LRF of 6.16E-6, which is higher than the REGDOC's limit of 1E-6 per reactor year. Further details are provided in Safety Factor 6.</p> <p>Although the result of each individual PRA meets the safety goal limits set up for Bruce B PRAs (with the exception of high wind LRF result as noted above), their aggregates obtained by respective summation of SCDFs and LRFs do not meet the more stringent quantitative safety goal targets set up in the requirement clause. Therefore, a gap is assessed against this clause (Gap).</p>	




Article No.	Clause Requirement	Assessment	Compliance Category
4.2.3	<p>To demonstrate achievement of the safety objectives, a comprehensive hazard analysis, a deterministic safety analysis, and a probabilistic safety assessment shall be carried out. These analyses shall identify all sources of exposure, in order to evaluate potential radiation doses to workers at the plant and to the public, and to evaluate potential effects on the environment.</p> <p>The safety analyses shall examine plant performance for:</p> <ol style="list-style-type: none"> <li>1. normal operatio</li> <li>2. AOOs</li> <li>3. DBAs</li> <li>4. BDBAs, including DECAs (DECAs could include severe accident conditions)</li> </ol> <p>Based on these analyses, the capability of the design to withstand PIEs and accidents shall be confirmed, the effectiveness of the items important to safety demonstrated, and requirements for emergency response established. The results of the safety analyses shall be fed back into the design.</p> <p>The safety analyses are discussed in further detail</p>	<p>The change in item 4 is provided for clarification and to align with the newly defined plant state DEC.</p> <p>The requirement to undertake accident analysis for the equivalent of AOOs, DBAs and BDBAs has always been part of the licensing requirements for Bruce B, based on the range of analyses performed. It is recognized that when Bruce B was originally licensed, there were no requirements to account for severe accidents as now defined in this clause.</p> <p>The deterministic safety analysis for Bruce B documented in Part 3 of the Safety Report [NK29-SR-01320-00002, R005] does not distinguish between these four classes of events. The DECAs introduced in CNSC REGDOC-2.5.2 are not considered in the design basis; however, the design basis includes some event sequences that would be categorized as BDBAs and meet the definition of DECAs. The focus of the Safety Report is primarily on design basis events, which include design basis accidents and AOOs. The specific event classification scheme has not been followed for deterministic safety analysis and hence identified as a gap (Gap 1).</p> <p>As reflected in the compliance verification criteria of the Licence Conditions Handbook [NK21-CORR-00531-12135 / NK29-CORR-00531-12545 / LCH-BNGS-R000], section 4.1, a three-year Safety Report Improvement (SRI) Project is undertaken to upgrade the Bruce A and B Safety Reports to align with RD-310 (and now CNSC REGDOC-2.4.1). New analyses for Common Mode Failures (CMF) will be introduced as an Appendix into the Safety Reports for Bruce A and Bruce B and are the highest priority. This component of the SRI Project is to determine the approach for deterministic analyses in support of seismic events, fire and</p>	Gap

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	in section 9.0.	<p>floods, drawing from post-Fukushima assessments and Probabilistic Risk/Safety Assessments performed in compliance with CNSC Regulatory Standard S-294. The current version of the Industry guidance document COG-09-9030, Principles and Guidelines for Deterministic Safety Analysis [COG-09-9030, Rev. 3, November 2014] previously discussed with the CNSC, is being utilized in the project [NK21-CORR-00531-12334 / NK29-CORR-00531-12767].</p> <p>The project is scheduled to be completed in time for the next Safety Report update by December 31, 2017. The analysis schedule of the SRI Project will be guided by gap assessments undertaken by Bruce Power along with business drivers and operational needs. Bruce Power will meet with CNSC staff annually to review and communicate the SRI Project Status and progress. Since full compliance with REGDOC-2.4.1 may not be feasible or may not provide additional safety benefit beyond the current safety case, a graded approach has been adopted to evaluate the significance of the gaps against REGDOC-2.4.1. Following the project improvements and enhancements, Bruce Power will programmatically ensure that new safety analysis and assessments are consistent with REGDOC-2.4.1 through the implementation of the ongoing Safety Analysis Improvement Program (SAIP) responsible for future updates to the Safety Reports.</p> <p>Although some common-cause internally and externally initiated events form part of the design basis for the plant, these have not been explicitly addressed in the deterministic safety analysis as required in this clause. Subsequently, this is assessed as a gap. (Gap 2)</p> <p>As documented in the Regulatory Communication Plan for</p>	

 <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		the Safety Report Improvement Project [NK21-CORR-00531-12334 / NK29-CORR-00531-12767 Action Item 090739: Safety Report Improvement Project - Regulatory Communication Plan, November 24, 2015] , Bruce Power is implementing a Safety Report Improvement Program which started in 2014 including annual status and progress updates to the CNSC staff. The Regulatory Communication Plan formally provides the timeframe and associated tasks for execution of the SRI Plan. This program is expected to address both gaps.	
4.2.4	<p>The design shall include provisions to limit radiation exposure in normal operation and AOOs to ALARA levels, and to minimize the likelihood of an accident that could lead to the loss of normal control of the source of radiation. However, given that there is a remaining probability that an accident may occur, measures shall be taken to mitigate the radiological consequences of accidents.</p> <p>These measures shall include:</p> <ol style="list-style-type: none"> <li>1. consideration of inherent safety features</li> <li>2. incorporation of engineered design features</li> <li>3. onsite accident management procedures</li> </ol>	<p>There is a new requirement in the last paragraph for the design to facilitate the transfer of control between procedures for operational states, accident conditions, severe accident management and onsite emergency response.</p> <p>The Bruce B design incorporates engineered safety features and specific accident management procedures for AOOs, DBAs and some BDBAs as described in the Abnormal Incidents Manual [NK29-AIM-03600.1, Rev.056].</p> <p>As a result of Fukushima event lessons learned Bruce Power is implementing Expanded Severe Accident Management Guidelines for dealing with severe accidents. In 2015, Bruce A and B Severe Accident Guides and Severe Challenge Guides were updated to consider the possibility of severe accidents occurring concurrently on more than one unit as challenges, mitigating strategies, and priorities may be impacted for stations with multi-unit design [Attachment B, Section 2.8, of [NK21-CORR-00531-12209 / NK29-CORR-00531-12635].</p> <p>Bruce Power assessed the reactor's defence-in-depth for a severe accident and identified areas for potential</p>	IC

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>established by the operating organization</p> <p>4. establishment of offsite intervention measures by responsible authorities</p> <p>The design shall apply the principle that plant states that could result in high radiation doses or radioactive releases have a very low frequency of occurrence, and that plant states with significant frequency of occurrence have only minimal – if any – potential radiological consequences.</p> <p>The design shall facilitate the clear transfer of control between procedures for operational states, accident conditions, severe accident management and onsite emergency response.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>Canadian Nuclear Safety Commission (CNSC), G-129, rev 1, Keeping Radiation Exposures and Doses “As Low as Reasonably Achievable (ALARA),” Ottawa, Canada, 2004.</li> <li>CNSC, REGDOC-2.3.2, Accident</li> </ul>	<p>enhancements. In cases, the evaluation indicates that there is a gap, mitigating features are provided; if enhancements of the systems, structures and components are not an option. For example, where the existing means to protect containment integrity and prevent uncontrolled releases of radioactive products in beyond-design-basis accidents including severe accidents are found inadequate, a plan and schedule for design enhancements to control long-term radiological releases and, to the extent practicable, unfiltered releases are developed. Bruce Power considered the installation of containment bypass tees and containment boundary valves into the existing EFADS piping where it exits the Vacuum Building and Pressure Relief Valve (PRV) manifold at Bruce A and B. Further details are provided in compliance notes for clause 7.3.4.</p> <p>Bruce Power performed assessments, in conjunction with COG, of equipment and instrument survivability and habitability of control facilities under conditions arising from beyond-design-basis accidents and severe accidents. Following the issuance of the generic methodologies for instrument and equipment survivability (FAI 1.8.1) and control facility habitability (1.9.1) in [Letter, F. Saunders to R. Lojk, "Bruce Power Progress Report No. 4 on CNSC Action Plan - Fukushima Action Items", January 30, 2014, NK21-CORR-00531-10963/ NK29-CORR-00531-1 1349/ NK37-CORR-00531-02162] Bruce Power has completed the Bruce specific analysis, provided in Enclosures 2 and 3 respectively. The approach used was to focus on the essential Severe Accident Management Guidance (SAMG) parameters and strategies and to build upon existing Environmental Qualification work and Level 2 Probabilistic Risk Assessments, SAMG programs and BDBA provisions</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Management: Severe Accident Management Programs for Nuclear Reactors, Ottawa, Canada, 2013.</p> <ul style="list-style-type: none"> <li>International Atomic Energy Association (IAEA), Safety Guide NS-G-2.15, Severe Accident Management Programmes for Nuclear Power Plants, Vienna, 2009.</li> </ul>	<p>including the use of Emergency Mitigation Equipment (EME). The instrument and equipment survivability report include various recommendations to enhance Emergency Mitigating Equipment (EME) response and SAMG at Bruce A and B. These items have been dispositioned, as described in Attachment B, with some follow-up actions to update the SAMGs and assess options to environmentally qualify the moderator level transmitters. The results of the habitability report indicate that Bruce Powers installed and planned upgrades are sufficient to terminate event progressing at, or before, the early in vessel retention stage, thereby supporting station habitability and providing reasonable confidence that essential operator actions can be completed in a timely manner. No further upgrades to address radiological habitability are warranted, therefore, Bruce Power requested closure of FAI 1.9.1 in Bruce Power Progress Report No. 6 on CNSC Action Plan - Fukushima Action Items [NK29-CORR-00531-12195].</p> <p>An off-site emergency plan that is integrated with appropriate off-site authorities [Bruce Power Nuclear Emergency Response Plan, BP-PLAN-00001, R005, December 02, 2014] is in place. The Bruce B design supports the fundamental principle that plant states that could result in high radiation doses or radioactive releases are of very low probability of occurrence, and plant states with significant probability of occurrence have only minor or no potential radiological consequences. Bruce Power has formalized various external support agreements including a Mutual Aid agreement with all Canadian Nuclear Power operators, Dosimetry Services Lab Support Agreement and Transportation Emergency Response support with Ontario Power Generation (OPG) and Atomic Energy of Canada</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		Limited (AECL). Funding agreements are in place with the Municipality of Kincardine to support the Provincial Nuclear Emergency Response Plan. Contracts are also being put in place for the supply of emergency consumables such as clothing, fuel and food on short notice.	
4.3.1	<p>The concept of defence in depth shall be applied to all organizational, behavioural, and design-related safety and security activities to ensure they are subject to overlapping provisions. The levels of defence in depth shall be independent to the extent practicable.</p> <p>If a failure were to occur, the defence-in-depth approach allows the failure to be detected, and to be compensated for or corrected.</p> <p>This concept shall be applied throughout the design process and operation of the plant to provide</p> <p>a series of levels of defence aimed at preventing accidents, and ensuring appropriate protection in the event that prevention fails.</p> <p>The design shall provide all of the following five levels of defence during normal operation; however, some relaxations may be specified for certain shutdown states. These levels are introduced in general terms below, and are</p>	<p>A new requirement for independence of the levels of defence to the extent practicable is introduced in this clause.</p> <p>The concept of defence in depth has been applied to the design of all CANDU reactors. The various levels of defence-in-depth are independent of each other to the greatest extent practicable. For example, level 1 defence-in-depth systems, i.e., process systems, are designed so that any failure in the system is not propagated to the control systems that control these processes. Similarly a failure in a control system does not propagate to the next level of defence-in-depth, i.e., the safety systems. This is accomplished through adequate separation of the control systems from the safety systems; internationally this is achieved by ensuring adequate buffering of any components shared between the control and safety systems so that the failure cannot be propagated, in Canada, it has been done to date through complete separation of the control and safety systems. As part of this defence-in-depth, pressure retaining components in any safety system are required to meet the highest design standards. The fourth level of defence-in-depth makes use of many systems that are not normally credited in Canadian safety analysis. They are used to mitigate the consequences of a BDDBA or a Severe Accident. Such accidents have a very low frequency and usually occur because safety systems have not been able to perform their function, either through multiple component failures within those systems or through</p>	C



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>discussed in greater detail in section 6.1.</p> <p>Level One</p> <p>The aim of the first level of defence is to prevent deviations from normal operation, and to prevent failures of structures, systems and components (SSCs) important to safety.</p> <p>Level Two</p> <p>The aim of the second level of defence is to detect and intercept deviations from normal operation, in order to prevent AOOs from escalating to accident conditions and to return the plant to a state of normal operation.</p> <p>Level Three</p> <p>The aim of the third level of defence is to minimize the consequences of accidents by providing inherent safety features, fail-safe design, additional equipment and mitigating procedures.</p>	<p>loss of common services. They are generally backup process systems and as such would have been designed such that their failure would in no way affect the control or safety systems.</p> <p>The application of defence in depth is described in more detail in later sections.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Level Four</p> <p>The aim of the fourth level of defence is to ensure that radioactive releases caused by severe accidents are kept as low as practicable.</p> <p>Level Five</p> <p>The aim of the fifth level of defence is to mitigate the radiological consequences of potential releases of radioactive materials that may result from accident conditions.</p> <p>Section 6.1 discusses the application of levels of defence in further detail.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>IAEA, INSAG-10, Defence in Depth in Nuclear Safety, Vienna, 2010.</li> </ul>		
4.3.2	An important aspect of implementing defence in depth in the NPP design shall be the provision of	The change (i.e., second sentence) is provided for clarification and does not impact the requirement.	C

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	a series of physical barriers to confine radioactive material at specified locations. Physical barriers are discussed in further detail in section 6.1.1.	<p>As described in the previous sections and Safety Report, the general safety objectives and principles that are fundamental to the Canadian safety philosophy and regulatory process are being followed by all nuclear power stations in Canada. Thus, Bruce B meets the general principles as formulated in this clause.</p> <p>Details of physical barriers incorporated in the Bruce B design are provided in the corresponding compliance sections of this assessment.</p>	
4.3.3	<p>Operational limits and conditions (OLCs) are the set of limits and conditions that can be monitored by or on behalf of the operator, and that can be controlled by the operator.</p> <p>The OLCs shall be established to ensure that plants operate in accordance with design assumptions and intent (parameters and components), and include the limits within which the facility has been shown to be safe. The OLCs shall be documented in a manner that is readily accessible for control room personnel, with the roles and responsibilities clearly identified. Some OLCs may include combinations of automatic functions and actions by personnel.</p> <p>OLCs shall include:</p>	<p>Compared to RD-337, this section is substantially revised to include clarifications and new requirements, i.e., item 1, 2, 4, 5, 6 and 7.</p> <p>Bruce Power developed a program to create Operational Safety Requirements (OSRs) for both the Bruce A and B plants. These operational requirements are essentially the OLCs as defined in the clause.</p> <p>The Bruce A and Bruce B LCH [NK21-CORR-00531-12135 / NK29-CORR-00531-12545 / LCH-BNGS-R000] specified under Licence Condition 3.1 Operations Program that the operations program establishes safe operating practices within the nuclear facility, under all operating conditions and provides the ability to ensure the facility is operated in accordance with the applicable regulatory requirements and operating polies and principles are implemented. ' The Operating Policies and Principles (OP&amp;P) [BP-OPP-00001, R019] outline the operating boundaries for safe operation, specify the authorities of the station staff and identify and differentiate between actions where discretion may be applied and where jurisdictional authorization is required. Bruce Power is implementing a Safe Operating Envelope</p>	AD


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>1. safety limits</p> <p>2. limiting safety system settings</p> <p>3. OLCs for normal operation and AOOs, including shutdown states</p> <p>4. control system constraints and procedural constraints on process variables and other important parameters</p> <p>5. requirements for surveillance, maintenance, testing and inspection of the plant to ensure that SSCs function as intended in the design and comply with the requirement for optimization by keeping radiation exposures ALARA, as per the Radiation Protection Regulations</p> <p>6. specified operating configurations, including operational restrictions in the event of the unavailability of SSCs important to safety</p> <p>7. action statements, including completion times for actions in response to deviations from the operational limits and conditions</p>	<p>(SOE) program which will provide the comprehensive identification of all operating limits and conditions in compliance with the requirements of CSA N290.15. The project portion of the SOE baseline implementation is considered complete; therefore any outstanding issues will be transferred to the maintenance phase of SOE sustainability which is currently under development.</p> <p>The safe operating limits are derived from the safety analysis limits. The SOE parameters are currently identified in various station documents, including Operational Safety Requirements (OSR), Instrument Uncertainty Calculations (IUCs), the Impairments Manual and surveillance documentation (licence condition 3.1 of Bruce A and B Licence Conditions Handbook).</p> <p>Bruce Power's safe operating limits, conditions and surveillance requirements as well as their bases are documented in station and system specific operational safety requirements (OSRs) documents along with any associated Instrument Uncertainty Calculations (Ucs). The limits and conditions defined in the OSRs, including any requirements for corrective or mitigating actions and action times, are specified in the applicable operations and maintenance tests, procedures and processes to ensure compliance with the SOE. Bruce Power is updating several of their program documents and completes the associated training requirements before they are fully compliant with N290.15. The completion date for these administrative updates was extended to February 2016 [NK21-CORR-00531-12546 / NK29-CORR-00531-12972].</p> <p>The current practice is to define three impairment levels as described in Impairments of Special Safety Systems and</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The basis on which the OLCs are derived shall be readily available in order to facilitate the ability of plant personnel to interpret, observe and apply the OLCs.</p> <p>Guidance</p> <p>The approaches and terminologies used for OLCs may vary as a result of the practices and regulatory systems that have been established in the country of origin for the plant's design.</p> <p>Regardless of the approaches and terminologies used, the design authority should provide clear definitions of the OLC terminologies used. The design should also include clear objectives and goals for the OLCs.</p> <p>The information related to OLCs should list the relevant standards (national or international) used, and document how the requirements from these standards have been met.</p> <p>OLCs should be defined for a suitable set of bounding plant operating configurations, and be</p>	<p>Other Safety Related Systems [NK29-OM-03500.1, Rev. 013]. The determination of the level of impairment is based upon the limits from the OSRs and the range of instrumentation uncertainty defined in the IUCs and the actions to be taken are dependent on the level of the impairment. This practice is somewhat different than that used in other countries where only the Limiting Condition of Operation is defined in the OLCs. The level of component redundancy in Canada in some cases is greater.</p> <p>Bruce Power has decided that the actions for the defined impairment levels will remain in the Impairments Manual (IM) rather than in the OSR documents. Bruce Power's decision is based on the fact that all of the station operating personnel is familiar and has received training in the use of IM, which reduces the chance for errors. The actual OSR document is being used more as a reference document that establishes technical basis for operating limits and conditions than an actual operating document. The OSRs contain the safety limits (based on the safety analysis), the operability conditions, testing and surveillance requirements.</p> <p>The IUCs are issued for each system containing instrumented loops. They contain the following information, used in the implementation of the OSR/IUCs:</p> <ul style="list-style-type: none"> <li>o The uncertainty associated with the surveillance instrumentation for instrument loops used by operator for direct surveillance and action (e.g., panel checks),</li> <li>o The uncertainty associated with the instruments specifically used for an automatic actuation in an instrument loop</li> </ul> <p>As discussed above the various operating limits and</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>based on the final design of the plant.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>o CSA Group, N290.15, Requirements for the safe operating envelope of nuclear power plants, Toronto, Canada.</li> <li>o IAEA Safety Guide NS-G-2.2, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, Vienna, 2000.</li> </ul>	<p>conditions as well as surveillance and testing requirements are incorporated into either the OSRs or the IUCs. The actions to be taken are documented in the Impairments Manual.</p>	
4.3.4	<p>Safety measures, nuclear security measures and arrangements for the system of accounting for, and control of, nuclear material for an NPP shall be designed and implemented in an integrated manner so that they do not compromise one another.</p>	<p>A new section is introduced.</p> <p>Assessment of nuclear security, safeguards and cyber security is outside the scope of this review. Due to the sensitivity of this topic, the design provisions for security and safeguards have not been assessed.</p>	RNA
5.	<p>The applicant or licensee shall be ultimately responsible for the design of the NPP and shall establish a management system for ensuring the continuing safety of the plant design throughout the lifetime of the NPP.</p>	<p>A new (first) paragraph is added to state the requirement for a management system for ensuring the continuing safety of the plant design throughout the lifetime of the plant. The changes are mostly editorial in nature and do not change the intent of the requirement.</p> <p>The original design of the plant met the original AECL Quality Assurance programs. Since Bruce Power is now responsible</p>	C




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The NPP design shall:</p> <ol style="list-style-type: none"> <li>1. meet Canadian regulatory requirements</li> <li>2. meet the design specifications</li> <li>3. be confirmed by safety assessment</li> <li>4. take into account current safety practices</li> <li>5. fulfill the requirements of an effective management system</li> <li>6. incorporate only those design changes that have been justified by technical and safety assessments</li> </ol> <p>The design process shall be carried out by technically qualified and appropriately trained staff at all levels, and shall include:</p> <ol style="list-style-type: none"> <li>1. a clear division of responsibilities with corresponding lines of authority and communication</li> </ol>	<p>for ongoing design modifications and upgrades, any such work carried out by Bruce Power staff or contractors must meet the quality assurance requirements of Bruce Power. Bruce Power does not have a single Quality Assurance Program document. Rather the quality approach is built into the PROG and PROC documents, as appropriate. The plant continues to meet current Canadian requirements or exceptions agreed to by the CNSC.</p> <p>The safety analyses have been updated many times since first criticality and take into account the results of the extensive safety experiments conducted both in Canada and internationally.</p> <p>Computer codes have been upgraded as new techniques and new technologies have become available. Bruce Power has established the basis for safe operation (the Safety Basis) of Bruce A and Bruce B covering a 5-year proposed licence period and beyond in the Safety Basis Report (SBR). The SBR takes into account information already submitted to the CNSC in support of licence renewal in 2014, plus the outcome of a recently completed interim PSR. The key elements of the Safety Basis are as follows.</p> <p>" Demonstration that the design basis is understood and controlled, and that the current condition of systems is understood.</p> <p>" Demonstration that important age-related degradation mechanisms are understood and that fitness for service of important systems is assured through proactive programs to manage the effects of ageing.</p> <p>" Demonstration that nuclear safety assessment takes into account the current and expected future condition of</p>	

 <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2. clear interfaces between the groups engaged in different parts of the design, and between designers, utilities, suppliers, builders and contractors, as appropriate</p> <p>3. design control measures (such as processes, procedures, and practices) as part of an established management system</p> <p>4. a management system that recognizes the importance of a healthy safety culture</p>	<p>systems and that safety criteria are and will continue to be met with confidence.</p> <p>" An extensive set of projects comprising an overall station improvement plan, with a major focus on process and physical improvements to incorporate lessons learned from Fukushima.</p> <p>" A set of opportunities for improvement arising from the PSR, which will be assessed using a risk-informed decision making process. Improvements selected for implementation will be merged with the station improvement plan.</p> <p>As part of its safety analysis program, Bruce Power is implementing a Safety Report Improvement project to align with REGDOC 2.4.1 Deterministic Safety Analysis. Regulatory deliverables of this project are listed in Table A-1 of Attachment A of the November 2015 letter [NK29-CORR-00531-12767]. The Safety Report Improvement project has a target completion date of 2017.</p> <p>Bruce Power is transitioning to REGDOC 2.4.2 for PSA over the current licence period and has a plan in place [NK21-CORR-00531-11715 / NK29-CORR-00531-12105] to meet the full compliance with it by the June 30, 2019, target date. In view of the importance of CNSC REGDOC-2.4.2 as the primary regulatory document for PSA, a clause-by-clause review was conducted against this standard and the results are included in Appendix B of Safety Factor Report 6.</p> <p>Any design changes follow the requirements of the Plant Design Basis Management Program BP-PROG-10.01, R009 (December 4, 2014), which identifies processes to ensure</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>that the design changes have been appropriately considered.</p> <p>As stated in the compliance verification criteria for licence condition 1.1 Management System Requirements, the management and operation of Bruce Power are defined by the programs and their implementing documents, as described by Bruce Power's Management System Manual BP-MSM-1. The Bruce Power Management System Manual [BP-MSM-1, R012, June 23, 2014] clearly identifies the requisite management responsibilities at the senior level. The requirement to define the interfaces and the roles among the various groups is identified in BP-PROG-10.01, R009 Plant Design Basis Management and in the BP-PROC-00335 Design Management [R007, July 30, 2015]. As described in section 2.1 of Bruce Power MSM, by design the Bruce Power Management System is based on the establishment of a safety culture that assures reactor, environmental, industrial and radiological safety, during normal operations as well as during extreme events. It also provides the necessary guidance for making risk-based decisions that satisfy the desired balance between safety, commercial and corporate reputation performance. In developing this management system, Bruce Power has taken into consideration the applicable statutory, regulatory and licensing requirements, and has taken advantage of relevant industry standards and best practices. Bruce Power Policy Statements defined in Appendix A of MSM establish philosophies, purpose, and shape the broad requirements of the associated programs. As described in section 3.3 of MSM, the appropriate management principles and policy statements together with business, legal, statutory and regulatory requirements are expected to guide the content of all Bruce Power documents.</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>To ensure that Bruce Power fosters and maintains a positive safety culture, periodic assessment activities are conducted. Nuclear Safety Culture Monitoring procedure [BP-PROC-00892, R001, September 29, 2014] documents the approach for monitoring nuclear safety culture using the framework described in INPO 12-012, Traits of a Healthy Nuclear Safety Culture and based on the approach described in NEI 09-07, Rev. 1, Fostering a Strong Nuclear Safety Culture (section 4.1 of BP-PROC-00892). The key process elements include the process inputs, the nuclear safety culture review meetings and the actions arising from the insights derived as a result of the process. The industry standards considered in this procedure are specified in section 5.6 of BP-PROC-00892. The organization, management system and safety culture elements are further assessed in SF10.</p> <p>It is noted that CSA N286-2005, including Update No. 2 (December 2010) has an effective date of June 1, 2015 whereas N286-12 has an effective date of December 31, 2015 as per licence condition 1.1 Management System (PROL 18.00/2020). Bruce Power will transition to the 2012 version of the standard during this licensing period. As part of Bruce Power's transition plan from CSA N286-05 to CSA N286-12 a gap analysis has been performed and submitted to CNSC [Letter F. Saunders to K. Lafreniere, Action Item 1307-4697: CSA N286-12 - Management Systems Requirements for Nuclear Facilities, NK21-CORR-00531-12570 / NK29-CORR-00531-12996, January 29, 2016]. As stated in Attachment A, 28 program FASAs were completed covering all the Functional Areas and the results used as input for developing the transition plan to CSA N286-12. No CSA N286-05 requirement gaps have been identified and CSA N286-12 citation gaps are currently being addressed by</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>Document Change Requests per the regular document review cycle.</p> <p>As stated in the LCH, Bruce Power shall transition to the 2012 version of CSA standard N286 during this licensing period. Bruce Power submitted the results of CSA N286-12 gap analysis and the transition plan to the CNSC and requested closure of Action Item 1307-4697 as per NK21-CORR-00531-12570 / NK29-CORR-00531-12996 [Letter F. Saunders to K. Larferniere, Action Item 1307-4697: CSA N286-12 - Management Systems Requirements for Nuclear Facilities, January 29, 2016]. During the transition to the 2012 version, CNSC staff will perform compliance activities in accordance with the 2005 version, and when applicable, the 2012 version of the N286.</p>	
5.1	<p>During the design phase, formal design authority typically rests with the organization that has overall responsibility for the design. Prior to plant start-up, this authority shall be transferred to the operating organization.</p> <p>The design authority may assign responsibility for the design of specific parts of the plant to other organizations, known as responsible designers. The tasks and functions of the design authority and any responsible designer shall be established in formal documentation; however, the overall responsibility remains with the design authority.</p> <p>The applicant or licensee shall confirm that the</p>	<p>The changes introduced in this clause are editorial in nature and do not impact the requirements. A reference to Nuclear Security Regulations is added, which is legally binding requirement. Due to sensitivity of security information, compliance with Nuclear Security Regulations is addressed elsewhere.</p> <p>Plant Design Basis Management Program [BP-PROG-10.01, R009] ensures that the plant design meets safety, reliability, and regulatory requirements including pressure boundary quality assurance requirements described in BP-PROG-00.04, [R022, May 27, 2015] Pressure Boundary Quality Assurance Program. Additionally, this program sets out requirements for engineering analysis and documentation such that the adequacy of the design can be demonstrated. The role of Design Authority is described in Section 4.3 of BP-PROG-10.01. The Design Authority Procedure, as</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>design authority has achieved the following objectives for the design:</p> <ol style="list-style-type: none"> <li>1. established a knowledge base of all relevant aspects of the plant design and kept it up-to-date, while taking experience and research findings into account</li> <li>2. ensured the availability of the design information that is needed for safe plant operation and maintenance</li> <li>3. established the requisite security provisions in accordance with the Nuclear Security Regulations and associated regulatory documents</li> <li>4. maintained design configuration control</li> <li>5. reviewed, verified, approved and documented design changes</li> <li>6. established and controlled the necessary interfaces with responsible designers or other suppliers engaged in design work</li> </ol>	<p>documented in DIV-ENG-00009, R005 outlines the processes by which the Chief Engineer and Senior Vice President, Engineering executes the role of Design Authority. The Design Authority Procedure is owned by the Chief Engineer and Senior Vice President, Engineering. The Chief Engineer and SVP Engineering as the Design Authority for the site ensures a strong nuclear safety culture consistent with Guideline WANO GL 2006 02 "Principles for a Strong Nuclear Safety Culture".</p> <p>As owner of BP-PROG-10.01, Plant Design Basis Management (section 7.3) the Divisional Manager Engineering Support ensures a strong nuclear safety culture consistent with Guideline WANO GL 2006 02 "Principles for a Strong Nuclear Safety Culture".</p> <p>" Provides a safe and reliable design for the nuclear facility.</p> <p>" Ensures engineering activities are performed in accordance with BP-PROG-00.04, Pressure Boundary Quality Assurance Program and applicable codes, standards and regulatory requirements.</p> <p>" Ensures all design activities are carried out in a manner that produces high quality design outputs in accordance with applicable codes, standards, and regulatory requirements.</p> <p>" Ensures that design configuration control is maintained.</p> <p>" Maintains the design expertise required for the safe design and operation of the facility.</p> <p>" Ensures that the risk is minimized by protecting the</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>7. ensured that the necessary engineering and scientific skills and knowledge have been maintained</p> <p>8. ensured that, with respect to individual design changes or multiple changes that may have significant interdependencies, the associated impact on safety has been properly assessed and understood</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>CSA Group, N286, Management system requirements for nuclear power plants, Toronto, Canada.</li> <li>IAEA, Safety Standards Series GS-G-3.5, The Management System for Nuclear Installations Safety Guide, Vienna, 2009.</li> <li>IAEA, INSAG-19, Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life, Vienna, 2003.</li> </ul>	<p>design basis intent for the station (i.e., station's physical condition and documents are consistent with the as-designed intent) for all permanent and temporary changes</p> <p>The Design Management Procedure, as documented in BP-PROC- 00335 [R007, July 30, 2015] specifies the design activities and outputs that define and manage the Plant Design Basis such that the nuclear operating stations can operate safely and reliably for the duration of their design life. Design Management relies upon the implementing procedures of BP-PROC-00363 [R003, January 24, 2013], Nuclear Safety Assessment to ensure nuclear safety requirements are incorporated into the design. This procedure interfaces with the implementing procedures of BP-PROG-10.02 [R010, November 12, 2014], Engineering Change Control, to ensure the correct tools are used during design changes and modifications. This procedure interfaces with the implementing procedures of BP-PROG-10.03 [R006, February 05, 2015], Configuration Management, to ensure margins are managed. The Design Management procedure is owned by the Department Manager, Plant Design Engineering.</p> <p>The Nuclear Safety Assessment procedure, as documented in section 1.0 of BP-PROC-00363 [R003, January 24, 2013] defines the elements, functional requirements, implementing procedures and key responsibilities associated with the Nuclear Safety Assessment (NSA) process. The objective of NSA is to ensure that all necessary nuclear safety requirements are defined for the actual or proposed design of the plant throughout the design modification process or in addressing emergent issues (e.g., plant ageing) that may affect the Design Basis or the Safety Report Basis. This</p>	




Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design


File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>procedure applies to all staff involved in NSA work undertaken by the Reactor Safety Support Department (RSSD), Nuclear Safety Analysis and Support Department (NSASD), and contractors that work as augmented staff within RSSD and NSASD. All such staff shall ensure the quality of their analysis work is acceptable, in compliance with this procedure and with associated program documents. This procedure interfaces with the implementing procedures of BP-PROG-10.02 [R010, November 12, 2014], Engineering Change Control, to ensure design changes and modifications arising from Safety Analyses are controlled. This procedure interfaces with the implementing procedures of BP- PROG-10.03 [R006, February 05, 2015], Configuration Management, to ensure margins are managed. The Nuclear Safety Assessment procedure is owned by the Manager, Nuclear Safety Analysis and Support Department.</p> <p>Bruce Power staff members are kept up-to-date on experimental programs relevant to safety both in Canada and abroad, through Bruce Power's participation in CANDU Owner's Group research activities.</p> <p>The requirements for design verification and technical reviews are specified in section 4.5 of the Design Management Procedure [BP-PROC-00335, R007] as follows: Design verification ensures, through the process of reviewing, confirming, or substantiating design by one or more methods, that design meets specified design inputs, is technically adequate, and fulfils established design process requirements. Verification activities, including independence, qualification of staff, documentation of results, correction of deficiencies and specialized Technical Reviews are covered in DPT-PDE-00007 [R009, November 01, 2013], Design</p>	


 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>Verification. The Design Authority is responsible for undertaking the task of ensuring that all such interactions have been accounted for. The Nuclear Oversight Group, through their oversight role should ensure that the process is being followed.</p> <p>In some cases, Audits may be required to ensure the quality of design products and activities meet their requirements. Audits are executed under BP-PROG-15.01 [R004, December 18, 2013] Nuclear Oversight Management.</p>	
5.2	<p>Appropriate design management shall achieve the following objectives:</p> <ol style="list-style-type: none"> <li>1. SSCs important to safety meet their respective design requirements.</li> <li>2. Due account is taken of the human capabilities and limitations of personnel.</li> <li>3. Safety design information - necessary for safe operation and maintenance of the plant and for any subsequent plant modifications - is preserved.</li> <li>4. OLCs are provided for incorporation into the plant administrative and operational procedures.</li> <li>5. The plant design facilitates maintenance and</li> </ol>	<p>In comparison to RD-337, the text in this clause is modified to include new requirements related to ageing management (item 5) hazards analysis (item 6), hazardous wastes (item 8), manufacturing (item 9) and cyber security programs (item 10).</p> <p>A review of the design documentation indicated that the Bruce B design does not fully meet this requirement. The Plant Design Basis Management [BP-PROG-10.01, R009] and the Design Management Program, [BP-PROC-00335, R007] do not explicitly refer to facilitation of maintenance as a requirement of any design modification. Nevertheless, maintenance is recognized as an important aspect of any design modification. The procedures and requirements in these documents take maintenance into account when a design modification is made. It is noted that the original plant design and layout specifically took into consideration facilitation of maintenance as an important aspect in support of ageing management.</p> <p>Ageing management is specifically described in the Equipment Reliability Program, BP-PROG-11.01 [R005, December 16, 2015], and is considered in design basis</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>aging management throughout the life of the plant.</p> <p>6. The results of the hazard analysis, deterministic safety analysis and probabilistic safety assessment are taken into account.</p> <p>7. Due consideration is given to the prevention of accidents and mitigation of their consequences.</p> <p>8. The generation of radioactive and hazardous waste is limited to minimum practicable levels, in terms of both activity and volume.</p> <p>9. A change control process is established to track design changes to provide configuration management during manufacturing, construction, commissioning and operation.</p> <p>10. Physical protection systems and cyber security programs are provided to address design-basis threats.</p>	<p>management, as per BP-PROG-10.01 [R009], "Plant Design Basis Management". Specifically, implementing procedure BP-PROC-00363, "Nuclear Safety Assessment", takes into account the effects of ageing. This procedure defines the elements, functional requirements, implementing procedures and key responsibilities associated with the Nuclear Safety Assessment (NSA) process. The objective of NSA is to ensure that all necessary nuclear safety requirements are defined for the actual or proposed design of the plant throughout the design modification process or in addressing emergent issues (e.g., plant ageing) that may affect the Design Basis or the Safety Report Basis. NSA is the systematic process carried out, throughout the design modification process or in addressing emergent issues (e.g., plant ageing) that may affect the Design Basis or the Safety Report Basis, to ensure that all necessary nuclear safety requirements are defined for the actual or proposed design of the plant.</p> <p>The implementation of Human Factor processes into plant modifications is addressed in procedure DPT-PDE-00013 [R008, June 16, 2014], Human Factors Engineering Program Plan. The procedure provides direction in implementing Human Factor processes into changes performed under the Design Change Package procedures BP-PROC-00539 [R016, June 23, 2015], If the classification of the human factors is determined to be "minor", DPT-PDE-00001 [R004, September 03, 2014], Human Factors Minor Change is to be followed.</p> <p>BP-PROC-00335 [R007, July 30, 2015], Design Management and BP-PROC-00363 [R003, January 24, 2013], Nuclear Safety Assessment are fundamentally iterative processes</p>	


 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>that provide assurance that the plant design basis as described in design documents and the safety analysis as described in the Safety Report (SR) agree and thus provide a consistent basis for safe operation. This iterative process continues until a design solution has been reached that meets all the safety requirements including those that may evolve during the course of design.</p> <p>The design intent is to provide, for a station operating over an expected range of conditions, a radioactive waste management system for each significant effluent route which is capable of limiting emissions to the target levels indicated in Part 1, Section 1.4.5 of the Safety Report. The design and operation of the active waste treatment facilities are governed by the derived emission limits that are explained in Part 1, Section 1.4 of the Safety Report. Several basic treatment processes are used in the management of these wastes depending upon their nature and activity level and these are discussed in the corresponding sections of this assessment document. The Conventional and Hazardous Waste Management Program BP-PROC-00888 [R001, November 2015] procedure ensures that Bruce Power is in compliance with applicable federal, provincial, and municipal regulations and corporate requirements affecting the generation, handling, storage, and disposal of conventional and hazardous waste.</p> <p>The Bruce Power Engineering Change Control program [BP-PROG-10.02, R010, November 12, 2014] specifies the manner in which design changes and modifications are defined, planned, implemented, and controlled. The Engineering Change Control (ECC) program objective is to ensure that design changes and modifications are controlled</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


Article No.	Clause Requirement	Assessment	Compliance Category
		<p>such that SSCTs continue to meet the design basis and operate safely for the full duration of design life.</p> <p>Due to sensitivity of the information, the issues related to design basis threats and cyber security are addressed elsewhere as part of the review process.</p>	
5.3	<p>Processes, procedures and practices shall be established as part of the overall management system so as to achieve the design objectives. This shall include identifying all performance and assessment parameters for the plant design, as well as detailed plans for each SSC, in order to ensure consistent quality of the design and the selected components.</p> <p>The design controls shall be such that the initial design, and any subsequent change or safety improvement, is carried out in accordance with established processes and procedures which call on appropriate standards and codes and address applicable requirements and design bases. Appropriate design control measures shall also facilitate identification and control of design interfaces.</p> <p>The adequacy of the design, including design tools and design inputs and outputs, shall be verified or validated by individuals or groups that are independent from those who originally performed the work. Verifications, validations, and</p>	<p>The changes in the text of this clause reflect the new terminology, i.e., design control measures versus quality assurance program. New requirement for qualification of the computer software used for design and analysis calculation is added.</p> <p>The Management System Manual [BP-MSM-1] assigns responsibility for the Plant Design Basis Management Program [BP-PROG-10.01] to the Engineering Division. The Engineering Division Organizational Manual [DOM-ENG-00001, R009, August 03, 2011] in turn, delegates the responsibility for the implementation and execution of the Nuclear Safety Assessment Procedure [BP-PROC-00363] to the Nuclear Safety Analysis and Support (NSAS) Department. The organization of NSAS is described in its organization manual [DPM-NSAS-00001, R008, October 14, 2011]. This manual describes the responsibilities of the functionaries of the department. Section 4.3 of the Quality Assurance of Safety Analysis [DPT-NSAS-00001, R006, August 20, 2014] specifies the required personnel capability as Staff assigned with the authority and responsibility for NSA will have adequate education, training, experience, supervision and capability to perform their assigned tasks effectively and to understand the importance of assuring nuclear safety. Staff capability records will be maintained.</p> <p>The procedure on Configuration Management of Safety</p>	Gap



 <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>approvals shall be completed before the detailed design is implemented.</p> <p>The computer software used for design and analysis calculations shall be qualified in accordance with applicable standards.</p> <p>Guidance</p> <p>Design control measures, in the form of processes, procedures and practices, include:</p> <ul style="list-style-type: none"> <li>• design initiation, including identification of scope</li> <li>• work control and planning of design activities</li> <li>• selection of competent staff</li> <li>• identification and control of design inputs</li> <li>• establishment of design requirements</li> <li>• evaluation of design concepts and selection of preferred concept</li> <li>• selection of design tools and computer software</li> <li>• conduct of conceptual safety analysis to</li> </ul>	<p>Analysis Software [DPT-NSAS-00011, R004, October 11, 2013] was prepared in consideration of N286.7-99. Although Bruce Power does not perform development or maintenance activities of the safety analysis software, it has acquired the right to use these computer codes from the Hosting Organizations by multiparty or bilateral agreements. As such, this procedure is limited to the description of the processes for use of safety analysis software, requesting software changes to the owner organizations and modification to scripts and utility codes.</p> <p>On the formal process to assess and update the safety analysis, Bruce Power procedure [DPT-NSAS-00002, R004, September 14, 2011] established the Safety Report update process and [DPT-NSAS-00003, R004, September 14, 2011] documents the guidelines for evaluating and prioritizing Safety Report issues.</p> <p>The original design met all of the codes and standards (or identified and agreed exclusions). The Bruce Power procedures for implementing design changes and the standards that will be used for these changes are documented in corresponding procedures as discussed in compliance notes for clauses 5, 5.1 and 5.2. A summary of the applicable procedures is presented as follows:</p> <p>1. This procedure on Quality Assurance of Safety Analysis [DPT-NSAS-00001, R006, August 20, 2014] specifies the QA process for performing Nuclear Safety Assessments and includes requirements for personnel under Section 4.3 on Personnel Capability. In the context of this procedure, nuclear safety assessment integrates deterministic safety analysis, the station Probabilistic Risk Assessments (PRA) and their ancillary analyses and</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>assess preferred design concept</p> <ul style="list-style-type: none"> <li>conduct of detailed design and production of design documentation and records</li> <li>definition of any limiting conditions for safe operation</li> <li>design verification and validation</li> <li>configuration management</li> <li>identification and control of design interfaces</li> </ul> <p>CSA N286, Management system requirements for nuclear power plants, is the Canadian standard identifying management system requirements for the design, purchasing, construction, installation, commissioning, operating, and decommissioning of NPPs. CNSC G-149, Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors, and CSA N286.7, Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants, provide complementary requirements and guidance for analytical, scientific and design computer programs.</p> <p>Organizations from nations not using the aforementioned documents should identify the codes, standards, and specifications on which their design and safety analysis control measures</p>	<p>assessments, and fitness for service assessments. It addresses and documents safety issues, including licensing requirements, risk to the public, risk to the plant, Operating Experience (OPEX), and practicality and operability.</p> <p>2. [DPT-NSAS-00015, R004, October 16, 2013] procedure on Planning and Execution of Nuclear Safety Assessments outlines the systematic methodology for conducting safety analysis.</p> <p>3. [DPT-NSAS-00013, R003, September 20, 2011] procedure on Guidelines for Managing Reference Data Sets ensures that only verified datasets are used for deterministic safety analysis.</p> <p>4. This practice has been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report.</p> <p>5. Not all of the existing analyses have used validated models and computer codes that would meet the current standards.</p> <p>6. This practice has been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report.</p> <p>7. This procedure on Planning and Execution of Nuclear Safety Assessments [DPT-NSAS-00015] outlines the review process for safety analyses.</p> <p>Qualification of computer software used for design and analysis calculations is further discussed in the clause-by-clause assessment against requirements of CNSC REGDOC-2.4.1 in Safety Factor 5.</p>	

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>are based, whether national or international – such as IAEA GS-G-3.5, The Management System for Nuclear Installations Safety Guide, referenced publications, and ISO 9001:2008 Quality Management Systems – Requirements. Such control measures should be mapped to the requisite CSA N286 clauses to demonstrate that they satisfy Canadian requirements. Where gaps are identified, the measures to address them should be described.</p> <p>Organizational processes and procedures can be specific to design and safety analysis, or be part of an overall management system (or quality assurance program) for other NPP lifecycle activities. In the latter case, the organization should identify those processes and procedures applicable to design and safety analysis.</p> <p>There are no specific platforms, styles or format requirements for documenting design control measures; however, design organizations should identify the types of documents, the style, the format and the media (paper-based, electronic or Web-based) they intend to use to control their design activities.</p> <p>Additional information</p>	<p>In general, the practice as defined in this clause has been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report for which validated codes have been available in the past. It is standard practice for all new safety analyses. However, the original design analyses had been produced using legacy tools predating N286.7-99. This is identified as a gap and further discussed in the clause-by-clause assessment against requirements of CNSC REGDOC-2.4.1 in Safety Factor 5 (Gap).</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>American Society of Mechanical Engineers (ASME), NQA-1-2008, Quality Assurance Requirements for Nuclear Facility Applications, New York, 2008.</li> <li>CNSC, G-149, Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors, Ottawa, Canada, 2000.</li> <li>CSA Group, N286, Management system requirements for nuclear power plants, Toronto, Canada.</li> <li>CSA Group, N286.7.1, Guideline for the application of N286.7-99, Quality assurance of analytical, scientific, and design computer programs for nuclear power plants, Toronto, Canada.</li> <li>IAEA, GS-R-3, The Management System for Facilities and Activities, Vienna, 2006.</li> <li>Nuclear Information and Records Management Association/American National Standards Institute (ANSI), 1.0, Standard Configuration Management, Washington, D.C., 2007.</li> </ul>		
5.4	The design authority shall identify the modern	There is no change to the requirements.	C


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>codes and standards that will be used for the plant design, and evaluate those codes and standards for applicability, adequacy, and sufficiency to the design of SSCs important to safety.</p> <p>Where needed, codes and standards shall be supplemented to ensure that the final quality of the design is commensurate with the necessary safety functions.</p> <p>SSCs important to safety shall be of proven design, and shall be designed according to the standards and codes identified for the NPP.</p> <p>When a new SSC design, feature or engineering practice is introduced, adequate safety shall be demonstrated by a combination of supporting research and development programs and by examination of relevant experience from similar applications. An adequate qualification program shall be established to verify that the new design meets all applicable safety requirements. New designs shall be tested before being brought into service and shall be monitored while in service so as to verify that the expected behaviour is achieved.</p> <p>The design authority shall establish an adequate</p>	<p>Bruce B design meets the intent of this requirement. All of the SSCs important to safety have been in place at Bruce B for 30 years (proven design). They were originally designed based upon experience gained from earlier plants (NPD, Douglas Point, Pickering A, Bruce A). Design changes over the years have been based upon design improvements (e.g., in-core detector assemblies) that have been tested and proven elsewhere. See Section 1.3 of Part 1 of the Safety Report [NK29-SR-01320-00001, R005].</p> <p>All future design changes will be in accordance with BP- PROG-10.01, Plant Design Basis Management, which governs BP- PROC-00335, Design Management, the latter of which interfaces with the implementing procedures of BP- PROG-10.02, Engineering Change Control. For example, BP- PROC-00539, Design Change Package "specifies the control of modifications to plant systems, structures, components... to meet regulatory requirements, ensure safety..."(section 1.0)</p> <p>As an illustration of the application of this process, there were at least two design modifications incorporated into the design, 37 element fuel bundles and self-powered in-core detectors. Both of these features had undergone comprehensive testing at Chalk River Laboratories. During the early years of operation, both were examined extensively to demonstrate that they met their objectives. The fuel bundles fully met their requirements and continue to exhibit very low failure rates. The self-powered detectors demonstrated that they could meet their functional requirements but experience showed that the containers in which they were encapsulated required modification. The containers have been modified and are now functioning</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>qualification program to verify that the new design meets all applicable safety design requirements.</p> <p>In the selection of equipment, due attention shall be given to spurious operation and to unsafe failure modes (e.g., failure to trip when necessary). Where the design has to accommodate an SSC failure, preference shall be given to equipment that exhibits known and predictable modes of failure, and that facilitates repair or replacement.</p>	<p>satisfactorily.</p> <p>For any new design, the process to be followed is defined in Design Management procedure [BP-PROC-00335, R007, July 30, 2015] and it shows that the required objectives are achieved as discussed earlier.</p> <p>The original design requirements for the Bruce A and B safety systems require that "As far as possible systems affecting safety shall be designed so that failure of component will result in the system or plant going to a more safe condition." Furthermore, the regulating system was designed "So that the reactor is shutdown, or, a channel of multi-channel system rejected, on failure of any major component of the system." A general requirement of all systems is that "As far as possible the plant shall be designed to facilitate maintenance." At the time when Bruce A was built, there was concern for spurious activation of the shutdown systems since there were considerably more trip parameters as well as a second shutdown system. Therefore each process and nuclear measurement loop that is essential for the operation of the special safety systems is redundantly designed, usually triplicated such that a single loop component or power supply failure will not incapacitate or spuriously invoke operation of the special safety system. To date spurious operation of the systems has not been a problem. Provision was made for the operation of the instrumentation and control circuitry under loss of normal plant power. Normal power is backed up by standby ac power for all instrumentation. Where feasible, elements and circuits are designed to "fail safe". For a final control element, "fail safe" is the position that provides the safest process condition. Special safety system components are designed</p>	



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


Article No.	Clause Requirement	Assessment	Compliance Category
		such that the most likely failure modes are in the fail-safe direction. Failures that are not automatically revealed are detected during the extensive testing required to demonstrate that the systems important to safety are available.	
5.5	<p>The NPP design shall draw on operational experience that has been gained in the nuclear industry, and on the results of relevant research programs.</p> <p>Guidance</p> <p>The design authority should describe the major design features, changes and improvements that have been incorporated as a result of operational experience and safety research including:</p> <ul style="list-style-type: none"> <li>• resolution of applicable safety issues from existing reactor designs</li> <li>• improvements in design due to advances in materials and their properties</li> <li>• improved methods of design and safety assessment</li> <li>• improved methods of construction and fabrication</li> <li>• improvements in reliability, operability and maintainability</li> </ul>	<p>There are no changes introduced in this clause.</p> <p>As documented in section 1.0 Of [BP-PROG-01.06, R014, July 18, 2014], the objective of the Bruce Power Operating Experience Program is to define the processes used to identify and capture lessons learned from sources within Bruce Power, and external to Bruce Power, in order to continuously improve performance by making improvements to processes, procedures, training or system/ equipment design. Bruce Power is making improvements via processing internal and external operating experience information, conducting Focus Self Assessments, Benchmarking others, and by attending industry conferences and workshops.</p> <p>The Nuclear Safety Assessment procedure [BP PROC 00363 R003] defines the elements, functional requirements, implementing procedures and key responsibilities associated with the Nuclear Safety Assessment (NSA) process. The objective of NSA is to ensure that all necessary nuclear safety requirements are defined for the actual or proposed design of the plant throughout the design modification process or in addressing emergent issues (e.g., plant ageing) that may affect the Design Basis or the Safety Report Basis. NSA is the systematic process carried out, throughout the design modification process or in addressing emergent issues (e.g., plant ageing) that may affect the Design Basis or the Safety Report Basis, to ensure that all necessary nuclear safety requirements are defined for the actual or proposed</p>	C

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00


Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>improved methods to mitigate the occurrence and consequences of human error</li> <li>improved methods in support of ALARA</li> </ul> <p>Operational experience can be found in documents such as the IAEA yearly publication Operating Experience with Nuclear Power Stations in Member States.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>IAEA Safety Guide Series NS-G-2.11, A System for the Feedback of Experience from Events in Nuclear Installations, Vienna, 2006.</li> </ul>	<p>design of the plant. BP- PROC- 00335, Design Management (interfacing document) and Nuclear Safety Assessment (BP- PROC-00363) are fundamentally iterative processes that provide assurance that the plant Design Basis as described in design documentation and the safety analysis as described in the SR agree and provide a consistent basis for safe operation. The process to identify, evaluate and apply lessons learned from operational issues, both from within Bruce Power and from the industry, is defined in, Processing External and Internal Operating Experience [BP-PROC-00062, R016, August 13, 2015]. The procedure addresses the issues arisen due to findings from Research and Development activities being performed on behalf of Bruce Power and the industry; issues due to findings from ongoing industry analysis programs, both within and outside Bruce Power etc.</p> <p>For example, Bruce Power and other Canadian utilities began assessing and taking actions to address the lessons learned immediately following the Fukushima accident.</p> <p>Further detailed discussions regarding use of operating experience from other plants and research findings are provided in Safety Factor 9.</p>	
5.6	<p>Safety assessment is a systematic process applied throughout the design phase to ensure that the design meets all relevant safety requirements. The safety assessment for the design shall include the requirements set by the operating organization and by regulatory authorities. The basis for the safety assessment shall be the data derived from the safety analysis,</p>	<p>There are no changes in the requirements.</p> <p>As discussed in BP-PROC-00363, R003 Nuclear Safety Assessment is the systematic process carried out, throughout the design modification process or in addressing emerging issues e.g., plant ageing that may affect the design basis or the Safety Report basis. Nuclear Safety Assessment ensures that all necessary safety requirements are defined for the actual or proposed plant design. The Nuclear Safety</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>previous operational experience, results of supporting research, and proven engineering practices.</p> <p>The safety assessment shall be part of the design process, with iteration between the design and analyses, and shall increase in scope and level of detail as the design process progresses.</p> <p>Before the design is submitted, an independent peer review of the safety assessment shall be conducted by individuals or groups separate from those carrying out the design.</p> <p>Safety assessment documentation shall identify those aspects of operation, maintenance and management that are important to safety. This documentation shall be maintained in a dynamic suite of documents, to reflect changes in design as the plant evolves.</p> <p>Safety assessment documentation shall be presented clearly and concisely, in a logical and understandable format, and shall be made readily accessible to designers, operators and the CNSC.</p> <p>Guidance</p>	<p>Assessment process integrates safety analysis, probabilistic risk assessment and criticality safety evaluations.</p> <p>BP-PROC-00335, R007 Design Management and BP-PROC-00363, R003, Nuclear Safety Assessment are fundamentally iterative processes that provide assurance that the plant design basis as described in design documents and the safety analysis as described in the Safety Report (SR) agree and thus provide a consistent basis for safe operation. This iterative process continues until a design solution has been reached that meets all the safety requirements including those that may evolve during the course of design.</p> <p>Nuclear Safety Assessment (NSA) establishes the bounds for the design basis of the plant by means of appropriate analytical tools, thereby ensuring that the overall plant design is capable of meeting prescribed and acceptable limits for radiation doses and releases for all plant conditions and design basis accidents. The plant design models and design basis data will be kept up to date throughout the life of the plant to ensure the validity of the Safety Analysis. This updating may include new information as it becomes available such as new physical phenomena, may use more up-to-date methodology and approach where necessary, and may assess the performance of modifications to the design of the plant and operating procedures that may be under consideration.</p> <p>The Safety Analysis supports safe operation by serving as an important tool in developing and confirming plant protection and control system set points and control parameters. It is also used to establish and validate operating specifications and limits, normal and off-normal operating procedures, maintenance and inspection requirements, and normal and</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>As per IAEA GSR Part 4, Safety Assessment for Facilities and Activities, aspects considered in the safety assessment should include:</p> <ul style="list-style-type: none"> <li>• defence in depth</li> <li>• safety margins</li> <li>• multiple barriers</li> <li>• safety analysis (including both deterministic and probabilistic approaches), as well as overall scope, approach, safety criteria, uncertainty and sensitivity analysis, use of computer codes, and use of operating experience</li> <li>• radiation risks</li> <li>• safety functions</li> <li>• site characteristics</li> <li>• radiation protection</li> <li>• engineering aspects</li> <li>• human factors</li> <li>• long-term safety</li> </ul> <p>The independent peer review should be performed by suitably qualified and experienced individuals.</p>	<p>emergency procedures. The Safety Analysis is managed to ensure timely resolution of new technical issues that arise over the life of the plant.</p> <p>Verification activities, including independence, qualification of staff, documentation of results, correction of deficiencies and specialized Technical Reviews are covered in DPT-PDE-00007, [R009, November 01, 2013], Design Verification. Several levels of review may take place, depending upon the significance of the design change being proposed.</p> <p>The verification methods are described in Appendix E of DPT-PDE-00007. (section 3.1.15 of DPT-PDE-00007) states: "Peer Verification (Mandatory) - Verification of the design documents by an independent and competent individual by review and comments on the design documents".</p> <p>Specialty (if required) review is arranged by specialty discipline(s), e.g., chemical or biological occupational health hazards, fire protection, machine guarding, human factors, and seismic or stress analysis.</p> <p>Technical Review is a verification method that is less formal and more flexible in scope, timing, conduct, review and documentation than a formal technical review. It is part of the design process to confirm that a design, activity, or condition satisfies the design requirements (section 3.1.19 of DPT-PDE-00007). Technical Review process is depicted in Appendix C.</p> <p>Formal Technical Review (if required) is a planned, systematic, documented and reported, disciplined review of selected systems, structures, and equipment, by personnel experienced in design, construction, and operation, such that</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>IAEA, GSR Part 4, Safety Assessment for Facilities and Activities, Vienna, 2009.</li> </ul>	<p>an appropriate broad engineering knowledge is synergistically applied to accomplish design verification. It is a critical evaluation of a design at predefined stages of the design process. For formal technical reviews, a review committee is established and participants are identified based on the disciplines involved in the design, which may include representatives from stakeholder organizations. The process for formal technical review is described in Appendix B of DPT-PDE-00007.</p> <p>The probabilistic safety assessment is covered in detail in the assessment of CNSC REGDOC-2.4.2 documented in Safety Factor 6. The requirement for independent peer review of safety assessments by suitably qualified and experienced individuals is reflected in the Bruce Power's quality management processes and procedures. External reviews are conducted as appropriate. For example, the acceptability of probability estimates in the containment event tree analysis for Level 2 at-power PRA report B0900/RP/055 R01, December 2013 (Enclosure 4 of NK21-CORR-00531-10958/NK29-CORR-00531-11342, Submission of S-294 Probabilistic Risk Assessment Deliverables, Bruce Power letter, F. Saunders to R. Lojk, December 24, 2013) was supported via an expert review process conducted by a four people expert panel (from Canada, US and UK).</p> <p>As described before, the SOE program ensures that the operation, maintenance and management that are important to safety. Bruce A and B PROL and LCH (licence condition 3.1 Operations Program), "shall at all times maintain and operated the nuclear facilities within the limits of the OP&amp;P and SOE. The program is established based on the guidance of COG-02-901 P&amp;G on the definition, Implementation and</p>	


 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>maintenance of SOE consistent with CSA N290.15-10 requirements. The implementation strategy for N290.15 full compliance includes updates of Bruce Power program documents and completion of the associated training requirements. As indicated in [NK21-CORR-00531-12546 / NK29-CORR-00531-12972] the completion date for these administrative updates is February 2016.</p> <p>All documents important to the safe operation of the plant are issued as "Controlled Documents" and are subject to the rules outlined in the Document Management Program [BP-PROG-03.01, R016, August 31, 2015]. The design documentation shall be maintained in a dynamic suite of documents, to reflect changes in design as the plant evolves. The most relevant implementation procedures are BP-PROC-00363, Nuclear Safety Assessment, DPT-NSAS-00012, [R004, October 28, 2014] Preparation and Maintenance of Operational Safety Requirements, and DPT-RS-00015, [R000, May 31, 2011] Safe Operating Envelope Gap Assessment.</p> <p>Detailed discussions related to safety assessment requirements are presented in Safety Factor 5 and Safety Factor 6.</p>	
5.7	Design documentation shall include information to demonstrate the adequacy of the design and shall be used for procurement, construction, commissioning and safe operation, including maintenance, aging management, modification and eventual decommissioning of the NPP.	<p>The introductory paragraph in this clause is new and includes reference to ageing management. In addition, a requirement for the design documentation to demonstrate the adequacy of the design is introduced. Cyber security programs are included in item 5.</p> <p>A general design description of the plant is provided in Parts 1 and 2 of the Bruce B Safety Report. The system Design Requirements were originally specified as part of the System</p>	C




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design documentation shall include:</p> <ol style="list-style-type: none"> <li>1. design description</li> <li>2. design requirements</li> <li>3. classification of SSCs</li> <li>4. description of plant states</li> <li>5. security system design, including a description of physical security barriers and cyber security programs</li> <li>6. operational limits and conditions</li> <li>7. identification and categorization of initiating events</li> <li>8. acceptance criteria and derived acceptance criteria</li> <li>9. deterministic safety analysis</li> </ol>	<p>Design Manuals and were provided to the AECB at the time of the design. Design Requirements for modifications are prepared according to Engineering Change Control procedure BP-PROG-10.02 [R010, November 12, 2014]. A Safety Related Systems list has been developed. This has evolved over the years and is now more extensive and more detailed than that originally produced when the plant was first licensed. Due to the sensitivity of information, security systems design and cyber security programs are assessed elsewhere.</p> <p>Bruce Power has introduced Operational Safety Requirements (OSRs), which essentially provide the same functions as OLCs. These are based upon the latest requirements of the safety analysis.</p> <p>Section 2.1, Identification of Initiating Events, of Part 3 of the Bruce B Safety Reports states that all systems and components are reviewed to identify those containing significant quantities of radioactive materials. For each source of radioactive material, it is possible to determine ways in which unplanned release of this material can occur, based on knowledge of the plant processes and past experience in selecting initiating events. This process leads to a comprehensive list of internal initiating events presented in Table 2-1. To complete the list of abnormal events, all combinations of initiating events and compounding failures in the special safety systems and other mitigating systems are identified.</p> <p>Bruce Power is leading a COG team to develop the recommendations of the Independent Technical Panel (ITP) into a set of Derived Acceptance Criteria (DAC) acceptable to the CNSC for future deterministic safety analysis performed</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>10. probabilistic safety assessment (PSA)</p> <p>11. hazard analysis</p> <p>Guidance</p> <p>A suite of design documentation should be developed, following the establishment of an overall baseline, listing all key design documents. Design documents should be contained in a logical and manageable framework.</p> <p>For additional guidance on derived acceptance criteria, refer to CNSC regulatory document REGDOC-2.4.1, Deterministic Safety Analysis.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>CNSC, RD/GD-369, Licence Application Guide: Licence to Construct a Nuclear Power</li> </ul>	<p>to support safe operation and RD-310 implementation. A report "Derived Acceptance Criteria for Deterministic Safety Analysis" (COG-13-9035) documents the derived acceptance criteria to be applied to deterministic safety analysis of postulated accidents and considers uncertainties in DAC; additional work is in progress. Further details are given in Safety Factor 5.</p> <p>The deterministic safety analysis is documented in Part 3 of the Safety Report. The Safety Report has been updated periodically, with the latest update performed in 2012. The Bruce B Probabilistic Risk Assessment (PRA) includes Level 1 and Level 2 analyses. The Bruce B Probabilistic Risk Assessment (BBRA) 2 models form the basis of determining the risk significant systems. The models are routinely updated with field engineering changes of the modeled systems. The models for Bruce B are also augmented each year with observed failure rate data using a Bayesian methodology. The Bruce B Probabilistic Risk Assessment (BBRA) had one major update completed to the unavailability models for the SIS in 2015. The restoration time update was completed on Negative Pressure Containment (NPC) system in 2015. The Negative Pressure Containment system Predicted Future Unavailability (PFU) which was already below the target in 2014 showed some improvement in the Radiation Accident parameter PFU due to the update of component restoration times. The PFU decreased further when the model was updated with the 2015 observed failure data. There were no changes to the list of SIS or their unavailability targets in 2015 [Enclosure 1 to NK29-CORR-00531-13197 Letter F. Saunders to K. Lafreniere, Bruce B Annual Reliability Report -2015, April 28, 2016. The list of current Bruce PRA analyses and corresponding guides is</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Plant, Ottawa, Canada, 2011.</p> <ul style="list-style-type: none"> <li>CNSC, REGDOC-2.4.1, Deterministic Safety Analysis, Ottawa, Canada, 2014.</li> </ul>	<p>presented in Safety Factor 6.</p> <p>The Bruce B design documentation does include Hazard Analysis. The detailed hazard analysis of protection against fire is documented in NK29-REP-71400-00004, NK29-REP-71400-00003 and NK29-REP-71400-00002. The safety-related systems in Bruce B requiring seismic qualification against earthquakes are defined in Design Guide NK29-DG-03650-002. The seismic qualification is carried out as per DPT-PDE-00017.</p> <p>Other internal and external hazards are assessed and documented in Bruce Power External Hazards Assessment [B-03611.7 P NSAS] and Bruce Power Probabilistic Risk Assessment Guide - High Wind Hazard [B-REP-03611-00012]. Additional information is provided in compliance notes for clause 9.3 Hazard Analysis. Detailed assessments related to hazards analysis are documented in Safety Factor 7.</p> <p>The design documentation follows well established processes and procedures as described in Design Documentation [BP-PROC-00335, R007, July 30, 2015]. This procedure specifies the design activities and outputs that define and manage the Plant Design Basis such that the nuclear operating stations can operate safely and reliably for the duration of their design life. Design Management relies upon the implementing procedures of BP-PROC-00363, Nuclear Safety Assessment to ensure nuclear safety requirements are incorporated into the design. Under the Equipment Reliability Program, BP-PROG-11.01, [R005, December 16, 2015] life cycle management integrates ageing management and economic planning to optimize the service life of SSCs and maintain an acceptable level of performance</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>and safety over the life of the plant. As described in section 4.1 of BP-PROC-00400 [R002, July 05, 2013] "Life Cycle Management for Critical SSCs", the author of a Life Cycle Management Plan (LCMP) reviews relevant documentation including design requirements and design descriptions when preparing or revising the LCMP. In addition, design changes described in design documentation can trigger a review of LCMPs.</p> <p>The assessment of CNSC REGDOC-2.4.1 is documented in Safety Factor 5.</p>	
6.1	<p>The design of an NPP shall incorporate defence in depth. The levels of defence in depth shall be independent to the extent practicable.</p> <p>Defence in depth shall be achieved at the design phase through the application of design provisions specific to the five levels of defence.</p> <p>Level One</p> <p>Achievement of Level one defence in depth shall include conservative design and high-quality construction to provide confidence that plant failures and deviations from normal operations are minimized and accidents are prevented.</p> <p>This shall entail careful attention to selection of</p>	<p>The introductory paragraph to this clause is new and requires independence of the levels of defence in depth.</p> <p>As presented in section 6.1.1 of the Bruce B Safety Report Part 2 [NK29-SR-01320-00001] in order to effectively reduce the risk presented by a postulated process system failure, special safety systems are independent of process systems, including the reactor regulating system, whose failure might require the subsequent action of the special safety system.</p> <p>To the greatest extent practicable, the special safety systems are also independent of each other in design and operation. This requirement evolves from the Canadian reactor safety principle of analyzing each postulated process system failure in conjunction with a failure of each of the special safety systems in turn.</p> <p>As an additional feature, credit is not taken for both shutdown systems acting together. The provision of two independent reactor shutdown systems with high reliability ensures that at least one will operate following any single process failure.</p> <p>Bruce B design provides the layers of defence against the</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>appropriate design codes and materials, design procedures, equipment qualification, control of component fabrication and plant construction, and use of operational experience.</p> <p>Level Two</p> <p>Level two shall be achieved by controlling plant behaviour during and following a postulated initiating event (PIE) using both inherent and engineered design features to minimize or exclude uncontrolled transients to the extent possible.</p> <p>Level Three</p> <p>Achievement of Level three defence in depth shall include the provision of inherent safety features, fail-safe design, engineered design features, and procedures that minimize the consequences of DBAs. These provisions shall be capable of leading the plant first to a controlled state, and then to a safe shutdown state, and maintaining at least one barrier for the confinement of radioactive material. Automatic activation of the engineered design features shall minimize the need for operator actions in the early phase of a DBA.</p>	<p>release of fission products to the environment as described in Section 1.3.1 of Part 2 of Safety Report. These include:</p> <ol style="list-style-type: none"> <li>1 The uranium dioxide (UO<sub>2</sub>) fuel, which contains almost all the radioactivity, is a ceramic with high melting point sealed in a corrosion resistant metallic cladding;</li> <li>2 The zirconium alloy fuel element sheath which has been demonstrated over thirty years to have a very low failure rate</li> <li>3 The Heat transport system designed to high quality, which contains any leakage from the fuel sheath;</li> <li>4 The sub-atmospheric Containment System designed to retain a large fraction of any fission products released from the heat transport system following an accident. In addition, the Filtered Air Discharge System removes particulates and iodine from controlled release following re-pressurization of containment;</li> <li>5 The exclusion boundary that provides a separation between the station and the public. An emergency response centre and emergency response plans which are in place to mitigate the consequences of any release from the station.</li> </ol> <p>The first three barriers prevent radioactive release accidents. As long as they are intact, very little radioactive material will escape into the reactor building. If it does, containment comes into play to mitigate doses. The fundamental principles that guide the design of CANDU reactors can be categorized as accident prevention and accident mitigation. Accident Prevention is based on built-in high quality and reliability to minimize the stresses on the first three barriers, as well as on accident anticipation. Accident Mitigation aims</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Level Four</p> <p>Level four shall be achieved by providing equipment and procedures to manage accidents and mitigate their consequences as far as practicable.</p> <p>Most importantly, adequate protection shall be provided for the confinement function by way of a robust containment design. This includes the use of complementary design features to prevent accident progression and to mitigate the consequences of DEC's. The confinement function shall be further protected by severe accident management procedures.</p> <p>Level Five</p> <p>The design shall provide adequately equipped emergency support facilities, and plans for onsite and offsite emergency response.</p> <p>Guidance</p> <p>IAEA INSAG-10, Defence in Depth in Nuclear</p>	<p>to minimize the consequences of accidents through anticipation and built-in defences (such as the last two barriers to release above).</p> <p>The Bruce B design meets the general requirements for the first level of defence namely; the plant be soundly and conservatively designed, constructed, maintained and operated in accordance with appropriate quality levels and engineering practices, such as the application of redundancy, independence and diversity. To meet this objective, careful attention is paid to the selection of appropriate design codes and materials, and to the control of fabrication of components and of plant construction.</p> <p>The second level of defence detects and intercepts deviations from normal operational states in order to prevent anticipated operational occurrences from escalating to accident conditions. This is done by measuring deviations from normal operating conditions by both the regulating system and the special safety systems. The process features of the regulating system (liquid zone control and setback function) and the safety features (stepback function) can shut the reactor down for all but the most serious PIEs. Either of the two fully independent shutdown systems is capable of shutting the reactor down for all PIEs, should the regulating system not be able to do this. In the case of fuel overheating, the ECI system can prevent failure of the fuel sheath (barrier 2) for all but the most serious LOCAs.</p> <p>In regard to item (3), the ECI or moderator systems are capable of maintaining the integrity of the Heat Transport system (barrier 3) for design basis accidents.</p> <p>As indicated in the compliance assessment against CNSC</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Safety, provides information regarding the concept and application of defence in depth.</p> <p>Guidance on performing a systematic assessment of the defence in depth can be obtained from the IAEA safety reports series No. 46, Assessment of Defence in Depth for Nuclear Power Plants.</p> <p>The application of defence in depth in the design should ensure the following:</p> <ul style="list-style-type: none"> <li>• The approach to defence in depth used in the design should ensure that all aspects of design at the SSCs level have been covered, with emphasis on SSCs that are important to safety.</li> <li>• The defence in depth should not be significantly degraded if the SSC has multiple functions (e.g., for CANDU reactors, the moderator and end-shield cooling systems may serve the functions of a process system and include the functions of mitigating DEC's).</li> <li>• The principle of multiple physical barriers to the release of radioactive material should be incorporated in the design; there should be a limited number of cases where there is a reduction in the number of physical barriers (as</li> </ul>	<p>REGDOC-2.4.1 in Safety Factor 5, Level 2 defence in depth is not demonstrated explicitly for AOOs and is identified as a gap (Gap).</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>may be the case where some components carrying radioactive material serve the function of primary coolant barrier and containment), and adequate justification should exist for such design choices.</p> <ul style="list-style-type: none"> <li>The design (e.g., in safety design guides, management system programs) should provide: <ul style="list-style-type: none"> <li>levels of defence in depth that are addressed by individual SSCs</li> <li>supporting analysis and calculation</li> <li>evaluation of operating procedures</li> </ul> </li> <li>The safety analysis should demonstrate that the challenges to the physical barriers do not exceed their physical capacity.</li> <li>The structure for defence in depth provisions at each level of defence should be established</li> </ul> <p>for a given plant design, and the evaluation of the design from the point of view of maintaining each safety function should be carried out. This evaluation should consider each</p> <p>and every one of the provisions for mitigation of a given challenge mechanism, and confirm that it is well founded, sufficient, feasible, and correctly engineered within the design.</p> <ul style="list-style-type: none"> <li>Special attention should be given to the feasibility of a given provision and the existence of</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>supporting safety analyses. Deficiencies in the completeness of the supporting safety analyses should be documented and flagged as issues to be queried.</p> <p>To ensure that different levels of defence are independently effective, any design features that aim to prevent an accident should not belong to the same level of defence as design features that aim to mitigate the consequences of the accident.</p> <p>The independence between all levels of defence should be achieved, in particular, through diverse provisions. The strengthening of each of these levels separately would provide, as far as reasonably achievable, an overall reinforcement of defence in depth. For example, the use of dedicated systems to deal with DEC's ensures the independence of the fourth defence level.</p>		
6.1.1	To ensure the overall safety concept of defence in depth is maintained, the design shall provide multiple physical barriers to the uncontrolled release of radioactive materials to the environment. Such barriers shall include the fuel matrix, the fuel cladding, the reactor coolant pressure boundary, and the containment. In addition, the design shall provide for an exclusion zone.	<p>A new requirement is introduced in item 4.</p> <p>In addition to notes in Clause 6.1, the minimum allowable performance standards for each of the Special Safety Systems are defined by the safety analyses and the requirement to shut down the reactor, or introduce compensatory measures, when these are not met are specified in the Operating Policies and Principles. (Note: The minimum allowable performance standards (MAPS) means the set of operating limits or the range of conditions established for components or subsystems which define the</p>	Gap

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>To the extent practicable, the design shall prevent:</p> <ol style="list-style-type: none"> <li>1. challenges to the integrity of physical barriers</li> <li>2. failure of a barrier when challenged</li> <li>3. failure of a barrier as a consequence of failure of another barrier</li> <li>4. the possibility of failure of engineered barriers from errors in operation and maintenance that could result in harmful consequences</li> </ol> <p>The design shall also allow for the fact that the existence of multiple levels of defence does not normally represent a sufficient basis for continued power operation in the absence of one defence level.</p>	<p>minimum acceptable states for those components or subsystems as credited in the safety analyses. Therefore, the minimum allowable performance standards are defined for each system and listed or referenced in the Safety Report and in the Operating Policies and Principles for the plant.)</p> <p>The Operating Policies and Principles - Bruce B, section 63.5 [BP-OPP-00001, R019] states: Regulating System Impairment: No portion of the regulating system shall be removed from service unless the ability to control reactor power is not impaired or the reactor has been placed in a guaranteed shutdown state.</p> <p>If the regulating system is incapable of controlling bulk power, then the reactor shall promptly be placed in a guaranteed shutdown state.</p> <p>If the regulating system is incapable of controlling the spatial power distribution, then the reactor power shall be reduced to a level where spatial control is not required.</p> <p>If the stepback or setback functions of the regulating system are impaired, and repairs cannot be made promptly, approval of the Senior Operations Authority and concurrence of the CNSC shall be obtained, on a case by case basis, for continued reactor operation.</p> <p>Human Factors Engineering Program Plan [DPT-PDE-00013, R008, June 16, 2014] provides direction in implementing Human Factor processes into changes performed under the Design Change Package procedures (BP-PROC-00539, R016, June 23, 2015). This procedure may also be applied to projects outside of the modifications procedures where it is deemed that a Human Factors (HF) review will provide added benefit. Examples would include changes to equipment</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>outside of BP- PROC-00539. For changes outside of BP- PROC-00539 the determination as to whether HF review is required will be made by the department manager or above of the line requesting the work in conjunction with the Manager, Plant Design Engineering (section 1.0 of DPT-PDE-00013). The Risk Assessment is part of the Licensing Basis for both Bruce A and Bruce B and contains human reliability modelling. There are Credited Human Actions that are most important to safety identified via a combination of probabilistic and deterministic analyses. If design changes impact event sequences in the Probabilistic Risk Assessment (PRA), human reliability estimates may be affected and these credited human actions are required to be assessed via a Human Reliability Analysis (HRA). Human Reliability Analysis is normally only monitored where Nuclear Safety Risk is at Levels 1, 2 or 3 on a project, or if an Abnormal Incidents Manual (AIM) action is impacted due to the potential for, and mechanisms of human error that might affect plant safety. If the change is found to meet the above level criteria, the affected human actions must be reviewed to determine if they affect the PRA or deterministic safety analysis. In some cases the deterministic safety analysis may include human actions that are credited in the analyses to prevent or mitigate the accidents and transients. These Human actions may, or may not, be found as risk important by the PRA but should be considered deterministically as significant requiring analysis or review. This must be addressed in design to minimize personnel errors, support their detection, and ensure recovery capability (element 6 of Appendix B of DPT-PDE-00013). As per BP-PROC-00539, all design change packages (DCPs) require at least a cursory level of HF involvement.</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		The list of internal initiating events is presented in Table 2-1 of Part 3 of the Bruce B Safety Report; however events initiated as a result of human errors in operation and maintenance are not explicitly identified. Initiating event frequencies include implicitly any relevant operator error that may cause the initiating event. Therefore, this is identified as a gap (Gap).	
6.2	<p>The NPP design shall provide adequate means to:</p> <ol style="list-style-type: none"> <li>maintain the plant in a normal operational state</li> <li>ensure the proper short-term response immediately following a PIE</li> <li>facilitate the management of the plant in and following DBAs and DEC's</li> </ol> <p>The following fundamental safety functions shall be available in operational states, DBAs and DEC's, except where the postulated accident involves a loss of that function:</p> <ol style="list-style-type: none"> <li>control of reactivity</li> </ol>	<p>New requirements for DEC's and shielding considerations are added to this clause.</p> <p>The Bruce A and B design incorporates control systems and special safety systems that meet the requirements as documented in Part 2 of the Safety Report [NK29-SR-01320-00001, R005]</p> <p>The regulating system is designed to maintain overall reactivity control during normal operation by controlling the light water level in the liquid zone controllers (A summary of the control system can be found in Section 7.1.1 of Part 2 of the Safety Report [NK29-SR-01320-00001 R005]). Long term reactivity control is achieved by on-power refueling. Medium and short term reactivity control is accomplished by zone controllers, adjusters, control absorbers and moderator poison. Addition or removal of moderator poison is normally controlled manually; however the addition of poison can be done under computer control if needed. The other reactivity devices are controlled from the control computers. The shutoff rods are withdrawn by the control computers after the trip has been cleared (section 7.1.4 of Part 2 of Safety Report). The reactor control program is described in section 7.2.2.3 of Part 2 of Safety Report. Under certain transient conditions, if the reactivity range of the liquid zone controllers</p>	IC



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2. removal of heat from the fuel</p> <p>3. confinement of radioactive material</p> <p>4. shielding against radiation</p> <p>5. control of operational discharges and hazardous substances, as well as limitation of accidental releases</p> <p>6. monitoring of safety-critical parameters to guide operator actions</p> <p>These safety functions shall apply to the reactor as well as fuel storage and handling.</p> <p>SSCs necessary to fulfill safety functions following a PIE shall be identified. This approach shall identify the need for such functions as reactor shutdown, emergency core cooling, containment, emergency heat removal and power systems.</p>	<p>is exceeded, then further control is achieved via the regulating system by using the Control Absorbers. If this additional control is not adequate then the regulating system can shut down the reactor through either the setback or the stepback routines. Under certain accident conditions if the reactivity control capability of the regulating system cannot keep parameters within acceptable limits, each of the two independent shutdown systems is capable of safely shutting down the reactor and maintaining it subcritical in accordance with CNSC requirements.</p> <p>Heat removal from the core is provided by a variety of systems (steam reject from the steam generators with feed water supplied by the auxiliary boiler feed pump, inter-unit feedwater tie, emergency boiler cooling system, heat removal via the shutdown cooling system or maintenance cooling system or ECI) depending upon the needs of the accident.</p> <p>Should the accident result in the release of fission products from the heat transport system, the containment and confinement systems are capable of containing the fission products to the extent required to meet the regulatory limits. Post-accident offsite releases are controlled through the filtered air discharge system. Control of operational discharges is maintained well below allowable limits by means of the solid, liquid and gaseous waste management systems. As described in Part 2, Section 6.6 of the Safety Report, the Safety System Monitoring Computer system is used to monitor the state of the shutdown and ECI systems.</p> <p>As discussed in Part 2, Section 12.2 of the Safety Report, all systems considered to have significant radiological implications for station personnel during operation or maintenance were reviewed in the design phase. The review</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>process included a series of Man-Rem Audit meetings on a system-by-system basis. AECL design, operations, health physics, and physics and analysis groups were represented. Each system design was examined with respect to reliability, maintainability, ease of handling, ease of access, shielding, etc. Radiation exposure was estimated for each system in man-rem per year, and the estimate compared with budgeted exposure figures prepared earlier as targets. (All estimates were based on Douglas Point radiation exposure data as reported for 1970). Proposals to reduce radiation exposure by improving system design were analyzed and, wherever feasible, implemented.</p> <p>All of the systems needed to fulfil the safety functions following a PIE have been identified at Bruce B. At the time Bruce B was constructed these systems were identified based on experience in the design and construction of NPPs in Canada. Since that time Bruce Power has conducted PRAs that have clearly identified SSCs that have credited safety functions. The original list of systems created at the time of the design has been expanded as new trends and requirements in safety have been identified. All SSCs now required to fulfil the safety functions at Bruce B are listed in the Safety Related Systems list [BP-PROC-0169, R0002, September 28, 2007].</p> <p>An Assessment of Systems Important to Safety for the Safety &amp; Licensing Portion of the Nuclear Asset Management Program [B-REP-00701-21Oct2013-058] presents the various system groupings at Bruce Power that rank the importance of SSCs based on safety and production. These groupings can be used to establish the overall list of SSCs to be in scope of the Nuclear Safety &amp; Licensing portion of the</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>Nuclear Asset Management Program. As indicated in section 3.2 of B-REP-00701-21 Oct 2013-058, tables of Bruce A and Bruce B systems and their relative placement in the hierarchy of importance in the definition of the scope of the performance and condition monitoring program are included in BP-PROC-00781, "Performance Monitoring" [R003, September 11, 2015].</p> <p>As specified in BP-PROC-00169, to meet the objective of ensuring adequate public radiological safety, Bruce Power stations (Bruce A and B) contain a number of unique systems, structures, equipment and design features Safety Related Systems. These Safety Related Systems receive special emphasis (in varying degrees) during the commissioning and operating life of the station. This procedure lists and identifies the systems to which the quality assurance provisions of the Bruce Power Management System will formally be applied and on which monitoring and audit procedures may be carried out with more emphasis. Systems in the Safety Related System list will receive increased emphasis in the area of maintenance, testing, availability and qualifications requirements. This emphasis will be graduated depending on the classifications and the safety related functions within the listing. Use of this listing applies to all staff in the execution of design, commissioning and operating work.</p> <p>Bruce Power has established the Asset Life Projection and Options (ALPO) process described in BP PROC 00899 Asset Life Projections and Options and BP-PROC-00936 Asset Management Planning.</p> <p>The objective of BP-PROC-00899 is to provide an input to the Strategic Planning process and provide the required</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>options to manage the asset to 2043 and to define the process of developing and revising an ALPO document.</p> <p>An ALPO will achieve the following:</p> <ol style="list-style-type: none"> <li>1. Establish the projected end of life based on the current condition of the SSCs.</li> <li>1. Identify the Mitigation Options to reach component end of life based on the ARDMs (Age Related Degradation Mechanisms) and/or obsolescence issues.</li> <li>2. Identify the activities to maintain the asset and the health of the maintenance and surveillance program(s).</li> <li>3. Identify and provide recommended numbers and rationale to include the component or sub components as part of the Strategic Spares set.</li> </ol> <p>The objective of BP-PROC-00936 is to select and approve Asset Management options to achieve a resource leveled, integrated Asset Management Plan that will provide safe, reliable long term operation in alignment with corporate strategic and business planning objectives.</p> <p>In this context Bruce Power's strategy is to complete any required work in normal outages but where this is not possible, in special outages such that MCR will focus on replacement of the critical life limiting components, i.e. Fuel Channels, Feeders and Steam Generators and associated enabling work. Asset Management scope will be considered within the MCR outage window if the associated work requires significant field time (&gt;90 days), or a defueled / dewatered state or nominal case End of Life (EOL) falls in the Refurbishment outage window.</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
		Systems Important to Safety (SIS) Decision Methodology [DPT-RS-00012, R001, September 24, 2013] describes the methodology and process involved in determining which station systems are Systems Important to Safety. The original list of systems, needed to fulfill the safety functions following a postulated initiating event has been developed based on design and construction experience. The list created at the time of the design has been expanded later to reflect the results of PRAs.	
6.3	<p>The design shall apply the principles of defence in depth to minimize sensitivity to PIEs. Following a PIE, the plant is rendered safe by:</p> <ol style="list-style-type: none"> <li>1. inherent safety features</li> <li>2. passive safety features</li> <li>3. specified procedural actions</li> <li>4. action of control systems</li> <li>5. action of safety systems</li> <li>6. action of complementary design features</li> </ol>	<p>A new requirement for action of complementary design features (item 6) is added to this clause.</p> <p>As described in Part 2, Section 1.2.1 of the Safety Report, the CANDU reactor is a heavy water moderated, heavy water cooled, natural uranium fuelled reactor. Each pressure tube is isolated from the heavy water moderator by its calandria tube. This configuration separates the moderator system from the high-temperature, high-pressure coolant in the pressure tubes. Thus, the calandria operates at nearly atmospheric pressure. The use of natural uranium fuel, on-power refuelling, and a heavy water moderator leads to a design characterized by good neutron economy and low excess reactivity. Also, a lattice of natural uranium and light water cannot be made critical in any configuration. Hence, no criticality problem exists in the irradiated fuel bays of CANDU reactors. The prompt neutron lifetime in a heavy-water-moderated CANDU lattice is much longer (0.9 ms) than in a light-water-moderated reactor (section 1.2.4 of Part 2 of Bruce B Safety Report). In addition, the delayed neutron fraction is enhanced due to the presence of delayed photoneutrons (produced via dissociation of deuterium by high-energy gamma rays from fission products). On-power</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>fuelling results in a reactor with very low reactivity control requirements and very low excess reactivity capacity, i.e., the capacity to add additional reactivity is physically limited (section 1.2.5 of Part 2 of Bruce B Safety Report).</p> <p>As described in Part 2, Section 1.3.1 of the Safety Report, in designing to meet the principles and release limits set out in Part 1 of the Safety Report, it is important to recognize the redundant barriers to release of radioactive material that are built into the design of the fuel, the process systems and special safety provisions. The barriers which are in place to prevent radioactivity from escaping to the public environment include:</p> <ol style="list-style-type: none"> <li>1. The UO<sub>2</sub> fuel pellets, which bind the majority of radioactive fission products within the solid matrix.</li> <li>2. The fuel sheath, which contains fission products not retained in the fuel matrix.</li> <li>3. The heat transport system boundary, which contains any leakage from the fuel sheath.</li> <li>4. The containment building, which contains any release from the heat transport system.</li> <li>5. The exclusion zone surrounding the facility, which provides for dilution of any release from containment.</li> </ol> <p>The first three barriers prevent radioactive release accidents. As long as they are intact, very little radioactive material will escape into the reactor building. If it does, containment comes into play to mitigate doses.</p> <p>Automatic action of the Safety Systems (e.g., some also</p>	




Article No.	Clause Requirement	Assessment	Compliance Category
		<p>utilize gravity and pressure for activation) at Bruce B puts the plant into a safe state immediately following any AOO, DBA or BDBA. Long-term actions to ensure that the plant remains in the safe state are carried out through the procedures in the Bruce B Abnormal Incidents Manual [NK29-AIM-03600.1. Rev. 056].</p> <p>It is recognized that there are no complementary design features at Bruce B original design to respond to management of severe accidents. Bruce Power is addressing the need for additional complementary design features through evaluations and potential design improvements as part of Fukushima Action Items.</p> <p>However, SAMGs have been put in place to respond to management of severe accidents together with additional design improvements such as PARs. In preparing the SAMGs, all systems that are available have been used for the recovery, some of them under conditions not normally envisaged for those systems. Details of the application of defence in depth principles in the design are discussed as part of compliance with relevant aspects of CNSC REGDOC-2.5.2.</p>	
6.4	<p>Achievement of the general nuclear safety objective (discussed in section 4.1) depends on all actual and potential sources of radiation being identified, and on provision being made to ensure that sources are kept under strict technical and administrative control.</p> <p>Radiation doses to the public and to site</p>	<p>The change in this clause is the replacement of "BDBAs" with "DECs" and does not affect the requirement.</p> <p>As discussed in Clause 4.2.1, the DSA in the Safety Report does not distinguish between AOO and DBA and does not address BDBAs explicitly. DECs were not considered in the design basis; however, the design basis includes some event sequences that would be categorized as BDBAs. The limits for AOOs are currently taken to be the same as for DBAs (this is the same gap previously identified for Clause 4.2.1).</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>personnel shall be as low as reasonably achievable. During normal operation, including maintenance and decommissioning, doses shall be regulated by the limits prescribed in the Radiation Protection Regulations.</p> <p>The design shall include provisions for the prevention and mitigation of radiation exposures resulting from DBAs and DEC's.</p> <p>The design shall also ensure that potential radiation doses to the public from AOOs and DBAs do not exceed dose acceptance criteria provided in section 4.2.1. The calculated overall risk to the public shall meet the safety goals in section 4.2.2.</p> <p>Guidance</p> <p>A detailed radiation dose assessment should include estimated annual collective and individual effective and equivalent radiation doses to site personnel and members of the public for normal operation, potential radiation doses to the public for AOOs and DBAs, and potential releases into the environment for DEC's.</p>	<p>Since the DEC's and BDBAs are not explicitly addressed in the design, this is identified as a gap. (Gap)</p> <p>As presented in Section 12 of Part 2 of the Safety Report, a radiation protection program is in place in support of radiation protection objective. Limiting personnel exposure is achieved by incorporating protective features into the initial station design, by controlling access to areas with elevated radiation levels, and by excluding personnel who are approaching certain administrative dose limits from further exposure.</p> <p>Requirements are in place, which govern the use of Radiation Protection Protective Equipment, which protect personnel from internal radiation resulting from the uptake of airborne and surface contamination. Decontamination facilities are provided to restrict the spread of contamination. Dosimetry and personnel monitoring devices as well as radiation monitors and detection devices are used extensively to monitor the doses that staff members receive, and to ensure that these doses are within allowable limits (section 12.1 of Part of the Safety Report). The review of all systems considered to have significant radiological implications for station personnel during operation or maintenance were reviewed in the design phase. Proposals to reduce radiation exposure by improving system design were analyzed and, wherever feasible implemented. The personnel dose reduction program resulted in improved station design that contributed significantly to the reduction of both collective and individual dose expenditures (section 12.2 of Part 2 of Safety Report).</p> <p>The limitation of external and internal radiation exposures to plant personnel is accomplished by a combination of facilities incorporated into the station design and by adherence to a</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The assessment process should be clearly documented and should include the process for consideration and evaluation of dose-reduction changes in the NPP design. Radiation doses resulting from the operation of the NPP should be reduced by means of engineered controls and radiation protection measures to levels such that any further expenditure on design, construction and operational measures would not be warranted by the expected reduction in radiation doses.</p> <p>The radiation dose assessment should include the expected occupancy of the NPP's radiation areas, along with estimated annual person-Sievert doses associated with major functions, including radioactive waste handling, normal maintenance, special maintenance, refuelling and in-service inspection. Such assessments should include information as to how ALARA and operating experience are used in the design to deal with dose-significant contributors.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>• CNSC, G-129, rev. 1, Keeping Radiation Exposures and Doses "As Low as Reasonably</li> </ul>	<p>set of approved operating procedures and regulations.</p> <p>Exposure to radiation is limited by shielding and by control of access to areas of high activity or of possible contamination. In addition, protective clothing, air masks and decontamination facilities are available for use when required. Personnel monitoring and dosimetry facilities are provided to monitor individual exposures. Zoning separates areas of contamination, and work practices are designed to maximize contamination control at the source.</p> <p>Bruce Power is implementing design changes to improve severe accident response. For example Passive Autocatalytic Recombiners (PARs) have been installed in both Bruce A and Bruce B units to provide additional hydrogen mitigation capability [NK29-CORR-00531-12635, Bruce Power Progress Report No. 7 on CNSC Action Plan - Fukushima Action Items, August 7, 2015].</p> <p>Bruce A &amp; B PARs project was initiated to provide mitigation of the potential buildup of Hydrogen gas in the Reactor Vaults or other areas of Containment during a severe accident scenario since buildup of hydrogen in the containment system has the potential to cause an explosion, if not properly mitigated.</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Achievable (ALARA)", Ottawa, Canada, 2004.</p> <ul style="list-style-type: none"> <li>CSA Group, N288.2, Guidelines for Calculating Radiation Doses to the Public from a Release of Airborne Radioactive Material under Hypothetical Accident Conditions in Nuclear Reactors, Toronto, Canada.</li> </ul>		
6.5	<p>The design shall include adequate provision for an appropriate exclusion zone. The appropriateness of the exclusion zone shall be based on several factors, including:</p> <ol style="list-style-type: none"> <li>1. evacuation needs</li> <li>2. land usage needs</li> <li>3. security requirements</li> <li>4. environmental factors</li> </ol> <p>Guidance</p> <p>The exclusion zone for NPPs in Canada has been typically defined as 914 metres from the reactor building. Rather than prescribe a particular size for the exclusion zone, this regulatory document</p>	<p>There are no changes to the requirements in this clause.</p> <p>As presented in Section 1.1.5.1 of Part 1 of the Safety Report [NK29-SR-01320-00001, R005], the Bruce B section includes part of a 914 m (3,000 ft) exclusion zone extending from the Bruce B powerhouse structure to the northern part of Inverhuron Park, which is leased to Ontario Power Generation. The entire park is leased to the Ministry of Natural Resources for unrestricted use of the area outside of the exclusion zone. The exclusion zone also includes two portions of Lake Huron that are not part of the Bruce Power site. These portions are assumed controlled by the Province of Ontario. All occupancy and use of the area within the zone is controlled by Bruce Power through the Bruce Site Lease, including the Hydro One usage of the switchyard and the power corridors.</p> <p>Due to the sensitivity of information, security requirements are addressed elsewhere.</p> <p>The Canadian Nuclear Safety Commission (CNSC) sets the radiation dose limits for members of the public for releases of radionuclides from nuclear facilities. The limits are provided in the Radiation Protection Regulations. The dose limits apply to the sum of the doses received from all exposure pathways, e.g., airborne, liquid, direct radiation exposure. At present,</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>specifies factors that must be considered in establishing an appropriate size, including evacuation needs, land usage needs, security requirements and environmental factors.</p> <p>Evacuation needs</p> <p>The design should take into account emergency response requirements based on the size of the exclusion zone and the facilities and infrastructures that are within the zone.</p> <p>The exclusion zone boundary should be defined with consideration for the capabilities of onsite and offsite emergency response. Environmental factors which can affect the response times should be taken into consideration. The design also considers projected changes over time in land use and population density, which could adversely affect response times, or the ability to shelter or evacuate persons from both the site itself and associated emergency planning regions.</p> <p>Evacuation needs are generally based on existing provincial nuclear emergency response plans.</p> <p>Land usage needs</p>	<p>the dose limits given in Table 1-2, section 1.4.1 of Part 1 of the Safety Report are in effect. The Dose Limits and Exposure Control procedure [BP-RPP-00009, R009, May 7, 2014] specifies that requirements at Bruce Power facilities to ensure the doses to the individuals do not exceed regulatory limits as required by BP-RPP-00044 ALARA Program.</p> <p>The detailed guidance provided in this clause is relevant to new build reactors. The guidance section includes specific information that is useful for the designers.</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design should ensure that the exclusion zone is large enough to accommodate the site for the nuclear plant (accounting for the full number of units postulated to be built at the site, whether or not they would be built immediately).</p> <p>The design activities should seek to optimize land usage by the plant as part of determining the exclusion zone.</p> <p>Security requirements</p> <p>The design should provide security requirements based on the size of the exclusion zone, the facilities and infrastructures that are within the zone, and the design of the facility. Generally, a larger exclusion zone would require more security capabilities, in order to avoid a longer response time. Physical characteristics of the site itself (which include geographical characteristics, such as proximity to elevated land) also play a role in determining these requirements.</p> <p>The design authority may decide to mitigate these risks while maintaining a smaller exclusion zone, by choosing highly robust facility designs, applying engineered security measures to the site,</p>		



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>and having a well-designed security program. These engineered measures should be described.</p> <p>In establishing the radius of the exclusion zone boundary, the design should take into account:</p> <ul style="list-style-type: none"> <li>the site selection and threat assessment report</li> <li>facility robustness against natural and human induced external hazards (including malevolent acts)</li> <li>the capability of the onsite security program, along with any offsite security resources that will supplement the onsite security program</li> </ul> <p>In each of the above parameters, the design should take into account projected changes over time in land use and population density, which could adversely affect that parameter. The design should be such that the exclusion zone, as established at the design stage, will be sustainable for the full lifecycle of the facility.</p> <p>The acceptability of the information to be provided in support of the above is discussed in section 7.22 of this document.</p>		


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Environmental factors</p> <p>Environmental factors which may have an impact on the size of the exclusion zone include local meteorological conditions which could affect the radiological dose received by members of the public. The design authority may use generic site data using conservative assumptions regarding meteorological conditions in the absence of a specific site.</p> <p>The Radiation Protection Regulations establish an effective dose limit of 1 mSv per year for members of the public. This limit implies that a hypothetical member of the public who lives at the exclusion zone boundary for 1 year (since no permanent dwelling is permitted within the exclusion zone) would not accumulate a dose of more than 1 mSv from normal operation of the NPP.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>• CNSC, RD-346, Site Evaluation for New</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	Nuclear Power Plants, Ottawa, Canada, 2008.		
6.6	<p>The facility layout shall take into account PIEs to enhance protection of SSCs important to safety. The design shall take into account the interfaces between the safety, security and safeguards provisions of the NPP and other aspects of the facility layout, such as:</p> <ol style="list-style-type: none"> <li>1. access routes for normal operational actions and maintenance</li> <li>2. access control to minimize radiation exposures</li> <li>3. actions taken in response to internal or external events</li> <li>4. egress routes</li> <li>5. movement of hazardous substances, nuclear materials, and radioactive materials</li> <li>6. movement of authorized and unauthorized personnel</li> </ol>	<p>New requirements for facility layout taking into account PIEs to enhance protection of SSCs and safeguards provisions in the design are introduced in this clause.</p> <p>The original Bruce B design includes some considerations of hazards; however as discussed later in Clause 9.3 it is recognized that the list is not complete. As presented in Section 3.1 of Part 2 of the Safety Report [NK29-SR-01320-00001, R005] the station is based on a four unit layout with central services, control centres, and administrative offices in a common power house. All units are as similar to each other as possible. Each unit consists of a single reactor housed in reinforced concrete vault. (The vault is the part of the reactor building that directly encloses the reactor). The steam generators protrude from the vaults into shielded rooms in the accessible area above the vaults. Each reactor supplies a single turbine generator housed in an adjacent turbine hall.</p> <p>Before the station was constructed, consideration was given to a number of possible arrangements of reactor, steam generator, and turbine generator. The arrangement that was finally selected is shown in Part 1 of the Safety Report, Figure 1-1. It has the station located close to the lake, with the vacuum building west (geodetic) of the nuclear part of the station, and the switchyard east of the conventional part. With this arrangement, the cooling water intake and discharge channels were relatively short, and the channels posed only a minimal impediment to construction traffic.</p> <p>The reactor buildings at older nuclear stations house a large number of systems and components that could be safely located outside the containment area. The buildings are</p>	IC

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>7. interaction of building and support functions</p> <p>It is likely that some design requirements associated with these factors will conflict with others in the determination of facility layout requirements. The design, therefore, shall reflect an assessment of options, demonstrating that an optimized configuration has been sought for the facility layout.</p>	<p>partly accessible during operation and have many shielded or separated areas with different ventilation and access requirements, and consequently differential loads due to postulated accidents. The approach at Bruce A and B was to simplify the design, even if this would exclude access to certain components during reactor operation, and increase the number of penetration through the containment envelope.</p> <p>The requirement for facility layout to take into account PIEs to enhance protection of SSCs important to safety is applicable to new build reactors.</p>	
6.6.1	<p>The design shall take due account of challenges to multiple units at a site. Specifically, the risk associated with common-cause events affecting more than one unit at a time shall be considered.</p> <p>Guidance</p> <p>The presence of multiple units at a site, or common-cause events could exacerbate challenges that the plant personnel would face during an accident. The events and consequences of an accident at one unit may affect the accident progression or hamper accident management activities at the neighbouring unit; available resources (personnel, equipment and consumable resources) would need to be shared among several units. These challenges should be identified and the available</p>	<p>This is a new section / requirement. In recognition that SAMG also needs to address multi-unit events involving a station blackout.</p> <p>Bruce Power expanded the scope of the SAMG to implement improvements proposed in COG JP-4426 and to include multi-unit IFB events in response to Fukushima lessons learned. The implementation of SAMG for multi-unit event is being undertaken in two parts as follows:</p> <ol style="list-style-type: none"> <li>1. first, the update of the Technical Basis Document (TBD) and the revision of the generic SAMG documentation, including multi-unit events will be developed by the Severe Accident Support Team under COG JP-4426. The report documenting the completion of the updated TBD and SAMG documentation is completed.</li> <li>2. Secondly, the station-specific SAMG documentation for multi-unit events and low power are prepared by Bruce Power.</li> </ol> <p>As reported in the Bruce Power Progress Report No. 7 on</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	resources and mitigation strategies shown to be adequate.	<p>CNSC Action Plan - Fukushima Action Items [NK29-CORR-00531-12635] the SAMG to address multi-unit events and irradiated bay events have been completed as described in Attachment B to [NK29-CORR-00531-12635]. Updates to the Bruce Power station specific SAMG for multi-unit events included changes to the station-specific SAMG documentation essentially as recommended by the COG topical report, COG-JP-4426-005-RO, "Multi-Unit Events Update of SAMG and Technical Basis Documents". The development of a parallel multi-unit severe accident modelling capability (FAI 3.2.1 and 3.2.2), being tracked under AI 1307-3703, has also been completed and site specific implementation and testing has been conducted for Darlington station. The results of the work indicate that the scaling and injection methods used previously to approximate multi-unit accidents in the single-unit MAAP4-CANDU models agree with the newly developed multi-unit model. The predictions from these two approaches are sufficiently well aligned such that further development of multi-unit models for Bruce A and Bruce B is not warranted. In the area of enhancing emergency response, Bruce Power is in the process of upgrading its Emergency Response Projection (ERP) code to allow multi-unit dose projection modeling capability under AI 1307-3790. Common-cause events are not analyzed explicitly in Part 3 of the Safety Report; therefore this is assessed as a gap (Gap). This gap is being prioritized to be considered early within Safety Report update towards the compliance with CNSC REGDOC-2.4.1.</p> <p>Bruce Power has completed the analysis and assessment activities to evaluate options for ensuring containment integrity and filtered venting in the event of a multi-unit severe accident. The report summarizes the results of assessments,</p>	

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>undertaken after the Fukushima-Daiichi event, to evaluate options for ensuring containment integrity and limiting fission product releases following an Extended Loss of AC Power (ELAP) event at Bruce A or Bruce B. The study considers the effectiveness of existing design features such as the deaerator storage tank and ECI soft injection, enhanced safety features (such as Emergency Moderator Makeup) that have either been installed or are being installed as part of Bruce Power's post-Fukushima response, and the addition of a new, passive Containment Filtered Venting System. The final report, provided in Enclosure 1 to Bruce Power Progress Report No. 6 on CNSC Action Plan - Fukushima Action Items [NK29-CORR-00531-12195], concludes that existing design capability and emergency mitigation measures aimed at preventing severe core damage represent a viable alternative to the installation of a filter vent system dedicated to management of containment pressure during severe accidents. Based on the conclusions of the report, which indicate that existing means to protect containment integrity and uncontrolled releases are adequate, Bruce Power requested closure of FAI 1.3.2. CNSC staff agreed that the closure criteria had been met as indicated in [NK29-CORR-00531-12979, February 4, 2016].</p> <p>Bruce Power Nuclear Emergency Response Plan [BP-PLAN-00001, R005, December 02, 2014] is developed to describe the concepts, structures, roles, and processes needed to implement and maintain Bruce Power's capability to prepare for and to respond to a nuclear radiological emergency. This Plan outlines the command, control, and coordination structure and activities, activation, site integration, external agency coordination, deployment of emergency resources, and emergency facilities through the use Emergency</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
		Response Procedures developed to guide effectively trained emergency response staff in emergency response and mitigation techniques.	
7.1	<p>The design authority shall classify SSCs using a consistent and clearly defined classification method. The SSCs shall then be designed, constructed, and maintained such that their quality and reliability is commensurate with this classification.</p> <p>In addition, all SSCs shall be identified as either important or not important to safety. The criterion for determining safety importance is based on:</p> <ol style="list-style-type: none"> <li>1. safety function(s) to be performed</li> <li>2. consequence(s) of failure</li> <li>3. probability that the SSC will be called upon to perform the safety function</li> <li>4. the time following a PIE at which the SSC will be called upon to operate, and the expected duration of that operation</li> </ol>	<p>The changes in this clause are editorial in nature and do no impact the requirements.</p> <p>Bruce Power employs a number of equipment lists to serve specific purposes related to safety. Most important and comprehensive of these is the Safety Related System List. The Safety-Related System List procedure [BP-PROC-00169, R002, September 28, 2007] presents the systems classified as important to safety. The safety related systems are divided into groups A to G and are listed in Appendix B. If only certain parts of a system have a safety related function, the system is classified as safety related. These systems receive increased emphasis in the area of maintenance, testing, availability and qualification requirements. This emphasis is graduated depending on the classifications and the safety related functions within the listing. The list is developed using all applicable design documentation and safety analyses. The list of safety related system systems specifies the USI, the system name, the applicable safety related group, and the safety related system function. The methodology and process to determine which station systems are important to safety are documented in Systems Important to Safety (SIS) Decision Methodology [DPT-RS-00012, R001, September 24, 2013]. This process utilizes the site Probabilistic Risk Assessments (PRAs) and identifies Systems Important to Safety as required by S-98, Reliability Programs for Nuclear Power Plants.</p> <p>Bruce B continued the basic design of the Bruce A station</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>SSCs important to safety shall include:</p> <ol style="list-style-type: none"> <li>1. safety systems</li> <li>2. complementary design features</li> <li>3. safety support systems</li> <li>4. other SSCs whose failure may lead to safety concerns (e.g., process and control systems)</li> </ol> <p>Appropriately designed interfaces shall be provided between SSCs of different classes in order to minimize the risk of having SSCs less important to safety adversely affecting the function or reliability of SSCs of greater importance.</p> <p>Guidance</p> <p>The method for classifying the safety significance of SSCs important to safety should be based primarily on deterministic methodologies, complemented (where appropriate) by probabilistic methods and engineering judgment. The safety classification of SSCs should be an</p>	<p>(see Section 1.3.2, of Part 1 of the Safety Report [NK29-SR-01320-00001, R005]). It is noted that the Bruce A (and B) systems have never been formally classified in a ranking system as suggested by this clause. There are no systems specifically designed to mitigate severe accidents. However, the defence in depth general principle has been applied to the design of all CANDU reactors, in that the various levels of defence-in-depth are independent of each other to the greatest extent practicable.</p> <p>For example, level 1 defence-in-depth systems, i.e., process systems, are designed so that any failure in the system is not propagated to the control systems that control these processes. Similarly a failure in a control system does not propagate to the next level of defence-in-depth, i.e., the safety systems. This is done through adequate separation of the control systems for the safety systems; internationally this is achieved by ensuring adequate buffering of any components shared between the control and safety systems so that the failure cannot be propagated, in Canada, it has been done to date through complete separation of the control and safety systems. As part of this defence-in-depth, pressure retaining components in any safety system are required to meet the highest design standards. The fourth level of defence-in-depth makes use of many systems that are not credited in safety analysis. They are used to mitigate the consequences of a BDBA or a Severe Accident. Such accidents have a very low frequency and usually occur because safety systems have not been able to perform their function, either through multiple component failures within those systems or through loss of common services. They are generally backup process systems and as such would have been designed such that their failure would in no way affect</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>iterative process that continues throughout the design process.</p> <p>The SSC classification process should include the following activities:</p> <ul style="list-style-type: none"> <li>• review and definition of PIEs</li> <li>• grouping and identification of bounding PIEs</li> <li>• identification of plant-specific safety functions to prevent or mitigate the PIEs</li> <li>• safety categorization of the safety functions, in accordance with their safety significance and role in achieving fundamental safety functions</li> <li>• identification of SSCs that provide the safety functions</li> <li>• assignment of SSCs to a safety class corresponding to the safety category</li> <li>• verification of SSC classification</li> <li>• identification of engineering design rules for classified SSCs</li> </ul> <p>This approach should be used for all SSCs including pressure retaining components, electrical, instrumentation and control (I&amp;C) and</p>	<p>the control or safety systems.</p> <p>Bruce Power performed an Assessment of Systems Important to Safety for the Safety &amp; Licensing Portion of the Nuclear Asset Management Program [B-REP-00701-21OCT2013-058] that documented the various system groupings at Bruce Power that rank the importance of SSCs based on safety and production. These groupings can be used to establish the overall list of SSCs to be in scope of the Nuclear Safety &amp; Licensing portion of the Nuclear Asset Management Program. It is noted that the requirements and guidance for classification of SSCs important to safety as defined in this clause are applicable to new reactor facilities.</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>civil structures.</p> <p>The identified PIEs should be grouped into limiting cases, which are referred to as bounding or enveloping PIEs. Once these bounding PIEs are known and understood, the required safety functions can be identified. The number of categories and classes may be chosen to allow for graded design rules.</p> <p>The time following the PIE captures the need for automatic action for short timescales, or manual actions being acceptable for longer-term actions. The expected duration of the operation is also important since some systems may need to operate for months. Others (such as shutdown means) can complete their mission within seconds.</p> <p>The potential severity of the consequences of a function failure should be evaluated. The severity should be based on the consequences that could arise if the function was not performed. The consequences of a function failure should be made assuming that the safety functions belonging to the subsequent level of defence in depth remain functional.</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Some specific SSCs classification guidelines are given below:</p> <ul style="list-style-type: none"> <li>SSCs whose failure cannot be accepted because the failure will result in unacceptable consequences with certainty should be allocated to the highest safety class.</li> <li>Supporting SSCs that are essential to achieve the safety function of the frontline SSCs to be supported should be assigned to the same class as that of the frontline SSCs.</li> <li>An SSC that contributes to the performance of several safety functions of different categories should be assigned to the class corresponding to the highest category of those safety functions requiring the commensurate design rules.</li> <li>Any SSC that is not part of a safety function group, but whose failure could adversely affect this safety function group in accomplishing its safety function (if this cannot be precluded by design) should be classified in accordance with the safety category of that safety function group.</li> <li>Where the safety class of connecting or interacting SSCs is not the same (including cases where one SSC belonging to a safety class is connected to another SSC not important to safety), the interference between the SSCs should be separated by a device (e.g., a physical or</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>optical isolator) classified in the higher safety class. This is to ensure that the failure of a lower safety class SSC will not propagate to an SSC belonging to a higher safety class.</p> <p>The adequacy of the safety classification should be verified using deterministic safety analysis, which should cover all PIEs and all the credited safety functions. This verification should be complemented, as appropriate, by insight from probabilistic safety assessment and by engineering judgment.</p> <p>The appropriate design rules and limits as indicated in section 7.5 are specified in accordance with the safety class of SSCs.</p> <p>Although the probability of SSCs being called upon during DEC's is very low, the failure of safety functions for the mitigation of DEC's may lead to consequences with high severity. SSCs that provide these safety functions should be assigned a safety category commensurate with the safety significance. For certain complementary design features (such as onsite portable equipment) with high redundancy and extremely low probability of being called upon, a low safety class may be appropriate. It should be noted that not all portable equipment is included in SSCs important</p>		




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>to safety.</p> <p>Firstly, SSCs are identified as important or not important to safety. By virtue of their roles, safety systems, complementary design features and safety support systems will be identified as important to safety. Additionally, other SSCs that can have a significant impact on nuclear safety will also be identified as important to safety.</p> <p>After the SSCs important to safety are identified, they are classified. The safety classification considers a number of factors as listed above. The safety classification enables appropriate design rules to be selected as described in section 7.5</p>		
7.2	<p>The design authority shall establish the plant design envelope, which comprises all plant states considered in the design: normal operation, AOOs, DBAs and DECAs, as shown in figure 1.</p> <p>Figure 1: Plant states</p> <p>The design basis shall specify the capabilities that are necessary for the plant in operational states and DBAs.</p>	<p>The requirement is changed to include DECAs.</p> <p>The original design envelope and design basis was documented in the system design manuals and in the Safety Reports, along with important assumptions which included capabilities that are necessary for the plant in operational states, SSC failure modes, event progression leading to accident conditions and methods of analyses, submitted in the application for the original operating licence. Similarly, the basis for each modification, assumptions and methods of analysis since that time were documented.</p> <p>The Plant Design Basis Management Program [BP-PROG-10.01, R009, December 04, 2014] ensures that the plant</p>	IC


 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Conservative design measures and sound engineering practices shall be applied in the design basis for operational states and DBAs. This will provide a high degree of assurance that no significant damage will occur to the reactor core, and that radiation doses will remain within established limits.</p> <p>Complementary design features address the performance of the plant in DEC's.</p> <p>Guidance</p> <p>The design basis for each SSC important to safety should be systematically defined and justified. The design should also provide the necessary information for the operating organization to run the plant safely.</p> <p>The design should adopt deterministic design principles of appropriate conservatism. For example, SSCs should be robust, tolerant of a large spectrum of faults with a gradual degradation in their effectiveness, and should not fail catastrophically under operational states, DBAs and DEC's.</p>	<p>design meets safety, reliability and regulatory requirements, including pressure boundary quality assurance requirements as defined in Pressure Boundary Quality Assurance Program [BP-PROG-00.04, R022, May 27, 2015]</p> <p>As discussed before, there are no systems at Bruce Power that were specifically designed for severe accidents. As a result of Fukushima Related Action Items, Bruce Power initiated design and programmatic evaluation and subsequent changes to improve plants severe accident response. Design modifications and alternative means are being incorporated based on the results of extensive reviews and assessments of the effectiveness of existing design provisions for severe accidents. For example, the results of Level 2 PRA analysis showed that containment integrity can be challenged during a multi-unit severe accident, particularly if no mitigating measures are available or are credited. Options for enhancing the ability of containment to accommodate severe accidents in multiple units were investigated. The analysis involves numerous multi-unit event combinations with various credits for mitigating actions and systems.</p> <p>In the area of strengthening defence-in-depth, Bruce Power is progressing the engineering of additional safely features to provide makeup water to the calandria, heat transport system and shield tank and to provide overpressure protection to the shield tank. These modifications are intended to provide further defence-in-depth against a severe accident and to support the Severe Accident Management Guidelines (SAMG) by mitigating severe accident progression and protecting containment integrity. The progress on implementing the modifications, being tracked under AI 2014-07-3688, is described in Attachment B to Bruce Power</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The conditions for deviating from conservative and deterministic design principles should be clearly stated, including the basis by which such deviation would be justified on a case-by-case basis; such basis may include a more sophisticated calculation methodology that has been well established, or a multiplicity of ways in which a particular function can be fulfilled.</p> <p>A complementary design feature is a design feature added to the design as a stand-alone SSC (including portable equipment), or added capability to an existing SSC to cope with DEC.</p> <p>The design principles for complementary design features to deal with DEC do not necessarily need to incorporate the same degree of conservatism as those applied to the design up to and including DBAs. However, the design authority should provide reasonable assurance that the complementary design features will function as designed when called upon.</p>	<p>Progress Report No. 8 on CSNC Fukushima Action Plan [NK29-CORR-00531-12979]. Bruce Power's assessment activities to evaluate options for ensuring containment integrity and filtered venting in the event of a multi-unit severe accident. In this assessment, Bruce Power concluded that existing design capability and emergency mitigation measures aimed at preventing severe core damage represent a viable alternative to the installation of a filter vent system. Bruce Power has made significant progress on the Fukushima action plan, resulting in the closure of the 70 FAls applicable to Bruce Power. Bruce Power has also made significant progress in completing field installation of enhanced safety features to strengthen defence-in-depth for beyond design basis accidents as well as completing station specific assessments. The majority of activities to further enhance emergency response capabilities are complete. Bruce Power is implementing design changes to improve severe accident response. For example Passive Autocatalytic Recombiners (PARs) have been installed in both Bruce A and Bruce B units to provide additional hydrogen mitigation capability [NK29-CORR-00531-12635, Bruce Power Progress Report No. 7 on CNSC Action Plan - Fukushima Action Items, August 7, 2015]. Bruce A &amp; B PARs project was initiated to provide mitigation of the potential buildup of Hydrogen gas in the Reactor Vaults or other areas of Containment during a severe accident scenario since buildup of hydrogen in the containment system has the potential to cause an explosion, if not properly mitigated.</p> <p>Short-term activities at Bruce Power have focused on the design and installation of modifications that would allow emergency makeup water to be added to the steam generators and the IFBs using EME equipment (fire pumper</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>trucks). Together with the procurement of EME, these plant modifications were deliberately given the highest priority following the Fukushima event because they provide the overall greatest benefit to safety in the least amount of time. As reported in [NK29-CORR-00531-11349] Bruce Power has completed all short term modifications to emergency water to be added to the steam generators and IFBs using EME pumps.</p> <p>Seven 100 kW, 600 VAC generators (including one spare) have been purchased to provide power to Bruce B in the event of a blackout. The generators will be removed from storage and deployed outside the powerhouse in the event of a total blackout and will supply selected Emergency Power Supply (EPS) loads through Motor Control Centres (MCCs). The generator and feeder cables have quick disconnects compatible with receptacle inside the plant for 5/6/7/8 SCA rooms, and the EFADS and EWPS buildings. The existing receptacle safety switch fuses will be replaced with larger size. The portable generators will have 120/240 V local receptacles to plug lighting cords for the deployment of hoses and cables during total blackout. The portable generator will also have flood lights mounted on the enclosure for operation and maintenance. The Emergency Electrical Power Upgrades for Bruce B are described in Attachment 2 of Bruce Power Progress Report No. 1 on CNSC Action Plan - Fukushima Action Items [NK29-CORR-00531-10193].</p>	
7.3	<p>Plant states considered in the design shall be grouped into the following four categories:</p> <p>1. Normal operation is an operation within</p>	<p>The requirements in this clause are modified with the introduction of the DEC's as defined in item 4.</p> <p>Bruce B continued the basic design of the Bruce A station (see Section 1.3.2, of Part 1 of the Safety Report [NK29-SR-</p>	Gap

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>specified OLCs, including start-up, power operation, shutting down, shutdown, maintenance, testing, and refuelling.</p> <p>2. An anticipated operational occurrence (AOO) is a deviation from normal operation that is expected to occur once or several times during the operating lifetime of the NPP but which, in view of the appropriate design provisions, does not cause any significant damage to items important to safety, or lead to accident conditions.</p> <p>3. Design-basis accidents (DBAs) are accident conditions for which an NPP is designed according to established design criteria, and for which damage to the fuel and the release of radioactive material are kept within regulated limits.</p> <p>4. Design extension conditions (DECs) are a subset of beyond-design-basis accidents that are considered in the design process of the facility in accordance with best-estimate methodology to keep releases of radioactive material within acceptable limits. Design extension conditions could include severe accidents.</p> <p>Acceptance criteria shall be assigned to each</p>	<p>01320-00001, R005]). Historically, the basis on which Bruce A and B were originally licensed was the grouping of accidents into two categories: process system failures (single failures) and process system failures in conjunction with the failure of a special safety system (dual failures). The acceptance criteria for each category recognize the different probabilities of these accident groups and allow higher release for the lower probability events. Using the definitions above, what are now generally referred to as transients, are called AOOs. The stepback functions provide coverage for a variety of transients such as PHT pump trip, steam generator low level, high heat transport pressure, high zone power, high neutronic power rate, calandria inlet high temperature, turbine trip loss of line or stator cooling. As part of the plant equipment protective function, automatic power reductions can be initiated via the setback or stepback functions, which are implemented in the dual, digital control computers. For many loss of control events, setback or stepback provide effective mitigating action; however such action is not credited in the analysis. A complete listing of both the setback and stepback parameters is given in Table 3-3 and Table 3-5 of Appendix 3 Control Failures of Part 3 of the Safety Report. These transients generally have a frequency higher than 1E-2/a. As noted before the AOOs are not explicitly covered in the existing design documentation; therefore this is assessed as a gap (Gap). This gap is being addressed by Bruce Power with the implementation of the Safety Report Improvement Program starting in 2014 including annual status and progress updates to the CNSC staff. Further details are provided in Bruce Power letter from F. Saunders to R. Lojk, Action Item 090739: Safety Report Improvement Plan for Bruce A and Bruce B, dated November 20, 2013, File: NK21-CORR-00531-10774 &amp; NK21-CORR-</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>plant state considered in the design, taking into account the principle that frequent PIEs will have only minor or no radiological consequences, and that any events that may result in severe consequences will be of extremely low probability.</p> <p>Guidance</p> <p>Plant states considered in the design are divided into normal operation, AOOs, DBAs and DEC. The design requirements of SSCs should then be developed to ensure that the plant is capable of meeting applicable deterministic and probabilistic requirements for each plant state. Note that the plant states diagram in section 7.2 identifies BDBA as a plant state. However, only a subset of BDBAs is considered in the design. These are DEC.</p> <p>The design should include the following:</p> <ul style="list-style-type: none"> <li>criteria for transition to normal operation following an AOO or DBA (e.g., the safety functions are provided, and the OLC limits for the operating configurations are met)</li> <li>key parameters and characteristics for operational states, including nominal values and</li> </ul>	<p>00531-11155.</p> <p>The definition of DBAs given in this clause is essentially the same as the single failures in the current licensing basis accidents used in the licensing of Bruce B. The one exception to that rule is the DBA used to verify the acceptability of the containment design leakage rate. This is a dual failure event in current design documentation.</p> <p>BDBAs include the dual failure events involving a process system failure and failure of any one safety system at a time. Definition in Clause 7.3 would include other multiple failure events involving safety support systems that may not have been explicitly considered in the Safety Report using deterministic methods of analyses. They have however been considered in the PRA for the plant and the risk from all of the accidents has been shown to be acceptable. Severe accidents have not been considered in the original design of the plant but are now being dealt with through the COG SAMG program. Bruce Power has committed to upgrade Safety Report and associated Safety analysis in compliance with CSA N286.7-99 and to address BDBA in deterministic safety analysis. This gap is being addressed by the CNSC Action Item 090739: Safety Report Improvement Plan for Bruce A and Bruce B.</p> <p>A summary of the acceptance criteria applied to Bruce Power accident analysis is provided in Section 1.5 of Part 3 of the Safety Report [NK29-SR-01320-00002, R005]. However, the current requirements deal only with the single process system failures (DBAs in the terminology of this report) and the dual failure limits, which would be considered as BDBAs/DECs in CNSC REGDOC-2.5.2.</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>deviations due to uncertainties and settings of instruments, controls, trips, equipment action time, or due to process fluctuations</p> <ul style="list-style-type: none"> <li>permissible conditions for different operating configurations (e.g., cold and pressurized) including transient time (e.g., power level of reactor or turbine, normal planned power transient rate, heat-up and cool-down rates) for the NPP's operating life</li> <li>methods of transferring the plant between different operating configurations</li> <li>final safe configurations after AOOs, DBAs, and DECAs</li> </ul>		
7.3.1	<p>The design shall facilitate the safe operation of the plant within a defined range of parameters, with an assumed availability of a minimum set of specified support features for safety systems.</p> <p>The design shall minimize the unavailability of safety systems. The design shall address the potential for accidents to occur when the availability of safety systems may be reduced, such as during shutdown, start-up, low power operation, refuelling and maintenance.</p> <p>The design shall establish a set of requirements and limitations for safe normal operation,</p>	<p>There are no changes to the requirement.</p> <p>Any analysis or at least a summary of that analysis, provided to demonstrate that the plant can operate within its defined operating parameters would be included in the design manuals for the various systems. The minimum specified support features for safety systems are identified in the OSRs and in the Bruce B Abnormal Incidents Manual [NK29-AIM-03600.1, Rev.056]. These would be available for both normal and accident conditions. Additionally there are many backup process systems available for normal operation (e.g., auxiliary boiler feedwater) that would not be credited under accident conditions.</p> <p>As discussed previously, as part of the ongoing Safety Report Improvement Program, Bruce Power is updating safety analysis to align with the REGDOC-2.4.1</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>including:</p> <ol style="list-style-type: none"> <li>limits important to safety</li> <li>constraints on control systems and procedures</li> <li>plant maintenance, testing, and inspection requirements to ensure that SSCs function as intended, taking the ALARA principle into consideration</li> <li>clearly defined operating configurations, such as start-up, power production, shutdown, maintenance, testing, surveillance, and refuelling – these configurations shall include relevant operational restrictions in the event of safety system and safety support system outages</li> </ol> <p>These requirements and limitations, together with the results of safety analysis, shall form the basis for establishing the OLCs according to which the plant will be authorized to operate, as discussed in section 4.3.3 of this document.</p> <p>Guidance</p>	<p>requirements.</p> <p>Operating limits, including those for Normal Operation, are specified in the OP&amp;P [BP-OPP-00001, R019]. Further discussion regarding Safe Operating Envelope is presented in Clause 4.3.3.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design ensures that normal operations are carried out safely, thereby ensuring that radiation doses to workers and members of the public, as well as any planned discharges and releases of radioactive material from the plant, will be within the prescribed limits specified in the Radiation Protection Regulations, and will meet the requirements of section 4.1.1 of this regulatory document.</p> <p>Operating configurations for normal operation are addressed by the OLCs which are described in section 4.3.3. These typically include:</p> <ul style="list-style-type: none"> <li>• normal reactor start-up (from shutdown, through criticality, to full power)</li> <li>• power operation, including full-power and low-power operation</li> <li>• changes in reactor power, including load-follow modes (if applicable) and return to full-power after an extended period at low-power</li> <li>• operation during transition between configurations such as reactor shutdown from power operation (hot shutdown, cool-down)</li> <li>• refuelling during normal operation, where applicable</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>shutdown in a refuelling mode or other maintenance condition that opens the reactor coolant or containment boundary</li> <li>handling of fresh and irradiated fuel</li> </ul> <p>The key parameters and unique characteristics of each operational configuration, including the specific design provision for maintaining the configuration, should be identified. The permissible periods of operation at different configurations (e.g., power level) in the event of a deviation from normal operating configurations, should also be identified.</p>		
7.3.2	<p>The design shall include provisions such that releases to the public following an AOO do not exceed the dose acceptance criterion provided in section 4.2.1.</p> <p>The design shall also provide that, to the extent practicable, SSCs not involved in the initiation of an AOO shall remain operable following the AOO.</p> <p>The response of the plant to a wide range of AOOs shall allow safe operation or shutdown, if necessary, without the need to invoke provisions beyond Level 1 defence in depth or, at most, Level 2.</p>	<p>There are no changes to the requirement</p> <p>A review of the same clause in RD-337 [NK21-CORR-00531-11005 / NK29-CORR-00531-11397] indicated that the Bruce A and Bruce B designs do not fully meet this requirement. The licensing basis does not specify separate acceptance criteria for AOOs. The deterministic safety analysis provided in the Bruce B Safety Report [NK29-SR-01320-00002] does not distinguish between classes of events. Although AOOs have not been explicitly addressed in the analysis, they have been shown to meet the current single failure limit, as required.</p> <p>The requirement for the reactor to be able to continue operation after an AOO basically means that there should be no fuel failure following the event. For several of the AOO cases at Bruce B, this would be the case, e.g., loss of control system functions. For some of the other scenarios, e.g., PHT</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The facility layout shall be such that equipment is placed at the most suitable location to ensure its immediate availability when operator intervention is required, allowing for safe and timely access during an AOO.</p> <p>Guidance</p> <p>The guidance in this subsection also covers elements common to AOO and DBA.</p> <p>In accordance with the requirements of section 4.3.1 of this regulatory document for Level 2 and Level 3 defence in depth, the design should include the results of the analyses of AOOs and DBAs in order to provide a demonstration of the robustness of the fault tolerance in the engineering design and the effectiveness of the safety systems. The analysis should cover the full range of events over the full range of reactor power. The analysis should also cover all normal operating configurations, including low-power and shutdown states.</p> <p>For a wide range of AOOs, the design should be such that any deviations from normal operation can be detected, and that the control systems can be expected to return the plant to a safe state,</p>	<p>pump seal failure, the public doses arise from incipient iodine in the HT system and from tritium in the D2O (section 3.2.2.9.1 of Part 3 of the Safety Report). Thus, repair of the seal would enable the reactor to continue operation. The doses from this event, as calculated in the Bruce B Safety Report using very conservative assumptions are within the currently allowable single failure criterion, but would be outside the AOO limit proposed in Clause 4.2.1 of CNSC REGDOC 2.5.2. Therefore, this is assessed as a gap. (Gap)</p> <p>The most limiting AOO cases in regard to both pressure and fuel integrity, are loss of power scenarios and these are described in Appendix 2 Electrical System Failures of Part 3 of the Safety Report. Section 2.10 of that Appendix, discusses specifically the effect of control systems on the results of those analyses. Total and partial loss of Class IV power failures, and single pump seizure events, have been analyzed over the entire range of plant operating conditions. The results indicate that, in virtually all cases in which dryout can potentially occur, there are a least two diverse trip parameters on each of SDS1 and SDS2 which protect against fuel overheating. These trips occur either prior to or shortly after the onset of fuel sheath dryout in every case. Since the period of potential post-dryout operation is short, fuel and sheath temperature increases are not sufficient to challenge the integrity of the heat transport system due to fuel overheating, and in addition, fuel sheath failures are not expected to occur, even if shutdown by either SDS1 or SDS2 is initiated on the backup trip parameter. This has been confirmed with detailed calculations of post-dryout fuel behaviour performed for the bounding Class IV power failure and pump seizure scenarios. Overpressure protection provided by each shutdown system acting alone has also</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>normally without the activation of safety systems. For both AOOs and DBAs, there should be high confidence that qualified systems (as identified in REGDOC-2.4.1, Deterministic Safety Analysis) can mitigate the event even when acting alone.</p> <p>In the analysis of AOOs and DBAs for each group of PIEs, it may be sufficient to analyze only a limited number of bounding initiating events, which can represent a bounding response for a group of events. The rationale for the choice of these selected bounding events should be provided. The plant parameters that are important to the outcome of the safety analysis should also be identified. These parameters would typically include:</p> <ul style="list-style-type: none"> <li>• reactor power and its distribution</li> <li>• core component temperatures</li> <li>• fuel cladding oxidation, and deformation</li> <li>• pressures in the primary and secondary systems</li> <li>• containment parameters</li> <li>• temperatures and flows</li> <li>• reactivity coefficients</li> <li>• reactor kinetics parameters</li> </ul>	<p>been analyzed. The assessment credits one of the two 100% capacity liquid relief valves when SDS1 is credited with initiating reactor shutdown. No heat transport liquid relief action is credited when shutdown is initiated by SDS2. Overpressure is evaluated in terms of the peak pressure in the reactor outlet headers, relative to the outlet header design pressure of 9.86 MPa(a). This ensures that the limiting components are considered when assessing the acceptability of the peak overpressures. Shutdown system action has been shown to limit heat transport system overpressure to acceptable levels. The analysis therefore indicates that shutdown system action is both timely and effective and that long-term post-shutdown cooling is assured.</p> <p>In support of Bruce A and Bruce B operation to 2019, a suite of safety analysis was performed to address the effect of the Heat Transport System aging up to aged core conditions corresponding to 2019, i.e., the end of the licensing period. Specifically, the scope of work included analysis and assessments of those events most affected by HTS aging, i.e., Loss of Flow, Small Break LOCA, Loss of Regulation (i.e., NOP analysis), and Large Break LOCA (LLOCA). The assumptions and acceptance criteria depend upon whether an event (defined as an event, event sequence, or event combination) is analyzed as an Anticipated Operational Occurrence (ADO) or a Design Basis Accident (DBA). The events were classified as AOO or DBA based on event frequency. The results for Bruce B Safety Case for Aged Core documented in Attachment 3 of [NK21-CORR-00531-10943 / NK29-CORR-00531-11325] demonstrate adequate safety margins in support of the safe operation with aged</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>reactivity worth of reactivity devices</li> </ul> <p>Those characteristics of the safety systems, including the operating conditions in which the systems are actuated, the time delays, and the systems' capacity after the actuation claimed in the design, should be specified and demonstrated to be consistent with the overall functional and performance requirements of the systems.</p> <p>Additional information</p> <p>Examples of AOOs may be found in:</p> <ul style="list-style-type: none"> <li>CNSC, REGDOC-2.4.1, Deterministic Safety Analysis, Ottawa, Canada, 2014.</li> </ul>	<p>core conditions.</p> <p>At Bruce B there has never been a systematic analysis of the capability of the control system to cope with AOOs (or transients in current parlance) since no credit has been taken for the control system actions in current safety analysis. Some cases have been performed to demonstrate control system effectiveness for specific scenarios, usually when there was a gap in the trip coverage.</p> <p>Analysis of AOOs will be considered as part of the Safety Report Improvement activities, as identified in previous sections.</p>	
7.3.3	<p>The set of DBAs shall set the boundary conditions according to which SSCs important to safety are designed.</p> <p>The design shall be such that releases to the public following a DBA will not exceed the dose acceptance criterion provided in section 4.2.1.</p> <p>In order to prevent progression to a more severe</p>	<p>The addition of dose acceptance criteria in the second paragraph does not affect the requirement.</p> <p>A set of single and dual failure accidents were considered for Bruce Power. The complete list of accident sequences considered in the safety analysis is presented in Section 2 of Part 3 of the Safety Report [NK29-SR-01320-00002, R005].</p> <p>The reference dose limit for all DBAs (20 mSv) is met since the limit quoted is 4 times that of the single failure limit used as the current Bruce B reference dose limit documented in section 1.5 of Part 3 of the Safety Report. Bruce B meets this</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>condition that may threaten the next barrier, the design shall include provisions to automatically initiate the necessary safety systems when prompt and reliable action is required in response to a PIE.</p> <p>Provision shall also be made to support timely detection of, and manual response to, conditions when prompt action is not necessary. This shall include responses such as manual initiation of systems or other operator actions.</p> <p>The design shall take into account operator actions that may be necessary to diagnose the state of the plant and to put it into a stable long-term shutdown condition in a timely manner. Such operator actions shall be facilitated by the provision of adequate instrumentation to monitor plant status, and controls for manual operation of equipment.</p> <p>Any equipment necessary for manual response and recovery processes shall be placed at the most suitable location to allow safe and timely worker access when needed.</p> <p>Guidance</p>	<p>requirement considering that the definition of DBAs given in RD-337 and CNSC REGDOC-2.5.2 is equivalent to the single process system failure used as the basis for the original Bruce B licence.</p> <p>The immediate response to many PIEs is automatic action of the special safety systems. This action is initiated through the provision of two trip parameters on each of the two shutdown systems where practicable. In a limited number of cases where automatic action is not feasible, operator action maybe credited as follows:</p> <p>Following the first clear and unambiguous indication of the necessity for operator actions, such actions may be credited:</p> <p>" 15 minutes for actions in the main control room, and</p> <p>" 30 minutes for actions outside the main control room.</p> <p>A summary of the operator actions credited in the safety analysis is documented in Section 1.3 of Part 3 of the Safety Report. Table 1-1 to Table 1-10 present a summary of the operator actions credited for the various accident categories.</p> <p>The plant has operating procedures that identify the necessary actions, operator training, and reliable instrumentation designed to provide clear and unambiguous indication of the need to take action, whether required promptly or not. The procedures are clear, well defined, and readily available in the Abnormal Incidents Manual [NK29-</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design identifies the set of DBAs and associated conditions for which the NPP is designed. This includes such responses as manual initiation of systems, or other operator actions.</p> <p>See also section 7.3.2 of this regulatory document for guidance common to AOOs and DBAs.</p> <p>Additional information</p> <p>Examples of DBAs may be found in:</p> <ul style="list-style-type: none"> <li>• CNSC, REGDOC-2.4.1, Deterministic Safety Analysis, Ottawa, Canada, 2014.</li> </ul>	<p>AIM-03600.1, Rev.056].</p>	
7.3.4	<p>The design authority shall identify the set of design-extension conditions (DECs) based on deterministic and probabilistic methods, operational experience, engineering judgment and the results of research and analysis. These DECs shall be used to further improve the safety of the NPP by enhancing the plant's capabilities to withstand, without significant radiological releases, accidents that are either more severe than DBAs or that involve additional failures.</p>	<p>The first two paragraphs are substantially revised to include DECs.</p> <p>The original design of Bruce B lacks a systematic provision for severe accident mitigation. The source term as defined by the requirement was not used for the Bruce B design. As well, the original design has not provided for complementary design features to mitigate the effects of DECs.</p> <p>A gap is identified in Section 4.2.3 of Compliance assessment against CNSC REGDOC-2.4.1. The current deterministic safety analysis as documented in Part 3 of the</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design shall be such that plant states that could lead to significant radioactive releases are practically eliminated. For plant states that are not practically eliminated, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public, and sufficient time shall be made available to implement these measures.</p> <p>Complementary design features shall be provided to cope with DEC's. Their design shall be based on a combination of phenomenological models, engineering judgments, and probabilistic methods.</p> <p>The rules and practices that have been applied to the complementary design features shall be identified. These rules and practices do not necessarily need to incorporate the same degree of conservatism as those applied to the design basis.</p> <p>The design shall identify a radiological and combustible gas accident source term, for use in the specification of the complementary design features for DEC's. This source term is referred to as the reference source term and shall be based on a set of representative core damage accidents</p>	<p>Safety Report does not distinguish between these three classes of events. The focus of the Safety Report is primarily on design basis events, which include design basis accidents and AOOs. The specific event classification scheme has not been followed for deterministic safety analysis (Gap). Further details are presented in Safety Factor 5.</p> <p>The definition of design extension conditions (DECs), the classification of events that are at the border between two classes, and the scope of BDBA extending to beyond DEC's are recognized in the COG guidelines for DSA [COG-09-9030].</p> <p>This gap is addressed through the implementation of the SAMG program which considers the potential for radiological and combustible source terms and identifies measures to prevent uncontrolled radioactive releases. As noted in previous sections Bruce Power is implementing a Safety Report Improvement Program starting in 2014 to update the safety analysis to align with modern requirements. Annual status and progress updates to the CNSC staff are provided. Further information is presented in Bruce Power letter from F. Saunders to R. Lojk, Action Item 090739: Safety Report Improvement Plan for Bruce A and Bruce B, dated November 20, 2013, File: NK21-CORR-00531-10774 &amp; NK21-CORR-00531-11155.</p> <p>Historically, DEC's leading to severe accidents as defined in this clause have not been considered in the design explicitly. The dual failure events such as large LOCA plus loss of ECI were addressed. The Severe Accident Management Guidance (SAMG) program is developed to assess the plant system capabilities in dealing with severe accidents.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>established by the design authority.</p> <p>To the extent practicable, the design shall provide biological shielding of appropriate composition and thickness in order to protect operational personnel during DEC's.</p> <p>In the case of plants with multiple units at a site, the use of available support from other units shall only be relied upon if the safe operation of the other units is not compromised.</p> <p>Guidance</p> <p>DECs are the subset of BDBAs that are considered in the design. BDBAs are all events less frequent than DBAs; there is no lower frequency bound.</p> <p>For identifying DEC's, consideration should be given to:</p> <ul style="list-style-type: none"> <li>• factors of the accident progression (i.e., physical conditions, processes and phenomena)</li> <li>• BDBA (including severe accident) scenarios resulting from initiating events, human</li> </ul>	<p>Bruce Power recognized the need for SAMGs to address multi-unit events including a station blackout. Emergency Mitigating Equipment Guidelines (EMEG5) have been prepared to provide instructions on the deployment of Emergency Mitigating Equipment (EME) to operations staff in the event of a complete loss of electrical power for load shedding and re-powering of priority I&amp;C loads. For Bruce B, the following EMEGs related to the restoration of electrical power were prepared:</p> <p>Bruce B Emergency Mitigating Equipment Guides, NK29-EME-03600. 1, Station Loss of Class IV and Class I/I Power:</p> <p>1. 1 Station Loss of Class IV and Class III Power - Coordinating Instructions</p> <p>1.2 Operation Guide for Station Loss of Class IV and Class III Power - Units 5678</p> <p>1.3 Operation Guide for Station Loss of Class IV and Class III Power - Unit 0 FH</p> <p>1.4.4 Handout - Supply Essential Loads from Portable Emergency Diesel Generator - Units 5-8</p> <p>1.4.5 Handout - Supply Essential Loads from Portable Emergency Diesel Generators - Unit 0</p> <p>1.4.6 Handout - Battery Bank BY1 and BY2 Manual Load Shedding</p> <p>1.4.7 Handout- Battery Bank BY11 and BY12 Manual Load Shedding</p> <p>The EMEGs are entered through AIM procedure NK29-AIM-03600. 1-21.2, Common Mode Events (Units 5 to 8 SCA) following a common mode event resulting in a complete loss</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>actions, and SSC operability (success or failure)</p> <ul style="list-style-type: none"> <li>selection of bounding events that are considered in design and determination of limiting values and ranges of the parameters of these events</li> </ul> <p>The design should identify the features that are designed for use in, or that are capable of preventing or mitigating events considered in DEC's. These features include complementary design features and other SSCs that may be credited for DEC's. These features should:</p> <ol style="list-style-type: none"> <li>be independent, to the extent practicable, of those used in more frequent accidents</li> <li>have a reliability commensurate with the function that they are required to fulfill</li> </ol> <p>The choice of the DEC's to be analyzed should be explained and justified, indicating whether it has been made on the basis of a PSA or other analysis that identifies potential vulnerabilities of the plant.</p> <p>For use in the specification of the complementary design features for DEC's, the reference source</p>	<p>of electrical power [NK29-CORR-00531-10482].</p> <p>Bruce Power has completed an assessment that examined the effectiveness of various Containment Filtered Venting System (CFVS) designs as well as the effectiveness of other options for protecting containment integrity and limiting fission product release during a multi-unit severe accident for FAI 1.3.2. A report summarizing the results of the assessment was provided in Enclosure 1 of [NK29-CORR-00531-12195]. The report also included the results of a risk-informed Cost Benefit Assessment (CBA) undertaken to evaluate the overall cost versus risk reduction (equated to cost) for each modification. The results indicated that installation of a Westinghouse dry filter or AREVA multi-venturi wet scrubber system is not strongly supported by the risk-informed Cost Benefit Assessment. Instead, the existing design capability and emergency mitigation measures aimed at preventing severe core damage were confirmed to be a viable alternative to the installation of a filter vent system dedicated to management of containment pressure during severe accidents. As indicated in Bruce Power Progress Report No. 6 on CNSC Action Plan - Fukushima Action Items [NK29-CORR-00531-12195], Bruce Power has initiated a supplementary project to evaluate an AREVA dry filter design as well as a portable CFVS unit to serve as additional defence-in-depth. Bruce Power is on track to complete these additional evaluations by the end of 2016. In order to provide the option for a future system, Bruce Power successfully installed a connection point on the EFADs lines where they exit the Vacuum Building and Pressure Relief Valve (PRV) Manifold at Bruce B.</p> <p>The implementation of SAMG for multi-unit events is being</p>	




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>term should be calculated for a set of representative accident scenarios based on the best-estimate models. This should take into account the uncertainties of key parameters and the possible changes in governing physical processes.</p> <p>Accidents in this category are, typically, sequences involving more than one failure (unless these are taken into account in the DBAs at the design stage). Such sequences may include DBAs with degraded performance of a safety system, and sequences that could lead to containment bypass. The analysis of those accidents may:</p> <ul style="list-style-type: none"> <li>• use best-estimate models and assumptions</li> <li>• take credit for realistic system action and performance beyond original intended functions, including the potential use of safety, non-safety and temporary systems</li> <li>• take credit for realistic operator actions</li> </ul> <p>Where this is not possible, reasonably conservative assumptions should be made in which the uncertainties in the understanding of the physical processes being modelled are</p>	<p>undertaken in two parts: (1) update of the Technical Basis Document (TBD) and the revision of the generic SAMG documentation, including multi-unit events will be developed by the Severe Accident Support Team under COG JP-4426. (2) the station-specific SAMG documentation for multi-unit events and low power will be prepared by Bruce Power. Plans and schedules for the inclusion of multi-unit events in Bruce Power operating documentation are captured under Fukushima Action Items. The inclusion of irradiated fuel bay (IFB) events in station operating documentation was assessed under the COG Severe Accident Joint Project JP-4426. The work related to Irradiated Fuel Bay (IFB) events involved primarily the creation of new documents for each station (e.g., IFB Severe Challenge Guidelines and associated Computational Aids, including IFB Enabling Procedures) as opposed to updates of existing documentation. However, it was recognized that the new SAMG documents created for IFB events would need to be integrated into the existing set of SAMG documents. The SAMG updates to address multi-unit events and IFB events have been completed as described in Attachment B to Bruce Power Progress Report No. 7 on CNSC Action Plan - Fukushima Action Items [NK29-CORR-00531-12635].</p> <p>As reported in the Bruce Power Progress Report No. 7 on CNSC Action Plan - Fukushima Action Items [NK29-CORR-00531-12635] the SAMG to address multi-unit events and irradiated bay events have been completed as described in Attachment B to [NK29-CORR-00531-12635]. Updates to the Bruce Power station specific SAMG for multi-unit events included changes to the station-specific SAMG documentation essentially as recommended by the COG topical report, COG-JP-4426-005-RO, "Multi-Unit Events</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>considered. The analysis should justify the approach taken.</p> <p>Accident conditions with a significant release are considered to have been practically eliminated:</p> <ul style="list-style-type: none"> <li>if it is physically impossible for the condition to occur, or</li> <li>if the condition can be considered with a high degree of confidence to be extremely unlikely to arise</li> </ul> <p>Physical impossibility can be demonstrated by a design feature that would preclude initiation or further progress of an accident scenario. Care should be taken when assumptions are used to support the demonstration. Such assumptions should be adequately acknowledged and addressed.</p> <p>To demonstrate practical elimination as extremely unlikely with a high degree of confidence, the following should be considered:</p> <ul style="list-style-type: none"> <li>The degree of substantiation provided for the demonstration of practical elimination should take account of the assessed frequency of the</li> </ul>	<p>Update of SAMG and Technical Basis Documents". The development of a parallel multi-unit severe accident modelling capability (FAI 3.2.1 and 3.2.2), being tracked under AI 1307-3703, has also been completed and site specific implementation and testing has been conducted for Darlington station. The results of the work indicate that the scaling and injection methods used previously to approximate multi-unit accidents in the single-unit MAAP4-CANDU models agree with the newly developed multi-unit model. The predictions from these two approaches are sufficiently well aligned such that further development of multi-unit models for Bruce A and Bruce B is not warranted.</p> <p>In the area of enhancing emergency response, Bruce Power is in the process of upgrading its Emergency Response Projection (ERP) code to allow multi-unit dose projection modeling capability under AI 1307-3790. Due to the collaborative nature of the ERP tool, Bruce Power has consulted with OPG, the CNSC, the province of Ontario and industry vendors in order to develop a solution which best satisfies all stakeholders. These discussions have resulted in a delay to the effective start date of the project but have provided an opportunity to share on a number of issues which should permit a more predictable project execution. Bruce Power now forecasts completion of the ERP upgrade project by September 30, 2017 [Bruce Power Progress Report No. 8 on CNSC Action Plan - Fukushima Action Items, NK29-CORR-00531-12979].</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>situation to be eliminated and of the degree of confidence in the assessed frequency.</p> <ul style="list-style-type: none"> <li>Practical elimination of an accident should not be claimed solely based on compliance with a probabilistic cut-off value. Even if the probability of an accident sequence is very low, any additional design features, operational measures or accident management procedures to lower the risk further should be implemented to the extent practicable.</li> <li>The most stringent requirements regarding the demonstration of practical elimination should apply in the case of an event with the potential to lead directly to a severe accident; i.e., from Level 1 to Level 4 for defence in depth. For example, demonstration of practical elimination of a heterogeneous boron dilution event in a pressurized water reactor (PWR) would require a detailed substantiation.</li> <li>The necessary high confidence in low likelihood should, wherever possible, be supported by means such as: <ul style="list-style-type: none"> <li>multiple layers of protection</li> <li>application of the safety principles of independence, diversity, separation, redundancy</li> <li>use of passive safety features</li> <li>use of multiple independent controls</li> </ul> </li> <li>It should be ensured that the practical elimination provisions remain in place and valid</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>throughout the plant lifetime; for example, through in-service and periodic inspections.</p> <p>In each case, the demonstration should show sufficient knowledge of the accident sequence analyzed and of the phenomena involved, substantiated by relevant evidence.</p> <p>To minimize uncertainties and to increase the robustness of a plant's safety case, demonstration of practical elimination should preferably rely on the criterion of physical impossibility, rather than the second probabilistic criterion (extreme unlikelihood with high confidence).</p> <p>Portable equipment should be classified based on its safety importance.</p> <p>There may be different options available to fulfill the fundamental safety functions during DEC's. However, when called upon the portable onsite or offsite equipment credited is expected to be effective with reasonable confidence.</p> <p>Portable onsite or offsite equipment may be one of the means for mitigation in support of the severe accident management guidelines.</p>		

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Additional information</p> <p>Examples of BDBAs may be found in:</p> <ul style="list-style-type: none"> <li>CNSC, REGDOC-2.4.1, Deterministic Safety Analysis, Ottawa, Canada, 2014.</li> </ul>		
7.3.4.1	<p>The design shall be balanced such that no particular design feature or event makes a dominant contribution to the frequency of severe accidents, taking uncertainties into account.</p> <p>Early in the design process, the various potential barriers to core or fuel degradation shall be identified, and features that can be incorporated to halt core or fuel degradation at those barriers shall be provided.</p> <p>The design shall also identify the equipment to be used in the management of severe accidents including equipment that is available onsite and offsite.</p> <p>The design shall include redundant connection points to provide for water and electrical power which may be needed to support severe accident</p>	<p>The text is modified to include DEC's with severe core damage as well as new requirements for design provisions for severe accidents.</p> <p>The enhancements to SAMG are undertaken under COG JP-4426 followed by station-specific implementation at each station. The scope of work is as follows:</p> <p>" Enhancement of SAMG to include multi-unit events and IFB events.</p> <p>" Assessment of instrument and equipment survivability under severe accident and identification of equipment upgrades required.</p> <p>" Assessment of plant habitability under severe accident conditions and identification of modifications required.</p> <p>" Improvement to understanding of severe accident phenomena including containment integrity, hydrogen production, aerosol behavior, and in vessel retention.</p> <p>As documented in Bruce Power Progress Report No. 4 on CNSC Action Plan - Fukushima Action Items, [NK29-CORR-</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>management actions.</p> <p>Provisions for testing the equipment shall be provided to the extent practicable.</p> <p>A reasonable level of confidence that this equipment will perform as intended in the case of a severe accident shall be demonstrated by fire and seismic assessments, and consideration of environmental conditions.</p> <p>Consideration shall be given to the plant's full design capabilities, including the possible use of safety, non-safety, and temporary systems, beyond their originally intended function. This shall apply to any system that can be shown with a reasonable degree of assurance to be able to function in the environmental conditions expected during a severe accident.</p> <p>For DEC's with severe core damage, the containment shall maintain its role as a leak-tight barrier for a period that allows sufficient time for the implementation of offsite emergency procedures following the onset of core damage. Containment shall also prevent uncontrolled releases of radioactivity after this period.</p>	<p>00531-11349] Bruce Power has completed all short term modifications to allow emergency water to be added to the steam generators and Irradiated Fuel Bays (IFBs) using Emergency Mitigating Equipment (EME) pumps.</p> <p>External power supply enhancements have been incorporated as part of Fukushima Action Items response. Seven 100 kW generators were purchased for Bruce B (six to be deployed in the field and one spare). The Bruce B generators have a standard tow hitch and can be deployed using a truck, tractor, or heavy equipment such as a payloaders [Bruce Power Progress Report No. 1 on CNSC Action Plan - Fukushima Action Items, NK21-CORR-00531-09676 / NK29-CORR-00531-10193]. The power cables from the generators have quick disconnects which are intended to be convenient for emergency responders. Design modifications were carried out at Bruce B to provide easily accessible connection points which will provide power to Emergency Power Motor Control Centres (MCCs) located in the Units 5 to 8 SCAs, EFADS and EWPS buildings. Bruce Power assessed the capability of Class 1 and 2 power supplies. Class 1 and 2 power supplies are capable of providing uninterruptible power for a period of about 40 minutes following a loss of Class 3 and 4 power. Operational procedures were being prepared to shed unnecessary Class 1 and 2 loads to extend the battery life from existing 40 minutes to up to 3 hours. Bruce Power has performed a review of the emergency electrical power system and determined that technical specifications [NK29-TS-55100-001 Revision 04] confirm that lead-calcium flat plate batteries are acceptable battery designs to meet the Bruce B design requirements for the 250Vdc Class I distribution system</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Particular attention shall be placed on the prevention of potential containment bypass in severe accidents.</p> <p>The design authority shall establish initial severe accident management guidelines, taking into account the plant design features including requirements for multiple units at a site, and the understanding of accident progression and associated phenomena.</p> <p>Consideration shall be given to the prevention of recriticality following severe accidents.</p> <p>Guidance</p> <p>Severe accidents represent accidents that involve significant fuel degradation, either in-core or in fuel storage.</p> <p>Detailed analysis should be performed and documented to identify and characterize accidents that can lead to significant fuel damage or offsite releases of radioactive material (severe accidents).</p>	<p>[NK29-CORR-00531-12979].</p> <p>Assessments of adequacy of the existing means to protect containment integrity and prevent uncontrolled release in beyond-design-basis accidents including severe accidents have been carried out as part of Fukushima Action Items initiatives. Based on the supporting analysis for the level 2 PRA which showed that containment integrity can be challenged during a multi-unit severe accident, options for enhancing the ability of containment to cope with severe accidents have been explored. Bruce Power assessment of adequacy of the existing means to protect containment integrity and prevent uncontrolled release in BDBAs including severe accidents is documented in Enclosure 1 of [NK29-CORR-00531-12195]. In this assessment, Bruce Power concluded that existing design capability and emergency mitigation measures aimed at preventing severe core damage represent a viable alternative to the installation of a filter vent system [NK29-CORR-00531 -12979].</p> <p>Bruce Power is implementing design changes to improve severe accident response. For example Passive Autocatalytic Recombiners (PARs) have been installed in both Bruce A and Bruce B units to provide additional hydrogen mitigation capability [NK29-CORR-00531-12635, Bruce Power Progress Report No. 7 on CNSC Action Plan - Fukushima Action Items, August 7, 2015].</p> <p>Bruce A &amp; B PARs project was initiated to provide mitigation of the potential buildup of Hydrogen gas in the Reactor Vaults or other areas of Containment during a severe accident scenario since buildup of hydrogen in the containment system has the potential to cause an explosion, if not</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>In addition, evaluations should be carried out on the capability of complementary design features to cope with DEC's. The challenges to the plant presented by such events, and the extent to which the design may be reasonably expected to mitigate their consequences should be considered in establishing the initial severe accident management guidelines which will facilitate meeting the expectations of CNSC REGDOC-2.3.2, Accident Management: Severe Accident Management Programs for Nuclear Reactors.</p> <p>Containment leakage in a severe accident should remain below the design leakage rate limit (as defined in section 8.6.4) for sufficient time to allow implementation of emergency measures. Beyond this time, containment leakage that would lead to exceeding the small and large release safety goals should be precluded. This may be achieved by provision of adequate filtered containment venting along with other features.</p> <p>The design should include the analysis performed for severe accident progression and consequence evaluation including assessments on topical issues, as applicable, such as:</p>	properly mitigated.	

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>corium stratification</li> <li>thermal-chemical interaction between corium, steel components and vessel</li> <li>heat transfer from corium to vessel or end-shield</li> <li>hydrogen burn</li> <li>steam explosion due to molten fuel-coolant interaction</li> <li>corium-concrete interaction</li> </ul> <p>The results of the severe accident analysis should be taken into account when developing initial severe accident management guidelines and for emergency preparedness.</p> <p>Redundant connection points for water and electrical power which may be needed to support severe accident management actions should use standard connections and be readily accessible. These connection points should also be physically separated, to minimize risks from common- cause events. The design should facilitate the use of equipment and supplies from onsite and offsite locations, such as fuel supply, batteries, onsite and offsite temporary pumps, generators and battery chargers.</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>CNSC, RD-327, Nuclear Criticality Safety, section 16 - Nuclear Criticality Accident Emergency Planning and Response, Ottawa, Canada, 2010.</li> </ul>		
7.4	<p>The design for the NPP shall apply a systematic approach to identifying a comprehensive set of postulated initiating events, such that all foreseeable events with the potential for serious consequences or with a significant frequency of occurrence are anticipated and considered.</p> <p>Postulated initiating events can lead to AOOs, DBAs or BDBAs, and include credible failures or malfunctions of SSCs, as well as operator errors, common-cause internal hazards, and external hazards.</p> <p>For a site with multiple units, the design shall take due account of the potential for specific hazards simultaneously impacting several units on the site.</p> <p>Guidance</p>	<p>This clause is expanded and two new (first and last) paragraphs are included.</p> <p>A systematic event identification process is not well documented and/or demonstrated; therefore this is assessed as a gap (Gap). Postulated initiating events are not categorized into AOOs, DBAs or BDBAs. Additional details are provided in the assessment against CNSC REGDOC-2.4.1 documented in Safety Factor 5.</p> <p>Detailed assessment against the requirements related to probabilistic safety assessment is presented in the assessment of CNSC REGDOC-2.4.2.</p> <p>As described in the compliance note for Clause 7.3.4 above, Bruce Power recognized the need for SAMGs to address multi-unit events including a station blackout. The site-specific SAMGs have been completed and the overall SAMG implementation is being tracked and reported to the CNSC. The SAMG updates to address multi-unit events and irradiated fuel bay events have also been completed as reported in Attachment B to [NK29-CORR-00531-12635].</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The postulated initiating events (PIEs) are identified using engineering judgment and deterministic and probabilistic assessment. A justification of the extent of usage of deterministic safety analyses and probabilistic safety analyses should be provided, in order to show that all foreseeable events have been considered.</p> <p>Sufficient information should be provided regarding the methods used to identify PIEs, their scope and classification. In cases where the identification methods have made use of analytical tools (e.g., master logic diagrams, hazard and operability analysis, failure modes and effect analysis), detailed information is expected to be presented.</p> <p>A systematic approach to event classification should consider all internal and external events, all normal operating configurations, various plant and site conditions, and failure in other plant systems (e.g., storage for irradiated fuel, and tanks for radioactive substances).</p> <p>The design should take into account failure of equipment that is not part of the NPP, if the failure has a significant impact on nuclear safety.</p>		


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>CNSC REGDOC-2.4.1, Deterministic Safety Analysis and REGDOC-2.4.2, Probabilistic Safety Assessments, provide the requirements and guidance for establishing the scope of PIEs, and for classifying the PIEs in accordance with their anticipated frequencies, and other factors, as appropriate.</p> <p>For further information on the safety analysis for the identified PIEs, refer to section 9.0 of this document.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>CNSC, REGDOC-2.4.1, Deterministic Safety Analysis, Ottawa, Canada, 2014.</li> </ul>		
7.4.1	<p>SSCs important to safety shall be designed and located in a manner that minimizes the probability and effects of hazards (e.g., fires and explosions) caused by external or internal events.</p> <p>The plant design shall take into account the potential for internal hazards, such as flooding,</p>	<p>A new requirement for internal events to be identified and AOOs, DBAs and DECAs to be determined from these events in included in this clause.</p> <p>Since the current design documentation does not consider internal events as leading to AOOs, DBAs and DECAs, this is assessed as a gap in Clause 7.4 (Gap).</p> <p>When Bruce B was being designed the issue of postulated</p>	Gap



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>missile generation, pipe whip, jet impact, fire, smoke, and combustion by-products, or release of fluid from failed systems or from other installations on the site. Appropriate preventive and mitigation measures shall be provided to ensure that nuclear safety is not compromised.</p> <p>Internal events which the plant is designed to withstand shall be identified, and AOOs, DBAs and DECAs shall be determined from these events.</p> <p>The possible interaction of external and internal events shall be considered, such as external events initiating internal fires or floods, or that may lead to the generation of missiles.</p> <p>Guidance</p> <p>The design should take into account specific loads and environmental conditions (temperature, pressure, humidity, radiation) imposed on structures or components by internal hazards.</p> <p>The following potential initiators of flooding should be considered:</p>	<p>pipe rupture was revisited and the original design of Bruce B was modified. The assessment was documented in Bruce B Reactor Safety Note 29 RS-3, January 1982 titled "Summary of Analysis of postulated Breaks in the Primary Heat Transport Piping". This report summarizes a review of the original design of Bruce B (which was the Bruce A design) against the effects of pipe whip and jet impingement following postulated ruptures at several locations. As a result of that review there were 15 design modifications for Bruce B [Enclosure 3 of Letter F, Saunders to P. Webster, Bruce A Refurbishment for Life Extension - Systematic Review of Safety: Plant Design, NK21-CORR-00531-04059, March 30, 2006]. Section 2.2 of Part 2 of the Safety Report describes the wind and snow loading as well as flood design provisions. Section 2.5 of Part 2 of the Safety Report presents further discussion about Bruce B protection against common mode events.</p> <p>A systematic identification of internal hazards in accordance with current expectations has not been performed for the Bruce B original design. As a result, several hazards (e.g., pipe whip, jet impingement, missile generation, etc.) have not been taken into consideration in the original design. The effects of pipe whip and jet impingement are being addressed for Bruce B primarily by showing that any pipe leak will be detected with sufficient reliability and warning time such that appropriate actions will be taken to avoid a pipe break. As discussed in supporting documentation for NK21-CORR-00531-11567 / NK29-CORR-00531-11950 [Letter F. Saunders to K. Larfreniere, Integrated Implementation Plan for Bruce A, Bruce B and Centre of Site in the Next Licence Period, October 31, 2014] CNSC has accepted the results of the Pipe Whip and Jet Impingement Assessment of Piping</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>leaks and breaks in pressure-retaining components</li> <li>flooding by water from neighbouring buildings</li> <li>spurious actuation of the fire-fighting system</li> <li>overfilling of tanks</li> <li>failures of isolating devices</li> </ul> <p>The design considers internal missiles which can be generated by failure of rotating components (such as turbines), or by failure of pressurized components. For those potential missiles considered to be credible, the following actions should be taken:</p> <ul style="list-style-type: none"> <li>a realistic assessment is made of the postulated missile size and energy, and its potential trajectories</li> <li>potentially impacted components associated with systems required to achieve and maintain a safe shutdown state are identified</li> <li>a loss of these potentially impacted components is evaluated to determine if sufficient redundancy remains to achieve and maintain a</li> </ul>	<p>Inside the Reactor Vault for Bruce A [NK21-CORR-00531-12191]. The results of the Bruce A design assessment concluded that no design changes are required in the Units 1 and 2 vaults as a result of pipe-whip or jet impingement. Bruce Power is committed to develop a plan and assess pipe whip/jet impingement at Bruce B by December 16, 2019 using similar approach as for Bruce A.</p> <p>In addition the issue of assessing effects of pipe whip and jet impingement is reflected in CANDU Safety Issue (CSI) IH6 "Need for systematic assessment of high energy line break effects", originally designated as a Category 3 issue (measures are in place to maintain safety margins, but the adequacy of these measured needs to be confirmed) for all licenses [N-REP-03611-0381169, Application of the CNSC Risk-Informed Decision Making Process to Category 3 CANDU Safety Issues, Canadian Nuclear Safety Commission Report, August 2009]. Bruce Power requested a reclassification of Issue IH6 from Category 3 to lower Category 2 (appropriate measures are in place to maintain safety margins) for both Bruce A and Bruce B, with the Bruce B request based on an assessment that considered the dynamic effects of pipe whip of large Heat Transport System (HIS) piping, and their potential consequences on nuclear safety. The assessment confirmed that the capability to control, cool and contain would not be significantly impaired by the postulated breaks in containment [NK21-CORR-00531-09435 / NK29-CORR-00531-10019, CANDU Category III Safety Issues: Request for Reclassification of AA3, PF 20, SS5 and IH6, Bruce Power Letter, F. Saunders to G. Rzentkowski, June 25, 2012]. CNSC staff agreed to reclassify IH6 as a Category 2 issue for Bruce A and Bruce B stations, provided that probabilistic fracture mechanics</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>safe shutdown state</p> <p>The civil design takes into account loads generated by internal hazards in the environmental loading category consistent with section 7.15.</p>	<p>calculations be performed to demonstrate that the probability of double-ended guillotine breaks in large diameter high energy piping is acceptably low [NK21-CORR-00531-09822 / NK29-CORR-00531-10295, Reclassification of Category 3 CANDU Safety Issue IH6: "Need for systematic assessment of high energy line break effects" to Category 2, New Action Item 1207-3509, CNSC Letter, R. Lojk to F. Saunders, August 29, 2012]. Bruce A and B Action Item 1207-3509 was opened to track progress on this issue, and Bruce Power is working with the CANDU Industry in performing the requested probabilistic fracture mechanics calculations.</p> <p>The original design of Bruce A and B did not consider the potential for fires and explosions, although the effects of such events were addressed, and features were provided to protect against them. To address this gap, a Fire PRA is prepared for both Bruce A and B as part of an on-going project to implement the CNSC Regulatory Standard S-294 in support the operating licence renewal in 2014 [NK21-CORR-00531-11005 / NK29-CORR-00531-11397].</p> <p>A Fire Safe Shutdown Analysis has been performed for Bruce B [(FSSA) [Bruce-B Nuclear Generating Station Fire Safe Shutdown Analysis, NK29-REP-71400-00003, Revision 03, December 2012], to ensure safe design in case of fire events. In addition, a Fire Hazard Analysis [BNGS-B Fire Hazard Assessment (FHA) NK29-REP-71400-00004, Revision 04, January, 2013] and Fire Protection Code Compliance Reviews [NK29-REP-71400-00002, R03, December 2012] have also been prepared. Additional details are provided in the Fire PRA Summary Report [NK29-03611.1 P NSAS, July 24, 2014] and associated attachments. In addition, a detailed review of FSSA</p>	

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>recommended operator actions has been performed and documented in Enclosure 2 of Letter F. Saunders to K. Lafreniere, Action 1207-3890: Provide Annual Update for the Fire Protection Capital Projects, NK221-CORR-00531-12304/NK29-CORR-00531-12735, November 30, 2015].</p> <p>Bruce Power has already completed a PRA Guide - "Phase 1 Fire PRA Guide" [B-REP-03611-00008, R01, September 2012].</p> <p>Section 2.5.3 of Part 2 of the Safety Report [NK29-SR-01320-00001] indicates that features incorporated into the Bruce B design provide an adequate level of protection against any credible turbine generator missile. These features include:</p> <ol style="list-style-type: none"> <li>1. Separation of the 600 V Class II switchgear, such that a single missile cannot disable both halves of the system.</li> <li>2. Reinforced concrete barriers, such that a turbine generator missile cannot strike the HT pump motors.</li> <li>3. Adoption of separation measures [NK29-DG-29-03650-005], such that a single missile cannot disable sufficient equipment to prevent safe shutdown, monitoring, or decay heat removal.</li> </ol> <p>The safety Design Guide "Location and Separation Requirements for Safety Related Systems" [NK29-DG-03650-5 R03] specifies that hazards such as pipe whip, jet impingement, missiles, etc. must be taken into consideration. For example as described in section 6, the location of the safety related equipment must be such that the dynamic effect of the fluid jets produced by and credible process</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		failure can be absorbed by the equipment without adverse effects. If this is not possible, barriers must be provided.	
7.4.2	<p>All natural and human-induced external hazards that may be linked with significant radiological risk shall be identified. External hazards which the plant is designed to withstand shall be selected, and classified as DBAs or DEC's.</p> <p>Various interactions between the plant and the environment, such as population in the surrounding area, meteorology, hydrology, geology and seismology shall be identified during the site evaluation and environmental assessment processes. These interactions shall be taken into account in determining the design basis for the NPP.</p> <p>Applicable natural external hazards shall include such hazards as earthquakes, droughts, floods, high winds, tornadoes, tsunami, and extreme meteorological conditions. Human induced external hazards shall include those that are identified in the site evaluation, such as potential aircraft crashes, ship collisions, and terrorist activities.</p> <p>Guidance</p>	<p>There are no major changes to the requirement. The change introduced in CNSC REGDOC-2.5.2 is editorial in nature and does not affect the requirement.</p> <p>The intensity and distribution of all wind loads, including the dynamic action of wind gusts and snow loading, was determined in accordance with the requirements of the National Building Code of Canada, 1975. The design weather data selected for Bruce site are presented in Table 2.1, section 2.2 of part 2 of the Safety Report [NK29-SR-01320-00001, Rev.005]. The flood design considerations are summarized in section 2.2.2 of Part 2 of the Safety Report. The building site is protected from the lake by a dike which varies up to 1.39 m (4.5 ft) above grade level, and about 2.74 m (9 ft) above the highest water level recorded at the site. The dike provides an adequate safety barrier against the most severe anticipated combination of spring run-off, wind velocity and wave action. Buoyancy due to the presence of ground water will not be a problem.</p> <p>Loads and loading combinations, considered for the design of the containment and other structures are summarized in section 2.3 of Part 2 of the Safety Report.</p> <p>General description of the site and seismic and environmental considerations are presented in section 2 of Part 1 of the Safety Report. As described in section 2.6.2.2 the Design Basis Seismic Ground Motion (DBSGM) was determined from a statistical analysis of historical seismic events, obtained from the Earth Physics Branch of the Department of Energy Mines and Resources (EMR) for the</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design should take into account all site characteristics that may affect the safety of the plant, and should identify the following:</p> <ul style="list-style-type: none"> <li>• site-specific hazard evaluation for external hazards (of human or natural origin)</li> <li>• design assumptions or values, in terms of recurrence probability of external hazards</li> <li>• definition of the design basis for external hazards</li> <li>• collection of site reference data for the plant design (geotechnical, seismological, hydrological, hydrogeological and meteorological)</li> <li>• evaluation of the impact of the site-related issues to be considered in the application, concerning emergency preparedness and accident management</li> <li>• arrangements for the monitoring of site-related parameters throughout the life of the plant</li> </ul> <p>Natural external hazards other than earthquakes may be categorized as:</p> <ul style="list-style-type: none"> <li>• hazards that have potential to damage SSCs important to safety</li> </ul>	<p>Bruce site, in which 946 earthquakes between 1899 and 1963 were analyzed. This analysis demonstrated that an earthquake having a probability of exceedance of 0.01 events per year would result in a peak horizontal ground motion at the site of 0.015 g. However, in keeping with a design policy of designing for a minimum ground motion acceleration, in seismic zone 1 of 0.025 g, this value was selected and designated as the Site Design Seismic Ground Motion (SDSGM). The DBSGM for this site was taken as twice the SDSGM or equivalent to a horizontal ground acceleration of 0.050 g. This value was reviewed in conjunction with the more advanced techniques developed by the Earth Physics Branch of EMR in 1978. A seismic region for the Bruce B site was defined as an area encompassed by a radius of 300 km (186 miles) around the site. Considering the historical seismic events occurring within this area, a magnitude recurrence equation was developed for this region. Based upon this technique, an analysis was undertaken which verified the original DBSGM of 0.050 g. Dynamic analyses were carried out to determine the modal frequencies, mode shapes and modal participation factors of the structures. The seismic response of the structures was determined by modal analysis using the artificial acceleration time history as seismic input. The acceleration time history responses, calculated at selected points in the structure, were used as seismic input for the development of floor response spectra, which are required for the seismic qualification of the safety-related equipment and systems. Further details of the Bruce B seismic design are presented in section 2.6.2.3 of Part 1 of the Safety Report and section 2.5.2 of Part 2 of the Safety Report.</p> <p>A Probabilistic Seismic Hazard Assessment was completed</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>hazards that are evaluated and screened out</li> </ul> <p>Natural external hazards considered in the design process should include:</p> <ul style="list-style-type: none"> <li>earthquakes</li> <li>extreme meteorological conditions of temperature, snow, freezing rain, hail, frost, subsurface freezing and drought</li> <li>floods due to tides, tsunamis, seiches, storm surges, precipitation, waterspouts, dam forming and dam failures, snow melt, land slides into water bodies, channel changes and work in the channel</li> <li>cyclones (e.g., hurricanes, tornadoes) and straight winds</li> <li>abrasive dust and sand storms</li> <li>lightning</li> <li>volcanoes (site is sufficiently remote from volcanoes)</li> <li>biological phenomena</li> <li>collision of floating debris (e.g., ice, logs) with accessible safety-related structures, such as water intakes and ultimate heat sink components</li> <li>geomagnetic storm (solar flare and</li> </ul>	<p>for the Bruce site in 2011 (NK29-03500.8 P NSAS Bruce B Nuclear Generating Station Seismic Hazard Assessment) which indicated that the expected mean peak ground acceleration for an "annual probability of exceedance" of 1E-4 at 100Hz would be 0.016g. This indicates that the peak ground response used in the design of Bruce B of 0.05g, stated as having a "small probability of exceedance during the life of the plant" (clause 4.1 of NK29-DG-03650-002) is conservative and satisfies the definition of a DBE. Further details are presented in Safety Factor 3.</p> <p>Bruce Power has utilized specific Probabilistic Risk Assessment (PRA) Methodology Guides for conducting PRAs for the following internal and external hazards:</p> <p>" B-REP-03611-00007, Bruce Power PRA Guide, Internal Flood;</p> <p>" B-REP-03611-00008, Bruce Power PRA Guide, Internal Fire;</p> <p>" B-REP-03611-00009, Bruce Power Seismic PRA Guide;</p> <p>" B-REP-03611-00011, Bruce Power PRA Guide, Screening and Disposition of External Hazards;</p> <p>" B-REP-03611-00012, Bruce Power PRA Guide, High Wind Hazard; and</p> <p>" B-REP-03611-00013, Bruce Power PRA Guide, External Flooding.</p> <p>Bruce Power undertook, as part of its disposition of Fukushima Action Items, a re-evaluation of the site-specific magnitudes of each external event to which the plant might</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>electromagnetic pulses)</p> <ul style="list-style-type: none"> <li>combinations of extreme weather conditions that could reasonably be assumed to occur at the same time</li> </ul> <p>Natural external hazards that are evaluated and screened out may be based on the following criteria:</p> <ul style="list-style-type: none"> <li>a phenomenon that occurs slowly or with adequate warning with respect to the time required to take appropriate protective action</li> <li>a phenomenon which in itself has no significant impact on the operation of an NPP and its design basis</li> <li>an individual phenomenon which has an extremely low probability of occurrence</li> <li>the NPP is located sufficiently distant from or above the postulated phenomenon (e.g., fire, flooding)</li> <li>a phenomenon that is already included or enveloped by design in another phenomenon (e.g., storm-surge and seiche included in flooding or accidental small aircraft crash enveloped by tornado loads)</li> </ul>	<p>be susceptible, using modern calculations and methods; and an evaluation as to whether the current site-specific design protection for each external event so assessed is sufficient. An extensive screening assessment was conducted based on a screening methodology submitted to CNSC staff in [NK21-CORR-00531-09253/NK29-CORR-00531-09881, Submission of Revised Bruce Power Probabilistic Risk Assessment Guide - Screening and Disposition of External Events, Bruce Power Letter, F. Saunders to R. Lojk, March 9, 2012]. These hazards were initially subjected to a first-level screening [NK21-CORR-00531-09809/NK29-CORR-00531-10287, Bruce A and B External Hazard Assessment, Bruce Power Letter, F. Saunders to R. Lojk, September 28, 2012], and the hazards which were not eliminated in the first level were then subjected to a second level of screening ([88],[89]). Following this second level of screening, the only hazards requiring assessment are tornadoes, high winds and external flooding. To address these remaining external hazards, Bruce Power has submitted [NK21-CORR-00531-09969/NK29-CORR-00531-10409, Methodology for Tornados, High Winds and External Flooding, Bruce Power Letter, F. Saunders to R. Lojk, November 27, 2012] a methodology for analysis of tornados, high winds and external flooding. In addition Bruce Power submitted [NK21-CORR-00531-11324/NK29-CORR-00531-11729, Submission of S-294 Probabilistic Risk Assessment Final Reports, Bruce Power Letter, F. Saunders to K. Lafrenière, July 31, 2014] the following reports: a High Wind PRA Report, Seismic PRA Report, Fire PRA Report, and External Flooding Assessment (in addition to revised versions of a Seismic PRA Report and Fire PRA Report). Table B5 of [NK29-CORR-00531-12979] presents the schedule for external hazards assessment</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Human induced hazards considered in the design process should include:</p> <ul style="list-style-type: none"> <li>• aircraft crashes (general aviation)</li> <li>• explosions (deflagrations and detonations) with or without fire, with or without secondary missiles, originating from offsite and onsite sources (but external to safety-related buildings), such as hazardous or pressurized materials in storage, transformers, pressure vessels, or high- energy rotating equipment</li> <li>• release of hazardous gases (asphyxiant, toxic) from offsite and onsite storage</li> <li>• release of corrosive gases and liquids from offsite and onsite storage</li> <li>• release of radioactive material from offsite sources</li> <li>• fire generated from offsite sources (mainly for its potential for generating smoke and toxic gases)</li> <li>• collision of ships or floating debris with accessible safety-related structures, such as water intakes and ultimate heat sink components</li> <li>• collision of vehicles at the site with SSCs</li> <li>• electromagnetic interference from off the site (e.g., from communication centres and</li> </ul>	<p>activities.</p> <p>The requirements related to plane crash and terrorist activities are not addressed in this assessment due to the sensitivity of information.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>portable phone antennas) and on the site (e.g., from the activation of high voltage electrical switchgear and from unshielded cables)</p> <ul style="list-style-type: none"> <li>any combination of the above, as a result of a common initiating hazard (such as an explosion with fire and release of hazardous gases and smoke)</li> </ul> <p>Malevolent acts including aircraft crashes are considered separately, in section 7.22.</p> <p>For civil design, human induced hazards which are classified as DBAs are taken into account as loads in the abnormal or extreme environmental load category, consistent with section 7.15. Less frequent human induced hazards are considered part of DEC.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>American Nuclear Society (ANS), 2.3, Estimating Tornado, Hurricane, and Extreme Straight Line Wind Characteristics at Nuclear Facility Sites, La Grange Park, Illinois, 2011.</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>CNSC, RD-346, Site Evaluation for New Nuclear Power Plants, Ottawa, Canada, 2008.</li> <li>IAEA, NS-G-3.1, External Human Induced Events in Site Evaluation for Nuclear Power Plants, Vienna, 2002.</li> <li>National Research Council (NRC), National Building Code of Canada, Ottawa, Canada, 2010.</li> </ul>		
7.4.3	<p>Combinations of randomly occurring individual events that could credibly lead to AOOs, DBAs, or DECAs shall be considered in the design. Such combinations shall be identified early in the design phase, and shall be confirmed using a systematic approach.</p> <p>Events that may result from other events, such as a flood following an earthquake, shall be considered to be part of the original PIE.</p> <p>Guidance</p> <p>Where the results of engineering judgment, deterministic safety assessments and probabilistic safety assessments indicate potential combinations of events, such combinations of events should be considered to be AOOs, DBAs or DECAs, depending on their likelihood of</p>	<p>The change in this clause is minor and does not affect the requirement, i.e., "DECAs" replaces "BDBAs".</p> <p>Bruce B continued the basic design of the Bruce A station (see Section 1.3.2, of Part 1 of the Safety Report [NK29-SR-01320-00001, R005]).</p> <p>When Bruce A and Bruce B were originally built the only combinations of events considered in the licensing basis were the dual failures of a process system and a safety system. The type of dual PIEs resulting in AOOs or accident conditions were not considered in the original licensing basis. Recent Safety Report updates have considered many more dual failures, and these types of events have been included in the PSA. In all of the Bruce B accident analysis, causal effects of the initiating PIE have always been included in the accident scenario.</p> <p>Bruce Power is implementing a Safety Report Improvement Program starting in 2014 including annual status and progress updates to the CNSC staff as committed in Bruce Power letter from F. Saunders to R. Lojk, Action Item 090739: Safety Report Improvement Plan for Bruce A and Bruce B, File:NK21-CORR-00531-10774 &amp; NK21-CORR-</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	occurrence.	00531-11155.	
7.5	<p>The design authority shall specify the engineering design rules for all SSCs. These rules shall comply with appropriate accepted engineering practices.</p> <p>The design shall also identify SSCs to which design limits are applicable. These design limits shall be specified for operational states, DBAs and DECAs.</p> <p>Guidance</p> <p>Methods to ensure a robust design are applied, and proven engineering practices are adhered to in the design, as a way to ensure that the fundamental safety functions would be achieved in all operational states, DBAs and DECAs.</p> <p>The engineering design rules for all SSCs should be determined based on their importance to safety, as determined using the criteria in section 7.1. The design rules should include, as applicable:</p> <ul style="list-style-type: none"> <li>identified codes and standards</li> </ul>	<p>A new requirement for design limits related to DECAs is introduced in the second paragraph.</p> <p>Bruce B continued the basic design of the Bruce A station (see Section 1.3.2, of Part 1 of the Safety Report [NK29-SR-01320-00001, R005]). All of the SSCs important to safety have been in place at Bruce A (and B) reactors for 30 years. They were originally designed based upon experience gained from earlier plants (NPD, Douglas Point, Pickering A). Design changes over the years have been based upon design improvements (e.g., in-core detector assemblies) that have been tested and proven elsewhere.</p> <p>All future design changes will be in accordance with BP-PROG-10.01, Plant Design Basis Management, which governs BP- PROC-00335, Design Management, the latter of which interfaces with the implementing procedures of BP-PROG-10.02, Engineering Change Control. For example, BP- PROC-00539, Design Change Package "specifies the control of modifications to plant systems, structures, components... to meet regulatory requirements, ensure safety..."</p> <p>The Plant Design Basis Management Program, BP-PROG-10.01, ensures that the plant design meets safety, reliability and regulatory requirements. BP-PROC-00363, "Nuclear Safety Assessment", is an implementing procedure under this program which takes into account the effects of ageing.</p> <p>The Nuclear Safety Assessment process ensures that all necessary nuclear safety requirements are defined for the actual or proposed design of the plant throughout the design</p>	Gap



Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>conservative safety margins</li> <li>reliability and availability:</li> <li>material selection</li> <li>single-failure criterion</li> <li>redundancy</li> <li>separation</li> <li>diversity</li> <li>independence</li> <li>fail-safe design</li> <li>equipment qualification:</li> <li>environmental qualification</li> <li>seismic qualification</li> <li>qualification against electromagnetic interference</li> <li>operational considerations:</li> <li>testability</li> <li>inspectability</li> <li>maintainability</li> <li>aging management</li> <li>management system</li> </ul> <p>The design of complementary design features</p>	<p>modification process or in addressing emergent issues (e.g., plant ageing) that may affect the Design Basis or the Safety Report Basis.</p> <p>The current design documentation does not list design limits for DEC's; hence this is identified as a gap (Gap).</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>should be such that they are effective for fulfilling the actions credited in the safety analysis, with a reasonable degree of confidence. Other SSCs that are credited for DEC's should also meet this expectation.</p> <p>Design rules should include relevant national and international codes and standards. In cases of SSCs for which there are no appropriate established codes or standards, an approach derived from existing codes or standards for similar SSCs may be applied; in the absence of such codes and standards, the results of experience, tests, analysis or a combination of these may be applied, and this approach should be justified.</p> <p>A set of design limits consistent with the key physical parameters for each SSC important to safety for the nuclear power plant should be specified for all operational states, DBAs and DEC's. The design limits specified are consistent with relevant national and international codes and standards.</p>		
7.6	All SSCs important to safety shall be designed with sufficient quality and reliability to meet the design limits. A reliability analysis shall be performed for each of these SSCs.	<p>There are no changes to the requirements in this clause.</p> <p>As described in section 6.1.1 of Part 2 of Safety Report [NK29-SR-01320-00001, Rev. 005] to provide a high degree of assurance that a special safety system will perform as designed when called upon to do so, the unavailability target</p>	AD

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Where possible, the design shall provide for testing to demonstrate that the reliability requirements will be met during operation.</p> <p>The safety systems and their support systems shall be designed to ensure that the probability of a safety system failure on demand from all causes is lower than 1E-3.</p> <p>The reliability model for each system may use realistic failure criteria and best-estimate failure rates, considering the anticipated demand on the system from PIEs.</p> <p>Design for reliability shall take account of mission times for SSCs important to safety.</p> <p>The design shall take into account the availability of offsite services upon which the safety of the plant and protection of the public may depend, such as the electricity supply and external emergency response services.</p> <p>Guidance</p>	<p>of each is limited to less than 1E-3 year/year. In addition, reliability requirements for the special safety systems have always been an integral part of the Canadian licensing process and demonstration that the station meets them on an ongoing basis are imposed as operating license conditions. The requirements are to have an unavailability of less than 1E-3 years/year. While these mandated requirements are limited to the special safety systems, the safety support systems have been designed with the requisite reliability or redundancy to ensure that the special safety systems meet their requirements. Generally, this has been chosen as an unavailability of less than 1E-2 years/year.</p> <p>Bruce B uses the reliability program described in BP-PROG-11.01 [R005, December 16, 2015] and in the hierarchy of its implementing procedures (listed in Appendix B of BP-PROG-11.01). The implementing procedures deal with scoping and identification of Critical SSCs, continuing equipment reliability improvement, preventive maintenance implementation, performance monitoring, equipment reliability problem identification and resolution, long-term planning and life-cycle management.</p> <p>The decision methodology described in DPT-RS-00012 determines which plant systems meet the criteria of 'Systems Important to Safety' (SIS). This identification incorporates the use of probabilistic unavailability models of SIS. The ongoing record of reliability of SIS is documented in Bruce B Annual Reliability Reports. The 2015 Bruce B Annual Reliability Report NK29-REP-09051.1-00016 [Enclosure 1 to Letter F. Saunders to K. Larfreniere, NK29-CORR-00531-13197, April 28, 2016] contains detailed results on the Bruce B systems that comprise the SIS list. Quantitative unavailability models</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design for reliability is based on meeting applicable regulatory requirements and industry standards. The design should provide assurance that the requirements of CNSC RD/GD-98, Reliability Programs for Nuclear Power Plants, will be met during operation. Not all SSCs important to safety identified in the design phase will necessarily be included in the reliability program.</p> <p>The following principles are applied for SSCs important to safety:</p> <ul style="list-style-type: none"> <li>the plant is designed, constructed, and operated in a manner that is consistent with the assumptions and risk importance of these SSCs</li> <li>these SSCs do not degrade to an unacceptable level during plant operations</li> <li>the frequency of transients posing challenges to SSCs is minimized</li> <li>these SSCs function reliably when challenged</li> </ul> <p>The reliability of SSCs assumed in the design stage needs to be realistic and achievable.</p> <p>Deterministic analysis or other methods may be used if the PSA lacks effective models or data to</p>	<p>exist for nine of these systems; for others, CANDU Owner's Group guidance COG-05-9011 is followed, where the applicable initiating events frequencies are used as system monitoring parameters.</p> <p>As per guidance provided by CNSC RD/GD-98, the resulting unavailabilities are assessed against their respective targets. The unavailability targets for the SIS were set out based on their design and operational requirements, per Section 2.3.2 of the COG guidance document COG-05-9011. As shown in the Bruce B Annual Reliability Report 2015 [NK29-REP-09051.1-00016] out of the nine SIS for which there are unavailability models, only five have the unavailability target of 1E-03. The Bruce Power's unavailability targets for the other four SIS are higher. Namely, the target for the Standby Class 3 Power System is 4.0E-02, the target for the Heat Transport Pressure and Inventory Control System (HTPICS) is 4.0E-02, the target for the Emergency Water System (EWS) is 1.0E-02, and Emergency Power System (EPS) is also 1.0E-02.</p> <p>In 2015, none of the twelve Systems Important to Safety (SIS) exceeded their Bruce Power Predicted Future Unavailability (PFU) targets. According to the 2015 Annual Reliability Report [NK29-REP-09051.1-00016] Actual Past Unavailability (APU) was observed for four out of twelve Systems Important to Safety. The four systems were Emergency Coolant Injection System, Emergency Water System, Shutdown System One and Shutdown System Two. The APU for Emergency Water System was above its target. Events that caused the APU have been addressed through Bruce Power's corrective action process. The Negative Pressure Containment (NPC) System Predicted Future</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	evaluate the reliability of SSCs.	<p>Unavailability (PFU) met the target in 2015 and a decrease in the PFU was observed for all NPC parameters due to the update of the model with plant specific data for the reporting period.</p> <p>The calculated unavailabilities of four SIS are above the 1E-03 value required in this clause. These are: 1.999E-02 for HTPICS, 3.835E-02 for the Standby Class 3 Power System, 5.66E-03 for the EPS, and between 3.926E-03 and 9.801E-03 for the three EWS top events. However, since Bruce Power uses plant-specific unavailability targets in accordance with the COG guidelines COG-05-9011, this is considered as an acceptable deviation from the requirements of this clause.</p>	
7.6.1	<p>The potential for common-cause failures (CCFs) of items important to safety shall be considered in determining where to apply the principles of separation, diversity and independence so as to achieve the necessary reliability. Such failures could simultaneously affect a number of different items important to safety. The event or cause could be a design deficiency, a manufacturing deficiency, an operating or maintenance error, a natural phenomenon, a human-induced event, or an unintended cascading effect from any other operation or failure within the plant.</p> <p>Guidance</p> <p>Failure of a number of devices or components to perform their functions could occur as a result of a</p>	<p>There are no changes that affect the requirements in this clause.</p> <p>As described in section 1.1.5.2 of Part 2 of the Safety Report, Bruce B was intended to be as similar as possible in design the previously built Bruce A plant, to make use of the design and construction experience obtained at Bruce A. In addition to high quality standards, safety systems and functions are diverse and physically separated from process control functions. Redundant components are used where possible, so that the failure of a single component does not cause system failure. As stated in section 6.1.3 of Part 2 of the Safety Report, the special safety systems are designed and installed in accordance with the guidelines established to meet the Canadian licensing requirements and in addition, the requirements of the Bruce B Design Guides (e.g., Location and Separation Requirements for Safety Related Systems, NK29-DG-03650-5]. The plan systems are separated into two groups, Group 1 and Group 2 to provide</p>	C



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>single specific event or cause. CCFs could also occur when multiple components of the same type fail at the same time. This could be caused by occurrences such as a change in ambient conditions, saturation of signals, repeated maintenance error or design deficiency.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>• United States Nuclear Regulatory Commission (U.S. NRC), NUREG/CR-7007, Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, Washington, D.C., 2010.</li> <li>• U.S. NRC, Branch Technical Position (BTP) 7-19, Guidance for Evaluation of Diversity and Defense-in-Depth and in Digital Computer-Based Instrumentation and Control Systems, Washington, D.C., 2007.</li> <li>• U.S. NRC, NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, Washington, D.C., 1994.</li> </ul>	<p>protection against common mode events. For example, the design considerations leading to full independence between the two shutdown systems as discussed in Part 2, Section 6.1.5 of the Safety Report [NK29-SR-01320-00001, R005] demonstrate compliance. The two shutdown systems, SDS1 and SDS2, are functionally and physically independent of each other and functionally independent of the reactor regulating system.</p> <p>Independence is achieved by employing diverse shutdown principles, i.e., SDS1 uses solid shutoff rods (gravity driven), and SDS2 directly injects poison into the moderator (pressurized injection).</p> <p>The systems are also geographically separated. The shutoff rods are inserted vertically into the top of the reactor. The poison injection tubes are inserted horizontally into the side of the reactor.</p> <p>Ancillary mechanical and process equipment is similarly separated. The shutoff rod drives are located above the reactor, whereas the poison supply system is located to the side of the reactor. The measurement elements for the two systems are physically separated as well.</p> <p>Separation of the instrumentation channels of the two systems is achieved by channelization. At Bruce B each of the three channels on a specific special safety system follows a separate route. This does not exclude that one of the triplicated channels on one special safety system may follow a common route with one of the associated triplicated channels of another special safety system, i.e., associated channels. Adequate separation is maintained with three different routes for three sets of associated channels.</p>	




Article No.	Clause Requirement	Assessment	Compliance Category
		<p>Channelization ensures that the three cable routes are separated, that the equipment associated with the three sets of channels is located in three different rooms, and that power to the three sets of channels is supplied by three different buses. Consequently, any credible local common mode event can affect only one set of channels, leaving the other two unimpaired and thus the special safety systems remain functional. More details are provided in the design guides DG-29-03650-5 and DG-29-57000-3.</p> <p>Each safety system's initiation logic is independent from each other and from process systems. SDS1 uses general coincidence logic, whereas SDS2 uses local coincidence logic to increase diversity.</p> <p>The safety support systems use the same principles of separation, diversity and redundancy.</p>	
7.6.1.1	<p>The design shall provide sufficient physical separation between:</p> <ol style="list-style-type: none"> <li>1. redundant divisions of a safety system</li> <li>2. redundant divisions of a safety support system</li> <li>3. a safety support system and a process system</li> </ol> <p>This shall apply to equipment and to the routing of items, including:</p>	<p>There are no changes in this clause that might impact the intent of the requirement.</p> <p>As discussed in Part 2, Section 6.1.2 of the Safety Report [NK29-SR-01320-00001] this requirement is addressed in the design. Each process and nuclear measurement loop that is essential for the operation of a special safety system is designed to be redundant (duplicated or triplicated), such that a single loop component or power supply failure cannot incapacitate a special safety system or spuriously invoke its operation. The design approach emphasizes both, segregation between channels and between different special safety systems.</p> <p>Selected redundant equipment and their control systems/supplies are arranged in separated areas to</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>1. electrical cables for power and control of equipment</p> <p>2. piping for service water for the cooling of fuel and process equipment</p> <p>3. tubing and piping for compressed air or hydraulic drives for control equipment</p> <p>Where physical separation by horizontal distance alone may not be sufficient for some CCFs (such as flooding), vertical separation or other protection shall be provided.</p> <p>Where physical separation is not possible, safety support system equipment may share physical space. In such cases, the reasons for the lack of separation and justification for the space sharing arrangement shall be explained in the design documentation.</p> <p>Where space sharing is necessary, services for safety systems and for other process systems important to safety shall be arranged in a manner that incorporates the following considerations:</p>	<p>minimize the probability of common accidents affecting all systems.</p> <p>The Location and Separation Requirements for Safety Related Systems Design Guide [NK29-DG-03650-5] establishes the minimum requirements for safety related systems in order to meet the separation philosophy associated with common mode events. As indicated in section 6.1.3 of Part 2 of the Safety Report, the safety systems are designed and installed in accordance with the requirements established in the Bruce B Design Guides as follows:</p> <p>" DG-29-03650-1: Purpose and Application of Safety System Design Guides.</p> <p>" DG-29-03650-2: Seismic Qualification of Safety Related Systems.</p> <p>" DG-29-03650-3: Environmental Qualification of Safety Related Equipment.</p> <p>" DG-29-03650-5: Location and Separation Requirements for Safety Related Systems.</p> <p>" DG-29-03650-6: Containment Provisions for Extensions of the Containment Envelope.</p> <p>These design guides also apply to various other safety related systems.</p> <p>For example the design consideration leading to full independence between the two shutdown systems are presented in section 6.1.5 of Part 2 of the Safety Report. The two shutdown systems, SDS1 and SDS2, are functionally and physically. Independent of each other and functionally</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>1. A safety system designed to act as backup shall not be located in the same space as the primary safety system.</p> <p>2. If a safety system and a process system must share space, then the associated safety functions shall also be provided by another safety system in order to counter the possibility of failures in the process system.</p> <p>The design shall provide effective protection against common-cause events where sufficient physical separation among individual services or groups of services does not exist. The design authority shall assess the effectiveness of specified physical separation or protective measures against common-cause events.</p> <p>Guidance</p> <p>Physical separation may be achieved by barriers, distance (both horizontal and vertical) or a combination of the two. For example, the design may provide elevation differences of redundant equipment to protect against flooding.</p>	<p>independent of the reactor regulating system. Independence is achieved employing different shutdown principles: SDS1 uses solid shutoff rods, and SDS2 direct poison injection into the moderator. Beyond this, the systems are also geographically separated. The shutoff rods are inserted vertically into the top of the reactor. The poison injection tubes are inserted horizontally into the side of the reactor. Ancillary mechanical and process equipment is similarly separated. The shutoff rod drives are located above the reactor, whereas the poison supply system is located to the side of the reactor. The measurement elements for the two systems are physically separated as well. Separation of the instrumentation channels of the two systems is achieved by channelization. The channelization approach for Bruce B is such that each of the three channels on a specific special safety system follow a separate route. This does not exclude that one of the triplicated channels on one special safety system may follow a common route with one of the triplicated channels of another special safety system. Such channels are referred to as associated channels. Adequate separation is maintained with three different routes for three sets of associated channels. This means, for example, that Channel D of SDS1 and Channel G of SDS2 may follow a common route. Similarly, Channels E and H may follow a common route but separate from Channels D and G, and so on. In addition to the separation achieved between the three routes, separation is also achieved between channels following a common route by routing the channels in separate cable pans. Further details are presented in DG-29-03650-5 and DG-29-57000-3. Channelization ensures that the three cable routes are separated, that the equipment associated with the three sets of channels is located in three different rooms, and that power to the three sets of channels is supplied by three</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>different buses. Consequently, any credible local common mode event can affect only one set of channels, leaving the other two unimpaired and thus the special safety systems remain functional.</p> <p>The systems subjected to a harsh environment following some design basis accidents are protected through environmental qualification of essential equipment. Bruce Power undertook an extensive program to retrofit such protection to essential equipment. As discussed in Section 2.6 of Part 2 of the Safety Report, the environmentally harsh conditions have been evaluated for all DBA categories considered and have been documented in the Room Conditions Manual [Bruce B Environmental Qualification Room Conditions Manual, B-STQ-03651-10001] ].</p> <p>The environmental qualification requirements are defined in the Design Guide Environmental Qualification of Safety Related Equipment [NK29-DG-03650-003]. The Bruce B Environmental Qualification Room Conditions Manual [B-STQ-0351-10001]. Provides the single approved source for the normal and accident environmental conditions for use in establishing and maintaining environmental qualification of station EQ equipment.</p> <p>The Environmental Qualification Safety Requirements Matrix [NK29-SRM-03651.04-00001, Rev. 001, June 2006] provides a list of Function Groups subject to EQ as well additional information and details associated with the plant level EQ requirements identified in the EQ Design Guide and other details used in the identification of the equipment safety related requirements. The document is used conjunction with the EQ DG and the EQIS Database. Together these documents establish an integrated and comprehensive set of</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>requirements that are used in the EQ process to provide assurance that essential equipment will function as required during design basis accidents, which result in harsh environments. This document also links the system functional requirements identified in the EQ DG and the equipment functional requirements documented and maintained in the EQIS Database EQ 12 Reports.</p> <p>The Bruce B design includes protection against common mode events as described in Section 2.5 and Section 2.6 of Part 2 of the Safety Report. This includes:</p> <ol style="list-style-type: none"> <li>1. Seismic Qualification</li> <li>2. Missile Protection</li> <li>3. Protection Against Dynamic Effects Associated with the Rupture of Piping</li> <li>4. Environmental Qualification of Safety-Related Equipment.</li> </ol> <p>A three-year Safety Report Improvement Project is undertaken to upgrade the Bruce A and B Safety Reports to align with an RD-310 framework (Note: REGDOC-2.4.1 superseded RD-310). Additionally a new Safety Report appendix on Common Mode Failures will be introduced into both the Bruce A and B Safety Reports. This new appendix will be structured as per the RD-310 framework, with new RD-310 compliant analyses.</p>	
7.6.1.2	Diversity shall be applied to redundant systems or components that perform the same safety function by incorporating different attributes into the systems or components. Such attributes shall	<p>There are no changes in the clauses that impact the intent of the requirement.</p> <p>As an example of the application of this principle, two different shutdown principles have been adopted in the</p>	IC

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>include different principles of operation, different physical variables, different conditions of operation, or production by different manufacturers.</p> <p>It is important that any diversity used achieves the desired increase in reliability. For example, to reduce the potential for a CCF, the application of diversity shall be examined for any similarity in materials, components, and manufacturing processes, or subtle similarities in operating principles or common support features. If diverse components or systems are used, there shall be a</p> <p>reasonable assurance that such additions are of overall benefit, taking into account associated disadvantages such as the extra complication in operational, maintenance, and test procedures, or the consequent use of equipment of lower reliability.</p> <p>Guidance</p> <p>The design should implement adequate diversity, such as:</p> <ul style="list-style-type: none"> <li>design diversity</li> </ul>	<p>design - SDS1 gravity drop shutoff rods (vertical) and SDS2 pressurized liquid poison injection into the moderator (horizontal). Additional details are presented of the Safety Report 6.1 of Part 2 of the Safety Report. The safety design philosophy is described in section 1 of Part 2 of the Safety Report.</p> <p>Redundant components are used where possible, so that the failure of a single component does not cause system failure. This leads to the use of 2 out of 3 voting logic, or channels, in many standby systems, which requires 2 of 3 separate instruments to fail before the system logic fails.</p> <p>This type of logic also permits on-power testing, channel by channel, without impairing the functionality of the system, and prevents spurious initiation of a system if one instrument or channel fails.</p> <p>Diversity of functions (e.g., process and neutronic measurements) for important control and safety systems is used such that a common fault in one type of component cannot cause complete failure of the function. To the extent possible, equipment is designed to fail safe on loss of electrical power (e.g., shutoff rods drop when power to their clutches is lost). Similarly, pneumatic instruments and components such as air-operated valves are designed to be fail-safe to the extent possible. Self-actuating devices are employed where possible.</p> <p>Since not all equipment can be designed to fail safe, power supply reliability is important. A graded system of grid-independent diverse power supplies is used, with separated, independent bus supplies to redundant components (this is discussed further in section 1.3.2.4 of Part 2 of the Safety</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>equipment diversity</li> <li>functional diversity</li> <li>human factor engineering diversity</li> </ul> <p>The design for I&amp;C systems should also consider:</p> <ul style="list-style-type: none"> <li>signal diversity</li> <li>software diversity</li> </ul> <p>For I&amp;C systems important to safety, it is recommended to use an automated diverse backup system. A manual diverse backup system could be used; its justification should include a human factor engineering analysis.</p> <p>The following diversity strategies should be considered:</p> <ul style="list-style-type: none"> <li>different technologies</li> <li>different approaches within the same technology</li> <li>different architectures within the same technology</li> </ul>	Report). Similarly, backup independent air is supplied for pneumatic equipment when necessary.	

Article No.	Clause Requirement	Assessment	Compliance Category
	A diversity and defence in depth analysis should be conducted, to assess design vulnerabilities to CCF. If the defence in depth analysis reveals that certain safety functions could be affected by CCF, the design should provide for a diverse backup system to perform the safety functions affected by the CCF.		
7.6.1.3	<p>Interference between safety systems or between redundant elements of a safety system shall be prevented by means such as electrical isolation, functional independence, and independence of information (e.g., data transfer), as appropriate.</p> <p>Guidance</p> <p>Means for providing independence include physical separation, functional independence and independence from the effects of data communication errors. Generally, a combination of these methods should be applied to achieve an acceptable level of independence.</p> <p>Functional independence (such as electrical isolation) should be used, in order to reduce the likelihood of adverse interaction between equipment and components of redundant or connected systems resulting from normal operation or failure of any component in the</p>	<p>This is a new requirement.</p> <p>As presented in Section 6.1.1 of the Bruce B Safety Report Part 2, to effectively reduce the risk presented by a postulated process system failure, special safety systems are independent of process systems, including the reactor regulating system, whose failure might require the subsequent action of the special safety system.</p> <p>To the greatest extent practicable, the special safety systems are also independent of each other in design and operation. This requirement evolves from the Canadian reactor safety principle of analyzing each postulated process system failure in conjunction with a failure of each of the special safety systems in turn. As an additional feature, credit is not taken for both shutdown systems acting together. The provision of two independent reactor shutdown systems permits the assumption that at least one will operate following any single process failure.</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>systems.</p> <p>SSCs important to safety should be independent of the effects of an event to which they are required to respond. For example, an event should not cause the failure or loss of a safety system or safety function that is necessary to mitigate the consequences of that event.</p> <p>Redundant portions of a safety group should be independent from each other, to ensure that the safety group can perform its safety function during (and following) any event that requires that function.</p> <p>The functional failure of the support features of a safety system should not compromise the independence between redundant portions of a safety system, or between a safety system and a system of lower safety classification.</p> <p>The potential for harmful interactions between those SSCs important to safety that might be required to operate simultaneously should be evaluated, and the effects of any harmful interactions should be prevented.</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	In the analysis of the potential for harmful interactions of SSCs important to safety, due account should be taken of physical interconnections, and of the possible effects of one system's operation, maloperation or malfunction on the local environmental conditions for other essential systems. This would ensure that changes in environmental conditions do not affect the reliability of systems or components while functioning as intended.		
7.6.2	<p>All safety groups shall function in the presence of a single failure. The single-failure criterion requires that each safety group can perform all safety functions required for a PIE in the presence of any single component failure, as well as:</p> <ol style="list-style-type: none"> <li>1. all failures caused by that single failure</li> <li>2. all identifiable but non-detectable failures, including those in the non-tested components</li> <li>3. all failures and spurious system actions that cause (or are caused by) the PIE</li> </ol> <p>Each safety group shall be able to perform the required safety functions under the worst permissible systems configuration, taking into</p>	<p>The requirements have been changed to include testing requirement for justification of exemptions to single failure criterion for passive components.</p> <p>A review of the same clause in RD-337 indicated that the Bruce A and B design does not fully meet this requirement, as documented in [NK21-CORR-00531-11005 / NK29-CORR-00531-11397]. The application of the single failure criterion for the Bruce A and B design reflects the interpretation of this criterion that was prevalent at that time, where licensing requirements imposed only that no single failure in the safety systems should impair their operation. This does not follow the newer, more restrictive, interpretations of the single failure criterion; therefore is assessed as a gap (Gap 1).</p> <p>As part of the Bruce 1&amp;2 Return to Service, a review of all the safety groups against the IAEA single failure criterion was performed, as documented in Enclosure 1 of [NK21-CORR-00531-04342]. The review resulted in identification of three design changes required for the Bruce A Units 1&amp;2 ECI, QPS and the bleed condenser relief valves. The application of the</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>account such considerations as maintenance, testing, inspection and repair, and equipment outage.</p> <p>Analysis of all possible single failures, and all associated consequential failures, shall be conducted for each component of each safety group until all safety groups have been considered.</p> <p>Unintended actions and failure of passive components shall be considered as two of the modes of failure of a safety group.</p> <p>The single failure shall be assumed to occur prior to the PIE, or at any time during the mission time for which the safety group is required to function following the PIE. Passive components may be exempt from this requirement.</p> <p>Exceptions to the single-failure criterion shall be infrequent, and clearly justified.</p> <p>Exemptions for passive components may be applied only to those components that are designed and manufactured to high standards of quality, that are adequately inspected and</p>	<p>IAEA Single Failure Criterion for Non-Detectable Identifiable Failures was also assessed, and is documented in [NK21-CORR-00531-05360]. All additional potential singleton effects that were extracted from the Bruce A PRA arising from non-detectable identified failures were evaluated and there were no additional singletons of concern. However, for Bruce B design there is no systematic analysis of all possible single failures, and all associated consequential failures, conducted for each component of each safety group as required in this clause. Therefore, this is assessed as a gap (Gap 2).</p> <p>A review of the same clauses in a draft version of RD-337 indicated that for passive parts of some of the safety systems, for example piping where there are no duplicate paths, grade level storage tank or dousing tank where there is only one tank, vacuum building seals, etc., inspection programs are in place to ensure structural integrity of these components. The water filled ECI system piping, for example, is under a small but continuous pressure and is routinely inspected for leakage. Similarly, leakage recovery systems are inspected rather than tested.</p> <p>For other passive components (e.g., pressure vessels) they are usually excluded on the basis that they have been designed, fabricated and operated within the nuclear requirements of the applicable engineering code and other requirements as the CNSC may deem appropriate. In-service and periodic inspection programs including those acceptable to the CNSC provide assurance that the likelihood of in-service degradation that will lead to leaks has not increased since the plant was placed into service. Such leaks will be detectable at normal operating pressure and will occur sufficiently well in advance of the critical crack length being</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>maintained in service, and that remain unaffected by the PIE. Design documentation shall include justification</p> <p>of such exemptions, by analysis, testing or a combination of analysis and testing. The justification shall take loads and environmental conditions into account, as well as the total period of time</p> <p>after the PIE for which the functioning of the component is necessary.</p> <p>Check valves shall be considered to be active components if they must change state following a PIE.</p> <p>Guidance</p> <p>The application of the single-failure criterion (SFC) in design should follow a systematic approach applied to all safety groups. The approach should be adequately verified, such as by using failure modes and effects analysis. The SSCs inside the safety group should include both the primary SSCs and the supporting SSCs.</p> <p>The detectability of failures is implicit in the application of the SFC. Detectability is a function</p>	<p>reached that a break will not occur. In addition, there are available reliable systems to detect the presence of a leak. Appropriate operating procedures have been developed describing action to be taken following detection of a leak. The piping and vessels of concern meet the design requirements and in-service inspections and procedures are in place at Bruce B.</p> <p>As discussed in Part 2, Section 1.3.2.2 of the Safety Report, pressure boundary piping is monitored periodically using non-destructive inspection techniques to assure that the likelihood of a pipe failure is kept low. Additionally, a system of testing components in standby safety systems is in place to monitor component reliability and to continuously compare system reliability against established requirements. This testing program applies to systems that contribute to both accident prevention (e.g., shutdown systems and standby electrical systems) and accident mitigation.</p> <p>The special safety systems and standby safety support systems are tested on a regular basis to ensure that they will be available to operate if called on. The systems are designed to facilitate testing of all components, either as a system or in a series of overlapping component tests. Test frequencies are established to ensure that the systems meet defined reliability requirements. By testing the components of these systems at known frequencies, the actual availability can be monitored and compared against the expectation.</p> <p>System reliability models were developed and used during the design of the plant to confirm that the systems would meet their system reliability requirements. The models predict component failure rates and proposed test frequencies to</p>	




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>of the system design and the specified tests. A failure that cannot be detected through periodic testing, or revealed by alarm or anomalous indication, is non-detectable. An objective in a single- failure analysis is to identify non-detectable failures. To deal with identifiable but non-detectable failures, the following actions should be considered:</p> <ul style="list-style-type: none"> <li>• preferred action: the system or the test scheme should be redesigned to make the failure detectable</li> <li>• alternative action: when analyzing the effect of each single failure, all identified non-detectable failures should be assumed to have occurred. Therefore, the design should take appropriate measures to address these non-detectable failures, such as adequate redundancy and diversity</li> </ul> <p>Justification in support of an exception to the SFC should consider the consequences of failure, practicality of alternatives, added complexity and operational considerations. The integrated effect of all exceptions should not significantly degrade safety; in particular, defence in depth should be preserved.</p> <p>For passive components that are exempt from the</p>	<p>arrive at predicted system reliability.</p> <p>During operation, component fault data is collected as part of the test program, and predicted future unavailability is recalculated on an ongoing basis, using this actual component experience.</p> <p>Standby safety support systems, such as the standby emergency generators, are also tested regularly so that the system reliability can be tracked. As described in section 1.3.3 of Part 2 of the Safety Report, rigorous, comprehensive, and increasingly accurate accident analysis is used initially to design the safety systems and later, during the final licensing process, to assess the response of the plant and the capability of the safety systems following a wide range of postulated accidents.</p> <p>Bruce Power is implementing a Safety Report Improvement Program starting in 2014 including annual status and progress updates to the CNSC staff as documented in Bruce Power letter from F. Saunders to R. Lojk, Action Item 090739: Safety Report Improvement Plan for Bruce A and Bruce B, dated November 20, 2013, File:NK21-CORR-00531-10774 and NK21-CORR-00531-11155.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>SFC, the following should be considered in order to demonstrate a high degree of performance assurance:</p> <ul style="list-style-type: none"> <li>adequate testing during the manufacturing stage</li> <li>sample testing from those components received from the manufacturer</li> <li>adequate testing during construction and commissioning stages</li> <li>necessary testing to verify their reliability after the components have been removed from service during the operation stage</li> </ul> <p>Any consideration for an exception to the SFC during testing and maintenance should fall into one of the following permissible categories:</p> <ul style="list-style-type: none"> <li>the safety function is provided by two redundant, independent systems (e.g., two redundant, fully effective, independent cooling means)</li> <li>the expected duration of testing and maintenance is shorter than the time available before the function is required following an initiating event (e.g., spent fuel storage pool cooling)</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>the loss of safety function is partial and unlikely to lead to significant increase in risk even in the event of failure (e.g., small area containment isolation)</li> <li>the loss of system redundancy has minor safety significance (e.g., control room air filtering)</li> <li>the loss of system redundancy may slightly increase PIE frequency, but does not impact accident progression (e.g., leak detection)</li> </ul> <p>A request for an exception during testing and maintenance should also be supported by a satisfactory reliability argument covering the allowable outage time.</p> <p>The OLCs should clearly state the allowable testing and maintenance time, along with any additional operational restrictions, such as suspension of additional testing or maintenance on a backup system for the duration of the exception.</p> <p>Additional information</p> <p>Additional information may be found in:</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>IAEA, Safety Series No. 50-P-1, Application of the Single Failure Criterion, Vienna, 1990.</li> <li>Institute of Electrical and Electronics Engineers (IEEE), Standard 379, Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems, Piscataway, New Jersey, 1988.</li> </ul>		
7.6.3	<p>The concept of fail-safe design shall be incorporated, as appropriate, into the design of systems and components important to safety. To the greatest extent practicable, the application of this principle shall enable plant systems to pass into a safe state if a system or component fails, with no necessity for any action to be taken.</p> <p>Guidance</p> <p>Knowing the failure modes of SSCs is important in applying the fail-safe concept to SSCs important to safety. An analysis, such as a failure modes and effects analysis, should be performed so as to identify the potential failure modes of SSCs important to safety.</p> <p>Failures of SSCs important to safety should be detectable by periodic testing, or revealed by</p>	<p>There are no changes to this requirement.</p> <p>As presented in Section 6.1.1 of Part 2 of the Safety Report, to provide a high degree of assurance that a special safety system will perform as designed when called upon to do so, the unavailability target of each is limited to less than 1E-3 yr/yr. In addition, where such choice is available, special safety system components are designed such that the most likely failure modes are in the failsafe direction. It is recognized that in the original design this approach has been followed to the extent practicable. Since there are exceptions to this design rule (e.g., as documented in Design Guide Supplements NK29-DGS-29-03650-003, NK29-DGS-29-03650-004, NK29-DGS-29-03650-004-007 etc.) this is assessed as a gap (Gap).</p> <p>As discussed in Section 1.3.2.3 of Part 2 of the Safety Report, diversity of functions (e.g., process and neutronic measurements) for important control and safety systems is used such that a common fault in one type of component cannot cause complete failure of the function. To the extent possible, equipment is designed to fail safe on loss of electrical power (e.g., shutoff rods drop when power to their clutches is lost). Similarly, pneumatic instruments and</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	alarms or another reliable indication.	components such as air-operated valves are designed to be fail-safe to the extent possible. Self-actuating devices are employed where possible.	
7.6.4	<p>The design shall include provisions for adequate redundancy, reliability, and effectiveness, to allow for online maintenance and online testing of systems important to safety, except where these activities are not possible due to access control restrictions.</p> <p>The design shall take into account the time allowed for each equipment outage and the respective response actions.</p> <p>Guidance</p> <p>If the design does not allow online maintenance or online testing for certain equipment, the design should adequately demonstrate that the equipment can maintain its reliability target between outages.</p> <p>The time allowed for each equipment outage and the respective response actions should be specified in the OLCs.</p>	<p>There is no change in the requirements.</p> <p>To provide a high degree of assurance that a special safety system will perform as designed when called upon to do so, the unavailability target of each is limited to less than 1E-3 years/year. In addition, where such choice is available, special safety system components are designed such that the most likely failure modes are in the fail-safe direction.</p> <p>As established in Section 1.1.3 and Section 6.1.1 of Part 2 of the Safety Report the unavailability target of special safety systems is limited to less than 1E-3 years/year. In addition, as discussed above, as far as practicable, special safety system components are designed such that the most likely failure modes are in the fail-safe direction. Numerous Safety System Tests (SSTs) have been devised to ensure that the systems meet these requirements. The systems use triplicated instrumentation logic to allow on-line maintenance and testing so that when testing of one parameter/channel is required, that parameter/channel is failed safe such that it is already "voting" for system actuation. If a redundant valve has to be tested, then the valve is taken out of service and the logic becomes one-out-of two while the valve is out of service. The reliability models for these systems take into account the testing frequency and the effect of the test on the component availability and its impact on system. For maintenance, the channel is tripped when equipment is being repaired.</p> <p>A similar situation exists on other systems that do not have</p>	IC

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>formal regulatory reliability requirements, and the same principles for testing and maintenance are employed. These systems must be similarly reliable (typically 1E-2 a/a) as specified in the system design and must be tested to demonstrate that the requirement is being met. In no case is the overall system function degraded below the minimum credited in the Safety Report when equipment is out of service for testing or repair. A maintenance outage allowance is built into the risk and reliability models for the Standby Generators.</p> <p>The plant operating instructions in general do not include within them an allowable time for maintenance of equipment. The plant staff makes a case-by-case assessment of how long the station can run without testing to avoid increasing the unavailability. The exception to this is the standby generators where allowed outage times are factored into their reliability calculations. The intent of the requirement is therefore met.</p>	
7.6.5	<p>In cases where a system performs both process functions and safety functions, the following design requirements shall apply:</p> <ol style="list-style-type: none"> <li>the process and safety functions are not required or credited at the same time</li> <li>if the process function is operating, and a PIE in that system is postulated, it can be shown that all essential safety functions of the system that</li> </ol>	<p>There are no changes in the requirements.</p> <p>As stated in Bruce B Safety Report, safety systems and functions are diverse and physically separated from process control functions. Redundant components are used where possible, so that the failure of a single component does not cause system failure. This leads to the use of 2 out of 3 voting logic, or channels, in many standby systems, which requires 2 of 3 separate instruments to fail before the system logic fails. This type of logic also permits on power testing, channel by channel, without impairing the functionality of the system and prevents spurious initiation of a system if one instrument or channel fails. Also, diversity of functions (e.g.,</p>	IC



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>are required to mitigate the PIE are unaffected</p> <p>3. the system is designed to the standards of the function of higher importance with respect to safety</p> <p>4. if the process function is used intermittently, then the availability of the safety function after each use, and its continued ability to meet requirements, can be demonstrated by testing</p> <p>5. the requirements for instrumentation sharing are met</p>	<p>process and neutronic measurements) for important control and safety systems is used, so that a common fault in one type of component cannot cause complete failure of the function. To the extent possible, equipment is designed to fail safe on loss of electrical power (e.g., shutoff rods drop when they lose power to their clutches). Similarly, pneumatic instruments and components such as air operated valves, are designed to be fail safe to the extent possible. Self-actuating devices are employed where possible.</p> <p>There is no sharing of safety and process systems. There is no instrumentation sharing between safety and process systems.</p>	
7.6.5.1	<p>Instrumentation shall not typically be shared between safety systems.</p> <p>Where justified, there may be sharing between a safety system and a non-safety system (such as a process or control system).</p> <p>The reliability and effectiveness of a safety system shall not be impaired by normal operation, by partial or complete failure in other systems, or by any cross-link generated by the proposed sharing.</p>	<p>The changes introduced in this clause are clarifications to the requirements. There are no new requirements introduced due to the modifications in the text.</p> <p>As discussed in Section 6.1.2 of Part 2 of the Safety Report each process and nuclear measurement loop that is essential for the operation of a special safety system is redundantly designed, usually triplicated, such that a single loop component of power supply failure will not incapacitate or spuriously invoke operation of the special safety system.</p> <p>Neither of the two shutdown systems shares equipment with process systems. None of the safety systems shares equipment. Bruce B does not share any instrumentation between safety and process systems so this part of the requirement does not apply.</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design shall include provisions to ensure that the sharing of instruments does not result in an increased frequency in demand on the safety system during operation.</p> <p>If the design includes sharing of instrumentation between a safety system and a non-safety system, then the following requirements shall apply:</p> <ol style="list-style-type: none"> <li>1. sharing shall be limited to the sensing devices and their pre-amplifiers or amplifiers as needed to get the signal to the point of processing</li> <li>2. the signal from each shared sensing device shall be electrically isolated so that a failure of a non-safety system cannot be propagated to a safety system</li> <li>3. an isolation device shall always be associated with the safety system and shall be classified and qualified accordingly</li> </ol>	<p>The channelized logic at Bruce B allows for testing of the instrumentation all the way from the sensing device to the actuating device. The majority of the systems are such that the physical equipment being actuated cannot be tested on line. For example, the SDS1 shutoff rods can, and are, dropped partially into the core to demonstrate that they are physically capable of moving. They are caught before actually entering the core to any significant degree so as not to induce unnecessary flux tilts. The SDS1 components are tested periodically to demonstrate availability. SDS1 detectors and logic can be tested at power without initiating system trips because two-out-of-three channels logic is used. Partial drop tests of the shutoff rods are done frequently and full drop tests when feasible (section 6.2.10 of Part 2 of the Safety Report).</p> <p>On the other hand, it is not possible to inject poison from SDS2 into the core during on-power testing. SDS2 components are tested periodically to demonstrate its availability. The tripping detectors and logic circuits can be tested, at power, without causing SDS2 to trip, since a full system trip requires 2 out of 3 channels to trip. The poison concentration is measured (one tank per week) and an integrated test of the whole system is performed once approximately every 3 years (section 6.3.9 of Part 2 of the Safety Report). Similarly ECI is tested up to the point of actually injecting water into the core. Full testing of the shutdown system capability is periodically carried out when entering planned shutdown.</p>	
7.6.5.2	SSCs important to safety shall typically not be shared between two or more reactors.	The change introduced in item 1 relates to the safety requirements during DEC's.	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>In exceptional cases when SSCs are shared between two or more reactors, such sharing shall exclude safety systems and turbine generator buildings that contain high-pressure steam and feedwater systems, unless this contributes to enhanced safety.</p> <p>If sharing of SSCs between reactors is arranged, then the following requirements shall apply:</p> <ol style="list-style-type: none"> <li>1. safety requirements shall be met for all reactors during operational states, DBAs and DEC's</li> <li>2. in the event of an accident involving one of the reactors, orderly shutdown, cool down, and removal of residual heat shall be achievable for the other reactor(s)</li> </ol> <p>When an NPP is under construction adjacent to an operating plant, and the sharing of SSCs between reactors has been justified, the availability of the SSCs and their capacity to meet all safety requirements for the operating units shall be assessed during the construction phase.</p>	<p>The early design philosophy used for the multi-unit stations in Canada was to share some of the systems that were important to safety. The ECI and Containment systems are shared among the four units. The four Class III standby generators, each of which is capable of supplying the safe shutdown needs of any two units, supply all four reactor units. For Bruce A the emergency boiler cooling system is common to all four units. In the event of an accident in one unit requiring the use of the ECI or the containment system, the other units will be shut down in a controlled and orderly manner. For Bruce B the emergency water system, containment and the turbine building are common to four units. The procedures and practices in place for the use of shared systems, the measures taken to strengthen those systems in dealing with common mode events, and over twenty five years of safe operation of the plant provides confidence that there is a very low risk to the public from this sharing.</p> <p>Bruce B design includes sharing of special safety systems between reactors without justification that such sharing contributed to enhanced safety as required in this clause. Therefore it is assessed as a design gap (Gap).</p> <p>This sharing of systems was factored into the reliability requirements of these systems and each has redundant components to ensure adequate reliability.</p> <p>The accident analyses and the PRA recognize the shared functions and have shown that the design is adequate to meet Bruce Power's safety goals and all of the regulatory requirements in Canada.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
7.7	<p>All pressure-retaining SSCs shall be protected against overpressure conditions, and shall be classified, designed, fabricated, erected, inspected, and tested in accordance with established standards. For DEC's, relief capacity shall be sufficient to provide reasonable confidence that pressure boundaries credited in severe accident management will not fail.</p> <p>All pressure-retaining SSCs of the reactor coolant system and auxiliaries shall be designed with an appropriate safety margin to ensure that the pressure boundary will not be breached, and that fuel design limits will not be exceeded in operational states, or DBA conditions.</p> <p>The design shall minimize the likelihood of flaws in pressure boundaries. This shall include timely detection of flaws in pressure boundaries important to safety.</p> <p>Unless otherwise justified, all pressure boundary SSCs shall be designed to withstand static and dynamic loads anticipated in operational states, and DBAs.</p> <p>SSC design shall include protection against postulated pipe ruptures, unless otherwise justified. The operation of pressure relief devices</p>	<p>The text in the first paragraph is modified to include the requirement for DEC's. Editorial changes have been made to streamline the text; however these changes do not impact the intent of the requirement.</p> <p>The Safety Report for Bruce B (NK29-SR-01320-00002, R005) includes a wide range of accidents that are considered to be AOO's, although no credit is taken for control system protective action. Since there is not a systematic analysis of the control system capability to cope with AOO's, no definitive statement can be made in regard to the compliance with the AOO section of this clause (Gap).</p> <p>As presented in clause 7.4.1, the requirements associated with pipe whip and jet impingement, were not fully addressed in the original design of Bruce B. Bruce Power has performed an assessment that considered the dynamic effects of pipe whip of large Heat Transport System (HIS) piping, and their potential consequences on nuclear safety. The assessment confirmed that the capability to control, cool and contain would not be significantly impaired by the postulated breaks in containment [NK21-CORR-00531-09435 / NK29-CORR-00531-10019]. Bruce A and B Action Item 1207-3509 was opened to track progress on this issue, and Bruce Power is working with the CANDU Industry in performing the requested probabilistic fracture mechanics calculations.</p> <p>All interfaces between systems with different design pressures have dual isolation to ensure that single failures in a high-pressure system will not result in the low-pressure system exceeding its design pressure. For example, there are dual isolation valves between the HTS and lower</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>shall not lead to significant radioactive releases from the plant.</p> <p>Where two fluid systems operating at different pressures are interconnected, failure of the interconnection shall be considered. Both systems shall either be designed to withstand the higher pressure, or provision shall be made so that the design pressure of the system operating at the lower pressure will not be exceeded.</p> <p>Adequate isolation shall be provided at the interfaces between the reactor coolant system and connecting systems operating at lower pressures, in order to prevent the overpressure of such systems and possible loss-of-coolant accidents. Consideration shall be given to the characteristics and importance of the isolation and its reliability targets. Isolation devices shall be either closed</p> <p>or close automatically on demand. The response time and speed of closure shall be in accordance with the acceptance criteria defined for postulated initiating events.</p> <p>All pressure boundary piping and vessels shall be separated from electrical and control systems to the greatest extent practicable.</p>	<p>pressure HPECI system (H<sub>2</sub>O injection valves outside containment, D<sub>2</sub>O isolation valves inside containment). In addition, there are dual check valves between the HPECI and the lower ECI recovery system. Thus, no single failure can result in the lower pressure system exceeding its design pressure. The reliability of isolation valves is factored into the overall system reliability for systems important for safety.</p> <p>Isolation valves are either closed or close automatically on demand as described in various sections throughout this document, and where credited, the safety analyses have shown that these valves close fast enough to ensure that acceptance criteria are met.</p> <p>The existing layout of Bruce B systems cannot be practically changed to meet the requirement for separation of all pressure boundary piping and vessels from electrical and control systems. The Bruce Power EQ Program [BP-PROC-00261, R005, November 07, 2012] was established to identify system functional requirements required to maintain the basic nuclear safety functions (i.e., Control, Cool, Contain and Monitor) following design basis accidents that result in harsh environments. Similar requirement is presented in Clause 8.3.2.</p> <p>For example, pressure tube leaks can be readily detected by monitoring the moisture content and pressure in the annular gas filled space between the pressure tube and calandria tube (Section 11.2.5.1 of Part 2 of the Safety Report). Section 1.3.2.2 of Part 2 of the Safety Report describes a comprehensive system for monitoring, inspection and testing to ensure ongoing integrity of mechanical components and reliability of equipment. This includes monitoring for leakage from systems to detect incipient failures before they occur,</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Pressure-retaining components whose failure will affect nuclear safety shall be designed to permit inspection of their pressure boundaries throughout the design life. If full inspection is not achievable, then it shall be augmented by indirect methods such as a program of surveillance of reference components. Leak detection is an acceptable method when the SSC is leak-before-break qualified.</p> <p>Guidance</p> <p>For the design of pressure-retaining systems and components, the design authority should ensure the selection of codes and standards is commensurate with the safety class and is adequate to provide confidence that plant failures are minimized. This is achieved by using industry standards - such as CSA N285, General requirements for pressure-retaining systems and components in CANDU nuclear power plants and ASME Boiler and Pressure Vessel Code - to meet the requirements of different classes of pressure-retaining systems, components, piping and their supports. Alternative codes and standards may be used if this would result in an equivalent or superior level of safety; justifications should be provided in such cases.</p>	<p>and a non-destructive periodic examination program for piping systems. In addition, the plant design permits access for periodic inspection of components as per N285.4 and N285.5 requirements.</p>	





Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design should make provisions to limit stresses and deformation of SSCs important to safety during and after PIEs. The list of PIEs should be comprehensive, and the loads generated by them should be included in the design analysis. The loads generated by these PIEs should be included in the stress analyses required by the design.</p> <p>REGDOC-2.5.2 requires the design to minimize the likelihood of flaws in pressure boundaries. For example, the reactor coolant pressure boundary should be designed with sufficient margin to ensure that, under all operating configurations, the material selected will behave in a non-brittle manner and minimize the probability of rapidly propagating fractures.</p> <p>The pressure boundary components in an NPP almost invariably contain process fluids at very high temperature and pressure. The design should take into account the location of high-energy lines in relation to SSCs important to safety, in order to limit or reduce pipe whip concerns. This includes consideration, where applicable, of items such as:</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>o components in the means of shutdown</li> <li>o main coolant pumps</li> <li>o headers</li> <li>o emergency core cooling system components</li> <li>o steam generators</li> <li>o steam lines</li> <li>o turbine</li> </ul> <p>Leak-before-break</p> <p>A qualified leak-before-break (LBB) system design will permit the design authority to optimize protective hardware - such as pipe whip restraints and jet impingement barriers - and to redesign pipe-connected components, their supports and their internals.</p> <p>A qualified LBB methodology should include the following:</p> <ul style="list-style-type: none"> <li>o LBB should be only applied to high-energy, ASME Code Class 1 or 2 piping or the equivalent. Applications to other high-energy piping may be performed based on an evaluation</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>of the proposed design and in-service inspection requirements.</p> <p>O No uncontrolled active degradation mechanism should exist in the piping system to be qualified for LBB.</p> <p>O An evaluation of phenomena such as water hammer, creep damage, flow accelerated corrosion and fatigue should be performed to cover the entire life of the high-energy piping systems. To demonstrate that water hammer is not a significant contributor to pipe rupture, reliance on historical frequencies of water hammer events in specific piping systems coupled with reviews of operating procedures and conditions may be used for this evaluation.</p> <p>O Leak detection methods for the reactor coolant should ensure that adequate detection margins exist for the postulated through-wall flaw used in the deterministic fracture mechanics evaluation. The margins should cover uncertainties in the determination of leakage from a piping system.</p> <p>O Stress analyses of the piping that is considered for LBB should be in accordance with the requirements of section III of the ASME code or equivalent.</p> <p>O The LBB evaluation should use design basis loads and, after construction, be updated to use the as-built piping configuration, as opposed</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>to the design configuration.</p> <p>O The methodology should take account of potential for degradation by erosion, corrosion, and erosion-cavitation due to unfavourable flow conditions and water chemistry.</p> <p>O The methodology should take account of material susceptibility to corrosion, the potential for high residual stresses, and environmental conditions that could lead to degradation by stress corrosion cracking.</p> <p>In addition, leak detection methods for the reactor coolant should be examined so as to ensure that adequate detection margins exist for the postulated through-wall flaw used in the deterministic fracture mechanics evaluation.</p> <p>Finite element methods</p> <p>The design authority customarily uses finite element methods to show that all of the pressure boundary components (both vessels and piping) meet the structural integrity requirements imposed by applicable design codes and standards. When finite element methods are used for design analyses covering all ASME (or equivalent) class components, the design authority should ensure that:</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>o finite element modelling and analysis assumptions are checked to make sure they are justified and conservative</li> <li>o finite element mesh is properly refined to account for geometric structural discontinuities with proper element shapes and aspect ratios</li> <li>o loads and boundary conditions are correct and properly applied in the finite element models</li> <li>o load combinations and scale factors applied to unit load cases conform to design or load specifications</li> <li>o linearized stress results, obtained from load combinations, are compared with ASME code (or equivalent) allowable limits</li> </ul>		
7.8	<p>The design shall include an equipment environmental qualification (EQ) program. Development and implementation of this program shall ensure that the following functions can be carried out:</p> <ol style="list-style-type: none"> <li>1. the reactor can be safely shut down and kept in a safe shutdown state during and following AOOs and DBAs</li> <li>2. residual heat can be removed from the reactor after shutdown, and also during and following</li> </ol>	<p>A new requirement for consideration of ageing effects due to service life is added, The text is modified as follows: "dose acceptance criteria" replaced "prescribed limits". This change does not impact the intent of the requirement.</p> <p>As discussed in Part 2, Section 2.6.1 of the Safety Report [NK29-SR-01320- 00001], essential SSCs provide a safety function in accordance with the design and licensing basis of the station and consistent with the assumptions and requirements in current accident analysis documented in Part 3 of the Safety Report. All design basis accidents (single and dual failure), with the potential to cause common mode equipment failures are considered. For each such accident, a reliable and qualified line of defence is provided to achieve</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>AOOs and DBAs</p> <p>3. potential for release of radioactive material from the plant can be limited, and the resulting dose to the public from AOOs and DBAs can be kept within the dose acceptance criteria</p> <p>4. post-accident conditions can be monitored to indicate whether the above functions are being carried out</p> <p>The environmental conditions to be accounted for shall include those expected during normal operation, and those arising from AOOs and DBAs. Operational data and applicable design assist</p> <p>analysis tools, such as the probabilistic safety assessment, shall be used to determine the envelope of environmental conditions.</p> <p>The equipment qualification program for SSCs important to safety shall include the consideration of aging effects due to service life.</p> <p>Equipment qualification shall also include</p>	<p>the basic nuclear safety functions, i.e., achieve and maintain reactor shutdown (Control), remove fuel heat (Cool), contain radioactive contamination (Contain) and monitor post-accident conditions (Monitor).</p> <p>The Environmental Qualification Program document [BP-PROC-00261, R005] establishes the authority for the EQ process at Bruce Power site. The EQ Process establishes an integrated and comprehensive set of requirements that provide assurance that credited essential equipment and components can perform their safety-related functions if exposed to harsh environmental conditions resulting from Design Basis Accidents, in accordance with the plant design and licensing basis and that this capability is preserved over the life of the plant (section 1.0 of BP-PROC-00261). The EQ Process is implemented in a manner consistent with the basis, assumptions and requirements in the safety analysis, licensing submittals, operating licenses, abnormal incident manuals and operating policies and principles. Use of assumptions or methodology that differ from those used in the safety analysis shall be clearly indicated as such and shall be subjected to the same review and approval process used for the safety analysis. For each DBA case determined to produce a harsh environment, a qualified line of defence shall be provided to achieve and maintain reactor shutdown, fuel heat removal, containment and post-accident monitoring. The basis for this analysis is documented by Reactor Safety Engineering in Design Guides (Environmental Qualification of Safety Related Equipment, NK29-DG-03650-003,R07) and Safety Requirements Matrix (Environmental Qualification Safety Requirements Matrix, NK29-SRM-03651.04-00001, Rev. 001, June 2006) documents (section 4.1.3 of BP-</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>consideration of any unusual environmental conditions that can reasonably be anticipated, and that could arise during normal operation or AOOs (such as periodic testing of the containment leak rate).</p> <p>Equipment and instrumentation credited to operate during DEC's shall be demonstrated, with reasonable confidence, to be capable of performing their intended safety function(s) under the expected environmental conditions. A justifiable extrapolation of equipment and instrumentation behaviour may be used to provide assurance of operability, and is typically based on design specifications, environmental qualification testing, or other considerations.</p> <p>Guidance</p> <p>The designer should provide detailed processes and specifications for an equipment EQ program, for qualifying safety-related equipment associated with systems that are essential to perform the credited safety functions. The EQ program should address qualification criteria and methods used, and all anticipated environmental conditions upon which the qualification of the equipment (mechanical, electrical, I&amp;C and certain post</p>	<p>PROC-00261)..</p> <p>The EQ process described in BP-PROC-00261 supports the Design Management procedure BP-PROC-00335 and provides assurance that credited essential equipment and components can perform their safety-related functions if exposed to harsh environmental conditions resulting from Design Basis Accidents, in accordance with the plant design and licensing basis and that this capability is preserved over the life of the plant. Ageing mechanisms considered in the process include thermal ageing, radiation ageing and cyclic ageing. The general steps of the EQ process are described in Part 2, Section 2.6.3 of the Safety Report.</p> <p>A review of the same clause in RD-337 [NK21-CORR-00531-11005 / NK29-CORR-00531-11397] indicated that survivability of instrumentation during severe accident conditions was not formally assessed as part of the Bruce Power SAMG Program. Note that practices associated with environmental and seismic qualification have been considered as part of the Fukushima related improvements [NK21-CORR-00531-12554 / NK29-CORR-00531-12979]. The current Bruce Power SAMG Program has been developed to address the possibility of a severe accident occurring on a single reactor unit operating initially at high power. Subsequent to the events that occurred at Fukushima and the resultant lessons learned, the COG SAMG Task Team has established an industry joint project, to review the original SAMG used at Canadian NPPs and identify gaps or improvements.</p> <p>One of the outcomes of this this effort was to develop a COG generic methodology for evaluating instrumentation and equipment survivability for severe accident conditions</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>accident monitoring) is based.</p> <p>The designer should identify the EQ-related standards and codes (e.g., CSA, IEEE and ASME). The latest editions of the applicable standards for use in the equipment qualification are preferred; any deviations should be justified.</p> <p>As a minimum, the basic EQ program elements should be provided as described below.</p> <p>Identification of equipment requiring harsh environmental qualification</p> <p>The design should identify:</p> <ul style="list-style-type: none"> <li>• systems and equipment required to perform safety functions in a harsh environment, including their safety functions and applicable DBAs</li> <li>• non-safety-related equipment whose failure due to harsh post-accident environment could prevent safety-related equipment from accomplishing its safety function</li> <li>• accident monitoring equipment</li> </ul>	<p>["Methodology for Performing Instrument and Equipment Survivability Assessments in CANDU Nuclear Generating Stations", COG-JP-4426-004]. Following the issuance of the generic methodologies for instrument and equipment survivability and control facility habitability, a Bruce Power specific Instrument and Equipment (I&amp;E) survivability assessment has been completed and documented in Fukushima Action Item (FAI) 1.8.1 "Bruce Power Severe Accident Management Guidance Instrument and Equipment Survivability - Summary Report" [Enclosure 2, NK21 -CORR-00531-11801 / NK29-CORR-00531-12195]. This assessment provides a reasonable level of confidence that the I&amp;E essential to manage BDBAs and severe accidents will perform its function in the accident and post-accident environment. The approach used optimizes the assessment process by focusing on the essential Severe Accident Management Guidance (SAMG) parameters and strategies and building upon existing Environmental Qualification (EQ) work, Level 2 Probabilistic Risk Assessments (PRAs), SAMG programs and BDBA provisions including the use of Emergency Mitigation Equipment (EME). As indicated in the latest Fukushima update from February 2016, FAI 1.8.1 was closed by the CNSC (see Attachment A [NK21-CORR-00531-12554 / NK29-CORR-00531-12979]).</p> <p>The instrument and equipment survivability report includes various recommendations to enhance EME response and SAMG at Bruce A and B. These items have been dispositioned, with some follow-up actions to update the SAMGs and assess options to environmentally qualify the moderator level transmitters. The results of the habitability report indicate that Bruce Power's installed and planned upgrades are sufficient to terminate event progressing at, or</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Identification of equipment service conditions</p> <p>Service conditions should be identified to determine required qualification methods as they apply to various types of qualification (e.g., harsh environments, mild environments, radiation-only harsh environments).</p> <p>The design should provide for:</p> <ul style="list-style-type: none"> <li>• a distinction between mild and harsh environments (e.g., specific criteria to define plant environments as either mild or harsh)</li> <li>• a list of bounding harsh DBAs for qualification of equipment</li> <li>• the environmental conditions (e.g., temperature, pressure, radiation, humidity, steam, chemicals, submergence) for each applicable DBA to which equipment is exposed in various plant locations</li> <li>• temperature, pressure and radiation profiles for harsh environment qualification</li> <li>• typical equipment mission time during DBAs</li> <li>• mild environmental conditions (e.g.,</li> </ul>	<p>before, the early in-vessel retention stage, thereby supporting station habitability and providing reasonable confidence that essential operator actions can be completed in a timely manner. No further upgrades to address radiological habitability are warranted, per FAI 1.9.1 [NK21 -CORR-00531-11801 / NK29-CORR-00531-12195, January 30, 2015]. As indicated in the latest Fukushima update from February 2016, FAI 1.9.1 was closed by the CNSC (see Attachment A [NK21-CORR-00531-12554 / NK29-CORR-00531-12979]).</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>temperature, pressure, humidity, radiation) for operational states, including the assumed duration of the AOOs to which equipment is exposed in various plant locations</p> <p>Qualification methods</p> <p>The design should describe methods used to demonstrate the performance of safety-related equipment when subjected to a range of environmental conditions during operational states or DBAs. The methods should determine whether equipment should be qualified for mild or harsh environments.</p> <p>For harsh environment qualification, the design should include the following:</p> <ul style="list-style-type: none"> <li>For equipment and components located in a DBA harsh environment, type tests are the preferred method of qualification (particularly for electrical equipment) of qualification; where type tests are not feasible, justification by analysis or operating experience (or a combination of both) may be used.</li> <li>Equipment should be reviewed in terms of design, function, materials and environment, to identify significant aging mechanisms caused by</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>operational and environmental conditions occurring during normal operation. Where a significant aging mechanism is identified, that aging should be taken into account in the equipment qualification.</p> <ul style="list-style-type: none"> <li>The qualification should systematically address the sequence of age conditioning, including sequential, simultaneous, synergistic effects, and the method for accelerating radiation degradation effects.</li> <li>Appropriate margins, as given in EQ-related standards, should be applied to the specified environmental conditions.</li> <li>For certain equipment (e.g., digital I&amp;C equipment, and new advanced analog electronics) additional environmental conditions – such as electromagnetic interference, radio frequency interference, and power surges – should be addressed.</li> </ul> <p>For mild environment qualification, equipment may be considered qualified, provided that:</p> <ul style="list-style-type: none"> <li>the environmental conditions are specified in a design specification</li> <li>the manufacturer provides certification that the equipment meets the specification</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Equipment and instrumentation credited under design extension conditions</p> <p>A demonstration of equipment and instrumentation operability should include the following:</p> <ul style="list-style-type: none"> <li>the accident timeframes for each function</li> <li>the equipment type and location used to perform necessary functions in each timeframe</li> <li>the functions credited in the accident timeframes that need to be performed to achieve a safe shutdown state for DEC's</li> <li>the postulated harsh environment of DEC's within each timeframe</li> <li>a reasonable assurance that the equipment will survive to perform its function in the accident timeframes, in the DEC environment</li> </ul> <p>Protective barriers</p> <p>The design should address protective barriers, if applicable. When protective barriers are designed to isolate equipment from possible harsh environmental conditions, the barriers themselves</p>		




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>should be addressed in a qualification program. Examples of protective barriers include:</p> <ul style="list-style-type: none"> <li>• steam-protected rooms and enclosures</li> <li>• steam doors</li> <li>• water-protected rooms (for flooding)</li> </ul> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>• ASME, QME-1, Qualification of Active Mechanical Equipment Used in Nuclear Power Plants, New York, 2002.</li> <li>• CSA Group, N290.13, Environmental qualification of equipment for CANDU nuclear power plants, Toronto, Canada.</li> <li>• Electric Power Research Institute (ERPI), Technical Report rev. 1, Nuclear Power Plant Equipment Qualification Reference Manual, Palto Alto, California, 2010.</li> <li>• IAEA, Safety Reports Series No. 3, Equipment Qualification in Operational Nuclear Power Plants: Upgrading, Preserving and Reviewing, Vienna, 1998.</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>International Electrotechnical Commission (IEC), 60780 ed 2.0, Nuclear Power Plants - Electrical Equipment of the Safety System – Qualification, Geneva, 1998.</li> <li>IEEE, Standard 323, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, Piscataway, New Jersey, 2003.</li> <li>IEEE, Standard 627, Qualification of Equipment Used in Nuclear Facilities, Piscataway, New Jersey, 2010.</li> </ul>		
7.9.1	<p>The design shall include provision of instrumentation to monitor plant variables and systems over the respective ranges for operational states, DBAs and DEC's, in order to ensure that adequate information can be obtained on plant status.</p> <p>This shall include instrumentation for measuring variables that can affect the fission process, the integrity of the reactor core, the reactor cooling systems, and containment, as well as instrumentation for obtaining any plant information that is necessary for its reliable and safe operation.</p> <p>The design shall be such that the safety systems and any necessary support systems can be</p>	<p>The requirement in the first paragraph is extended to cover DEC's. The text is modified to include new requirements related to design provisions for testing; design provisions to facilitate maintenance, detection and diagnosis of failure, and actuation of safety systems.</p> <p>The Bruce B instrumentation and control design philosophy is summarized in the Safety Report (Part 2 Section 7.1.6). The instrumentation and control systems are designed to a large variety of detailed requirements, depending on their function, importance and physical environment. However, all the systems are designed to the following general criteria:</p> <ol style="list-style-type: none"> <li>The maximum practical amount of automatic control is incorporated in the design to allow the station to be operated safely with a minimum staff and to leave operators free for higher level monitoring of overall unit status. The operator can readily intervene in the operation of the automatic control systems.</li> <li>Adequate, comprehensive information is designed to</li> </ol>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>reliably and independently operated, either automatically or manually, when necessary.</p> <p>The design shall include provision for testing, including self-checking capabilities.</p> <p>The design shall provide for periodic testing of the entire channel of instrumentation logic, from sensing device to actuating device.</p> <p>The design shall facilitate maintenance, detection and diagnosis of failure, safe repair or replacement, and recalibration.</p> <p>The design shall also include the capability to trend and automatically record measurement of any derived variables that are important to safety.</p> <p>Instrumentation shall be adequate for measuring plant parameters for emergency response purposes.</p> <p>The design shall include reliable controls to maintain plant variables within specified operational ranges.</p>	<p>be readily available at all times to allow the operator to assess the status of the unit quickly and to intervene with manual actions if necessary.</p> <p>3. Equipment is designed for a minimum of regular maintenance. Any necessary maintenance operations are kept as simple and speedy as possible.</p> <p>4. The instrumentation and control systems are designed for a very high reliability and availability, both to maximize plant availability and for safety. This reliability is achieved through a combination of component selection and design, and through redundancy</p> <p>5. The control systems are designed to make the unit as tolerant as possible to expected and unexpected transients, in order to prevent unnecessary unit outages.</p> <p>6. Where possible, the control systems are designed to prevent or minimize damage to equipment.</p> <p>The Bruce B design meets the requirement for periodic testing of the entire channel of instrumentation logic. The channelized logic at Bruce B allows for testing of the instrumentation all the way from the sensing device to the actuating device. The majority of the systems are such that the physical equipment being actuated cannot be tested on line. For example, the SDS1 shutoff rods can, and are, dropped partially into the core to demonstrate that they are physically capable of moving. They are caught before actually entering the core to any significant degree so as not to induce unnecessary flux tilts. On the other hand, it is not possible to inject poison from SDS2 into the core during on-power testing. The SDS1 components are tested periodically to demonstrate availability. SDS1 detectors and logic can be</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions shall continue until completion.</p> <p>The design shall minimize the likelihood of operator action defeating the effectiveness of safety and control systems in normal operation and AOOs, without negating correct operator actions following a DBA.</p> <p>System control interlocks shall be designed to minimize the likelihood of inadvertent manual or automatic override, and to provide for situations when it is necessary to override interlocks to use equipment in a non-standard way.</p> <p>Various safety actions shall be automated so that operator action is not necessary within a justified period of time from the onset of AOOs or DBAs. In addition, appropriate information shall be available to the operator to confirm the safety action.</p> <p>Guidance</p> <p>Particular attention should be paid to the provision</p>	<p>tested at power without initiating system trips because two-out-of-three channels logic is used. Partial drop tests of the shutoff rods are done frequently and full drop tests when feasible (section 6.2.10 of Part 2 of the Safety Report).</p> <p>A general description of the design provisions are described in Section 7.1 of Part 2 of the Safety Report. Instrumentation and control is centered around a dual, digital computer system that is used on each unit for control, alarm annunciation, data display and data logging. Direct digital control is used for such functions as regulating reactor power, steam generator pressure and level, and the de-aerator level. The unit control and data acquisition computer systems are conceptually based on the successful systems used in previous stations. The system consists of two independent digital computers, DCC X and DCC Y with each computer being capable of controlling the unit.</p> <p>The system is organized so that maintenance on one computer can take place while the unit is being controlled by the other computer. A fault in any essential part of one computer results in automatic transfer of control to the other computer. In the event that both computers fail, the unit is automatically shut down. The shutdown is initiated through the action of independent Watchdog Timers (WDTs) associated with each computer. The action of the timers ensures that all computer analog and digital outputs are isolated from the plant and are forced to a fail-safe condition. This results in the dropping of the control absorbers and the filling of the natural water zone controllers. The high reliability of this dual computer control system results from combining reliable solid-state hardware with a self-checking system. Faults, either software or hardware, are detected by a</p>	

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>of start-up instrumentation for measuring variables that can affect the fission process, the integrity of the reactor core, the reactor cooling systems and containment, as well as instrumentation for obtaining any plant information that is necessary for reliable and safe operation.</p> <p>The monitoring should not be limited to process variables of safety and safety-related systems. It should include the monitoring of radiation, hydrogen, seismic, vibration, and as applicable, loose parts and fatigue.</p> <p>The measurements should include continuous and discrete plant variables. Detection and testing should also consider failure, degradation, unsafe conditions, and deviation from specified limits, operator errors, and self-diagnosis. Correction of invalid, inauthentic and corrupted functions or data should be applied, to maintain the reliability of systems.</p> <p>Once safety systems are initiated, the reset of safety system functions should require separate operator actions for each system-level function. Deliberate operator action should be required to return the safety systems to normal. However, this should not prevent the use of essential equipment protective devices (such as the protection for</p>	<p>combination of internal hardware and software self-checking. Their effects are mitigated by the independent WDT associated with the computer. Detection of a specified fault condition will result in control being relinquished by the computer in which the failure occurs. A restart system, which automatically reloads the core memory from a solid state reference memory and restarts the computer, combined with the fault detection routine, provide a system practically immune to transient faults. Each computer is connected to an independent 120 V (AC), Class II bus (section 7.1.1 of Part 2 of the Safety Report).</p> <p>Further details of computer fault protection are provided in Section 7.1.1.2 and the design basis is presented in Section 7.1.6 of Part 2 of the Safety Report. The control computer system is built on a modular basis, with large sections being replaceable. This simplifies fault diagnosis and reduces computer downtime.</p> <p>Each process and nuclear measurement loop that is essential for the operation of a special safety system is redundantly designed, usually triplicated, such that a single loop component or power supply failure will not incapacitate or spuriously invoke operation of the special safety system (Section 6.1.2 of Part 2 of the Safety Report).</p> <p>As discussed in Section 1.3.3, Part 2 of the Safety Report: The special safety systems and standby safety support</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>electrical or mechanical components) or the provision for deliberate operator interventions (such as trip and isolation of the switchgear). Seal-in of safety system actuation is generally required at system or subsystem level, but not required at individual channel level.</p> <p>The design should provide for the capability to record, store and display historical information, if such displays will help plant staff to identify patterns and trends, understand the past or current state of the system, perform post-accident analysis, or predict future progressions.</p> <p>The design should take into account redundancy, independence, common-cause failure, interaction with other systems, and signal validation, so as to meet the reliability target.</p> <p>When a safety system has been taken out of service for testing or maintenance, clear indication should be provided for the duration of testing or maintenance activities. For any safety systems being bypassed, the bypassed condition should also be clearly annunciated.</p> <p>If the use of a system for testing or maintenance can impair an I&amp;C function, the interfaces should</p>	<p>systems are tested on a regular basis to ensure that they will be available to operate if called on. The systems are designed to facilitate testing of all components, either as a system or in a series of overlapping component tests. Test frequencies are established to ensure that the systems meet defined reliability requirements.</p> <p>By testing the components of these systems at known frequencies, the actual availability can be monitored and compared against the expectation. System reliability models were developed and used during the design of the plant to confirm that the systems would meet their system reliability requirements. The models predict component failure rates and proposed test frequencies to arrive at predicted system reliability. During operation, component fault data is collected as part of the test program, and predicted future unavailability is recalculated on an ongoing basis, using this actual component experience.</p> <p>The safety systems are designed to activate automatically when required to do so. This equipment can also be activated manually if needed but the operator's normal role in the event of an accident would be to monitor the actions of the safety systems and their support systems.</p> <p>In the event of loss of Class IV power, Class III power is automatically supplied to safety systems. In the event that both Class IV and Class III power are lost, the EPS diesels start automatically. The EPS is credited to function following all events leading to a loss of Class IV /Class III power but system-supplied loads must be manually activated. As indicated in the Emergency Power Supply OSRs [NK29-</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>be subject to hardware interlocking in order to ensure that interaction with the test or maintenance system is impossible without deliberate manual intervention.</p> <p>Testing provisions that are permanently connected to safety systems should be part of the safety systems and should be the same class as the safety systems unless reliable buffering is in place or system performance is not negatively impacted.</p> <p>The interlock systems important to safety should either reduce the probability of occurrence for specific events, or maintain safety systems in an available state, during an accident. The interlock systems should be described and justified.</p> <p>Means should be provided to automatically initiate and control all safety actions, except those for which manual action alone has been justified. Examples of situations in which manual action alone might be justified include:</p> <ul style="list-style-type: none"> <li>• initiation of safety tasks after completion of automatic sequences</li> <li>• initiation of safety actions that are not</li> </ul>	<p>OSR-54300-00001], EPS is a manually operated system. Credit is given to the operator to switch from the Normal (poised) state to the Emergency state. The surveillance requirements ensure that EPS contactors are able to remove the normal source of power from the specified panels using the handswitches in Secondary Control Area (SCA), and allow EPS to supply the panels (see Section 2.2.2 of [NK29-OSR-54300-00001 Rev.000]. The majority of actions required of the safety systems during an accident are automatically initiated. When this happens, operator actions cannot stop these interventions. For the cases where operator actions are called for in Part 3 of the Safety Report the design of the system in no way impedes the required actions.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>required until a considerable time after the PIE</p> <ul style="list-style-type: none"> <li>control actions to bring the plant to a safe state in the long term, after an accident</li> </ul> <p>The value of each input parameter used in safety system functions, the status of each trip and actuation function in each division, and the status of each system initiation, should be available to plant operators.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>CSA Group, N290.14, Qualification of Pre-developed Software for Use in Safety Related Instrumentation and Control Applications in Nuclear Power Plants, Toronto, Canada.</li> <li>CSA Group, N290.6, Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of an Accident, Toronto, Canada.</li> <li>IAEA, NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Plants, Vienna, 2002.</li> <li>IEC, 61226, Nuclear Power Plants -</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Instrumentation and Control Important to Safety - Classification of Instrumentation and Control Functions, Geneva, 2009.</p> <ul style="list-style-type: none"> <li>• IEC, 61513, Nuclear Power Plants – Instrumentation and Control Important to Safety, General Requirements for Systems, Geneva, 2011.</li> <li>• IEC, 60987, Nuclear Power Plants – Instrumentation and Control Important to Safety – Hardware Design Requirements for Computer-Based Systems, Geneva, 2007.</li> <li>• IEC, 62385, Nuclear Power Plants – Instrumentation and Control Important to Safety – Methods for Assessing the Performance of Safety System Instrument Channels, Geneva, 2007.</li> <li>• IEC, 60880, Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems Performing Category A Functions, Geneva, 2006.</li> <li>• IEC, 60671, Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Surveillance Testing, Geneva, 2007.</li> <li>• IEEE, 7-4.3.2, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, Piscataway, New Jersey, 2010.</li> <li>• IEEE, 603, Standard Criteria for Safety Systems for Nuclear Power Generating Stations,</li> </ul>		

 <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	Piscataway, New Jersey, 2009.		
7.9.2	<p>Appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the lifetime of the system or equipment, and in particular, throughout the software development cycle.</p> <p>A top-down software development process shall be used to facilitate verification and validation activities. This approach shall include verification at each step of the development process to demonstrate that the respective product is correct, and validation to demonstrate that the resulting computer-based system or equipment meets its functional and performance requirements.</p> <p>If pre-developed software is used in systems or equipment important to safety, then the software (and any subsequent release of the software) shall be developed, inspected, and tested in accordance with standards of a category commensurate with the safety function provided by the given system or equipment.</p> <p>The software development process, including control, testing, and commissioning of design changes, as well as the results of independent</p>	<p>The clause is modified to streamline the text and eliminate redundant requirements, e.g. protection against physical attack; effective detection of failures etc. These changes do not impact the requirements.</p> <p>The Bruce A and B safety systems use an analog system for critical safety functions. The control systems use digital computers as described above and these display information to the operator in addition to controlling the plant. As stated in section 6.6 of Part 2 of the Safety Report a computer system is used to monitor the state of the special safety systems. For each reactor unit, the system is optically linked to 9 intelligent multiplexers, one for each channel of the shutdown systems, and one for each channel of the unit-specific parts of the ECI system. In addition, a station safety system monitoring computer, optically linked to three intelligent multiplexers, is used to monitor the common ECI system. Each computer is equipped with a unidirectional (read only) optical link to each of the intelligent multiplexers. Each multiplexer is equipped with differential analog and digital inputs. The Safety System Monitoring Computer also provides only information to the operator. Neither system provides direct safety functions.</p> <p>At this time the safety systems at Bruce B are analogue; however there are many uses for real-time computing at the station and most modern equipment has some software integrated into it.</p> <p>BP Procurement of Software Products - Embedded or Custom [BP-PROC-00050 R004, December 12, 2012] defines the process for procurement of equipment to be installed in station SSCs that contain software. The</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>assessment of that process, shall be reviewable and systematically documented in the design documentation.</p> <p>Where a function important to safety is computer-based, the following requirements shall apply:</p> <ol style="list-style-type: none"> <li>1. Functions not essential to safety are separate from and shown not to impact the safety function.</li> <li>2. The safety function is normally executed in processors separate from software that implements other functions, such as control, monitoring, and display.</li> <li>3. The requirements associated with diversity apply to computer-based systems that perform similar safety functions – the choice of diversity type shall be justified.</li> <li>4. The design incorporates fail-safe and fault tolerance features, and the additional complexity ensuing from these features results in an overall gain in safety.</li> </ol> <p>Guidance</p>	<p>procedure ensures procured software has adequate quality assurance applied during the software development process. The software categorization process and associated procedures are described in section 4.1.1.1. Detailed description of the methods for software categorization is provided in Software Categorization procedure [DPT- PDE-00032, R001, November 5, 2008]. All three methods (i.e., (1) existing categorization; (2) based upon the safety related systems list and (3) full categorization) described in section 4.1 of DPT-PDE-0032 are based upon B-STI-69000-00002, Standard for Software Categorization, which specifies the underlying technical basis for categorization. The modifications to the installed software or introduction of new software are governed by BP-PROC-00539, Design Change Package,</p> <p>Real-Time Process Computing is used by Operations group to control plant operations or processes either directly (automated), or indirectly (through user intervention).</p> <p>This includes process control computers; annunciators, other control and monitoring devices; perimeter-monitoring systems and other computer based systems integral to the real-time operation of the facility. These systems are engineered in accordance with an applicable Quality Engineering Program, for compliance with CSA N286.2. Further, the software itself is subject to COG-95-264.1, Guideline for Categorization of Software in Nuclear Power Plant Safety, Control, Monitoring, and Testing Systems.</p> <p>Software is classified as Safety-Related if it meets definition of the Real-time Process Computing and is categorized as Category I, II, or III, according to the Guideline for Categorization of Software in Nuclear Power Plant Safety,</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The standards and practices used for computer-based systems or equipment are identified prior to the design. The I&amp;C development lifecycle, which implements the identified requirements, should be coordinated with the human factors engineering lifecycle and the cyber security lifecycle, since they have a strong influence on I&amp;C development.</p> <p>The I&amp;C development lifecycle includes verification and validation activities. These activities should be identified and use appropriate engineering approaches; e.g., a top-down or bottom-up approach. The relationship between design and verification and validation should be indicated and the outcome of verification and validation activities should be documented.</p> <p>The pre-developed software should have the same level of qualification as for software that is written specifically for the application. The qualification of software should be verified through the national or international standards relevant to the qualification activities of pre-developed software.</p> <p>When the pre-developed software was not</p>	<p>Control, Monitoring, and Testing Systems, COG-95-264.1, Revision 1". The different categories of software are defined in section 3 of BP-PROC-00050, R004. It is noted that currently Bruce Power does not have a process for Category I software, whenever such software product is designed for use all associated software procedures would need to be updated or created (section 4.1.1.1 of BP-PROC-00050).</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>developed to equivalent standards, they may be used to implement IEC 61226 category B and C functions. However, a qualification plan and qualification report should be prepared to demonstrate that this software is fit for its intended purpose and meet the requirements in IEC 62138.</p> <p>The software development process should include consideration of consistency, modularity, structuredness, traceability, understandability and verifiability:</p> <ul style="list-style-type: none"> <li>consistency applies to uniform notations, terminology, comments, symbology, and implementation techniques</li> <li>modularity ensures that any change to one component has minimal impact on the others</li> <li>structuredness means that the design should proceed in an orderly and systematic manner (e.g., top-down design) and have minimized coupling between modules and subsystems</li> <li>traceability provides a thread to antecedent and subsequent documents, and refers to the ability to trace the design decision history and reasons for changes</li> <li>understandability means that the development processes and outputs should be</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>clear to a third party</p> <ul style="list-style-type: none"> <li>• verifiability refers to the extent to which the development processes and outputs have been created to facilitate verification using both static methods and testing</li> </ul> <p>The complete software development documentation should provide all information throughout the software development lifecycle.</p> <p>Additional information:</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>• IAEA, NS-G-1.1, Software for Computer Based Systems Important to Safety in Nuclear Plants, Vienna, 2000.</li> <li>• IEC, 62138, Nuclear Power Plants – Instrumentation and Control Important for Safety – Software Aspects for Computer-Based Systems Performing Category B or C Functions, Geneva, 2004.</li> </ul>		
7.9.3	Instrumentation and recording equipment shall be such that essential information is available to support plant procedures during and following DBAs and DEC's by:	<p>There are no changes to this clause.</p> <p>As described in Section 6.5.2.11 of Part 2 of the Safety Report, the Post-Accident Radiation Monitoring System (PARMS) provides on-line radioisotopic analysis for noble</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>1. indicating plant status</p> <p>2. identifying the locations of radioactive material</p> <p>3. supporting estimation of quantities of radioactive material</p> <p>4. recording vital plant parameters</p> <p>5. facilitating decisions in accident management</p> <p>Guidance</p> <p>Instrumentation is provided to ensure that essential information is available for assessing plant conditions, monitoring safety system performance, making decisions related to plant responses to abnormal events, and predicting radioactive material releases. Instrumentation is also provided</p> <p>for recording vital plant parameters and variables, such as:</p>	<p>gases, gross gamma detection and off-line radioisotopic analyses for particulates, iodine and tritium. The detected and analyzed parameters are presented on a local and a remote display unit, located in the Unit 2 control equipment room.</p> <p>As described in compliance note for clause 8.10.2, Secondary Control Areas (SCAs) are provided for post-accident monitoring and to execute basic safety functions following any common mode incident that renders the main control room uninhabitable. The Post Accident Radiation Monitoring System is seismically qualified as indicated in Table 2-2 of Part 2 of the Safety Report.</p> <p>As described in section 7.1 of Part 2 of the Safety Report, for each unit, a dual control computer system is used for control, data acquisition, data display, and alarm annunciation. The system is used for the control of such functions as regulating the reactor power, the steam generator pressure and level, and the de-aerator level. The control computers and the SSMC can record and display the parameters that are important to safety. This information will be used to monitor the course of DBAs and provide information on the status of essential equipment. All of the necessary instrumentation for monitoring essential information is available in the MCR (and SCA) and these have been shown by the SMA to be capable of withstanding the Review Level Earthquake (RLE). Should the DCCs/SSMC (which are not seismically qualified) not be available there would be a need to rely on manual record keeping for trends. The four unit SCAs are located on the north side of each reactor building, are remote and isolated from the MCR in the Central Service Area. All instrumentation and control loops terminating in the SCAs originate from</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>temperature at various locations</li> <li>pressure of containment, and primary coolant system</li> <li>level of radioactivity at various locations</li> <li>reactor vessel water level for a light water reactor (LWR), or heat transport system water level and moderator level for a CANDU reactor</li> <li>containment water level</li> <li>hydrogen concentration</li> </ul> <p>The design should provide the design basis, design criteria, and display criteria for the accident monitoring parameters.</p> <p>Accident monitoring instrumentation should meet performance criteria, such as measurement range, accuracy, response time, operating time and reliability target. Appropriate design analysis should be performed to confirm that the performance criteria have been met.</p> <p>Accident monitoring instrumentation meets the single-failure criterion (section 7.6.2). The design should ensure that there are no common-causes that can lead to the failure of instrumentation providing redundant measurements.</p>	<p>seismically qualified instrument rooms or from other SCAs. All cable routes from the primary device to termination in the SCA are channelized and seismically qualified. All loops having a control or indication function in the main control room have that leg buffered in the appropriate instrument room so that its failure in the common mode even does not affect the SCA circuit. For Group II systems only the loops to the MCR are buffered, loops to the SCAs, in general, are not buffered (section 1.3.2 of Secondary Control Area Design Manual NK29-DM-63760-001).</p> <p>The classification of equipment as complementary design features is a new classification and has not been used at Bruce A and B in the past. The PARMS instrumentation and equipment described above will cope with a wide range of accident scenarios including many BDBAs and severe accidents.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>To the extent practicable, the same variables and displays should be used for both normal operation and accident monitoring.</p> <p>The design should:</p> <ul style="list-style-type: none"> <li>incorporate testing capability, to verify operability requirements on a periodic basis</li> <li>facilitate maintenance, repair and calibration</li> <li>permit administrative access control for instrument channel calibration and testing</li> </ul> <p>Accident monitoring instrumentation is demonstrated to be qualified to perform its required functions for the length of time when its function is required under DBAs and DEC's.</p> <p>Additional information:</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>CSA Group, N290.6, Requirements for Monitoring and Display of Nuclear Power Plant</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Safety Functions in the Event of an Accident, Toronto, Canada.</p> <ul style="list-style-type: none"> <li>• IEC, 61226, ed. 3.0, Nuclear Power Plants – Instrumentation and Control Important to Safety – Classification of Instrumentation and Control Functions, Geneva, 2009.</li> <li>• IEC, 62138, ed. 1.0, Nuclear Power Plants – Instrumentation and Control Important for Safety – Software Aspects for Computer-Based Systems Performing Category B or C Functions, Geneva, 2004.</li> <li>• IEEE, 497, Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations, Piscataway, New Jersey, 2010.</li> </ul>		
7.10	<p>The safety support systems shall ensure that the fundamental safety functions are available in operational states, DBAs and DEC's. Safety support systems provide services such as electrical power, compressed air, water, and air conditioning and ventilation to systems important to safety.</p> <p>Where normal services are provided from external sources, backup safety support systems shall also be available onsite.</p> <p>The design shall incorporate emergency safety</p>	<p>The text was modified to include two new requirements for emergency support systems, item 2.</p> <p>The standby generators and the Emergency Power Supply System provide back up to Class IV electrical system. As described in the Emergency Power Supply Design Manual [NK29-DM-54300-001, Rev. 04]. The Emergency Power Supply System (EPS) provides power for the equipment and instruments, which are required to maintain and monitor the reactor in a safe shutdown state, in the event of failure of the Group 1 Systems. As part of the protection against common mode incidents (such as fires, turbine/generator missiles, etc., which can cause multiple system failures), two physically separated groups of safety-related systems and equipment are provided at Bruce "B" NGS. These groups are</p>	Gap




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>support systems to cope with the possibility of loss of normal service and, where applicable, concurrent loss of backup systems.</p> <p>The systems that provide normal services, backup services and emergency services shall have:</p> <ol style="list-style-type: none"> <li>1. sufficient capacity to meet the load requirements of the systems that perform the fundamental safety functions</li> <li>2. availability and reliability commensurate with the systems to which they supply the service</li> </ol> <p>The emergency support systems shall:</p> <ol style="list-style-type: none"> <li>1. be independent of normal and backup systems</li> <li>2. support continuity of the fundamental safety functions until long-term (normal or backup) service is re-established: <ol style="list-style-type: none"> <li>a. without the need for operator action to connect temporary onsite services for at least 8 hours</li> </ol> </li> </ol>	<p>designed to provide redundant capability to maintain the reactor in a safe shutdown state. Relative to the electrical power systems, Group 1 includes Class IV, III, II and I Power Systems. Group 2 is composed of an on-site power generation and distribution system, physically separated from the Group 1 Power System. This Group 2 System is called the Emergency Power Supply System. The EPS System is the only power system with all its equipment seismically qualified to a Design Basis Earthquake (DBE) level. Therefore it may be the only operational power system after a postulated DBE/SDE to supply power to the equipment and instruments required for cooling and monitoring of the four reactors. EPS System has been designed as reliable as achievable. This is achieved by duplication of the buses and power sources - Emergency Power Generators (EPG's).</p> <p>The Emergency Power Supply System (EPS) is a separate power distribution network capable of supplying power for reactor shutdown, forced primary coolant circulation, and monitoring after a common mode incident, e. g. an earthquake or fire. All equipment associated with this system is seismically qualified for a Design Basis Earthquake (DBE) (Section 8.3.11 of Part 2 of the Safety Report). The EPS provides power to specific equipment and instrumentation required to maintain essential safety functions following an event and is sized accordingly. Two separate 125 V DC buses are interconnected through two normally open breakers. Each of the buses is supplied from a rectifier connected to a 600 V Motor Control Centre (MCC) in the Emergency Water and Power Supply Building (EWPSB) or a battery floating on the bus. Table 8-1 of Part 2 of the Safety Report presents a description of Class III/EPS loads. The system Design Manual [NK29-DM-54300-001, Rev. 04]</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>b. without the need for offsite services and support for at least 72 hours</p> <p>3. have a capacity margin that allows for future increases in demand</p> <p>4. be testable under design load conditions, where practicable</p> <p>Guidance</p> <p>The design basis for any compressed air system that serves an item important to safety at the NPP should specify the quality, flow rate and cleanness of the air to be provided.</p> <p>Systems for air conditioning, air heating, air cooling and ventilation should be provided (as appropriate) in auxiliary rooms or other areas at the nuclear power plant, so as to maintain the required environmental conditions for systems and components important to safety, in all plant states.</p> <p>Pre-installed equipment can be credited for accident mitigation after 30 minutes where only</p>	<p>specifies the functional and performance requirements for the EPS system. As a design requirement each Emergency Power Generator shall have a black start capability and a seven day emergency load capacity. Each EPG shall have a guaranteed rating of 4000 kW and an overload capability of the generator as 5050 kW (section 2.2 of EPS design manual). The EPG's automatically start on receipt of a LOCA signal as a prudent operating measure to insure the availability of the Group 2 power source if needed. In the case of following a SDE 24 hours after a LOCA, the EPS is designed to provide power to the EWS and ECI systems to remove decay heat from the reactor. EPS is designed to provide power to the instrumentation and control devices. Also the EPS system provides the power to EFADS system to maintain the operating capability of the Negative Pressure Containment system. The unavailability of the EPS after a common mode event is 1E-2 years/year (section 2.12 of the EPS design manual).</p> <p>The station has two sources of standby power on site - the station batteries and the standby generators. The batteries are lead acid batteries, which are connected to give a nominal output voltage of 250 V DC. They are capable of supplying the bus load for 40 minutes when there is no AC supply to the rectifiers. There is one set of batteries per 250 V DC bus in the plant. Each set of batteries is housed in its own ventilated room (section 8.4.2 of Part 2 of the Safety Report). There are four standby combustion turbine generator sets, each rated at 15 MVA and each capable of providing the Class III power requirements for safe plant shutdown of two units, plus the common loads. The standby generator sets are started automatically, following loss of Class IV power, which is the normal power supply to the</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>control room actions are needed or after 1 hour if field actions are needed. These actions should be limited to operating valves, starting pumps, etc. Guidance is provided in section 8.10.4 for justification of such actions.</p> <p>If equipment is not pre-installed, but is stored onsite, it can normally be credited after 8 hours. However, this should be justified based on an assessment of the actions required and the availability of procedures and training to support those actions. It is possible that longer times may be necessary for complex actions. Equipment or supplies stored offsite or support staff from offsite should not normally be credited for 72 hours. Again, the value used should be justified and may be longer.</p> <p>Guidance on redundant connection points for temporary services is described in section 7.3.4.1.</p>	<p>critical Class III loads, or following a Loss of Coolant Accident (LOCA) with ECI initiation (Section 8.4. of Part 2 of the Safety Report).</p> <p>As part of Fukushima Action Items consideration is given at Bruce B design to provide an additional path of 600 V to critical reactor control instrumentation and monitoring loads, Secondary Control Area (SCA) services, ECI D20 isolation valve operation (i.e., 34330-MV14), EFADS valves operation and Bruce B Emergency Intercom operation during Station Blackout (SBO). The additional path is accomplished by providing 600 V power supply from portable generators, using feeder cables with compatible quick connectors on both ends. During SBO, six portable generators will be removed from storage and installed outside the power house at specified locations in Units 5/6/7/8, Unit 0 SCA (EWPSB), Emergency Intercom System, Unit 0 EFADS, and the Vacuum Building. The portable generator will supply power to Bruce B Emergency Power Supply System (Environmentally and Seismically Qualified) for reactor monitoring and control, to prevent damage to the reactor core, and subsequent uncontrolled radioactive releases to the environment. This will work in conjunction with the emergency cooling water supply enhancements. Since the deployment of portable generators will take at least two hours, to bridge the gap of power loss between total loss of AC power and portable generator deployment, the existing Class I battery system is considered to supply power to the Bruce B essential reactor control/monitoring, lighting, and motorized valve loads until portable generators are deployed and operational. In the event of a loss of all normal, backup and emergency AC power, the guaranteed capability of Class I batteries to support all essential electrical equipment is 40 minutes</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>(although it is recognized that some services may last much longer). This duration is short compared to other essential supply capabilities and gives little time to restore AC power. Once batteries are exhausted, most control and instrumentation functions will be lost. As part of Fukushima Action Items an assessment on Bruce B Class I Batteries in Units 5, 6, 7 and 8 has been carried out to determine an extension of their availability for a minimum mission time of eight hours following a Beyond Design Basis Accident [NK29-REP-54900-00001, Rev. 000, March 13, 2013]. The assessment is documented as Appendix 4 of Bruce Power Progress Report No. 3 on CNSC Action Plan - Fukushima Action Items [NK21-CORR-00531-10560 / NK29-CORR-00531-10963]. The assessment determined that by de-energizing the 600 V Class II inverters on 55100-BUA and 55100-BUB a minimum mission time of 12 hours for battery BY1 and 8 hours for battery BY2 has been achieved thus allowing critical safety parameters to be monitored until backup portable supply is available.</p> <p>Group B Standby Safety Systems and Group C Safety Support Systems as per Safety Related System List [BP-PROC-00169, R002] meet the interpretation of emergency safety support systems in this clause. In the absence of a clear definition for emergency support systems, the interpretation is that under Group B, the Emergency Power Supply and the Emergency Water System are capable of supplying adequate emergency services to ensure that the reactor can be placed in and kept in a safe shutdown state. The design descriptions of Emergency Power Supply and Emergency Water System are provided in sections 8.3.11 and 11.1.3.5 of Part 2 of Safety Report.</p>	

 <div>Division of Kinectrics Inc.</div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>The purpose of the Bruce Power Nuclear Emergency Response Plan (NERP) [BP-PLAN-00001, R005, December 2, 2014] is to describe the concepts, structures, roles, and processes needed to implement and maintain Bruce Power's capability to prepare for and to respond to a nuclear radiological emergency. This Plan outlines the command, control, and coordination structure and activities, activation, site integration, external agency coordination, deployment of emergency resources, and emergency facilities through the use Emergency Response Procedures developed to guide effectively trained emergency response staff in emergency response and mitigation techniques. In addition to design basis events, as specified in section 4.1.1.1, this plan takes into account requirements to support a sustained response to a beyond design basis multi-unit event resulting in an extended loss of off-site power for up to 72 hours without assistance.</p> <p>A summary of the operator actions credited in the safety analysis is documented in Section 1.3 of Part 3 of the Safety Report. The current design documentation does not specifically address the timing requirements introduced in this clause; therefore this is assessed as a gap (Gap).</p> <p>Safety design guides NK29-DG-03650-001, NK29-DG-03650-002, NK29-DG-03650-003, NK29-DG-03650-005, NK29-DG-03650-006 and NK21-DG-20091-002 provide guidance for design of SSC(s) intended to mitigate DBA only. The design guide B-DG-03654-00001 is to provide guidance for design of portable SSC(s) which are enhancements intended to prevent progression of a BDBA, specifically a station blackout (SBO), into a severe accident. It is noted that the design considers BDBAs that do not involve core</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>damage. The guide will focus on providing guidance for the design of portable SSC(s) which will be used to prevent progression of a BDBA into a severe accident (SA). Such design features which are outside of the design basis envelope that are introduced to cope with beyond design basis accidents are termed Complementary Design Features (CDF). Complementary design features include design or procedural considerations, or both, and are based on a combination of phenomenological models, engineering judgments, and probabilistic methods. As indicated in section 5.1 of B-DG-03654-00001 equipment required to cope with a SBO during the first 72 hours should be available on the site. For equipment not located in the site, consideration is given to its availability and accessibility in the time required taking into account weather conditions likely to prevail during a loss of offsite power.</p> <p>The capacity margin of the Bruce A and B emergency support systems to allow for further increases in demand is limited, as it was sized for a considerably different safety case. However, this is rather a design objective and has no impact on safe operation. Should additional loads be required, the Engineering Change Control Program [BP-PROG-10.02, R010] will be used to determine how to address the emergency support system loading issue.</p> <p>EPS, EWS, as well as the Class III, II and I electrical systems and Standby generators, are seismically qualified as shown in Table 2-2 [Section 2.5., Part 2 of the Safety Report]. The Bruce B seismically qualified Powerhouse Emergency Venting System (PEVS) is a standby safety system designed to mitigate the consequence of a secondary side steam piping or feedwater piping failure. The fundamental function</p>	

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>of the overall system is to restrict powerhouse over-pressure and to mitigate the consequence of high energy secondary pipe breaks to support general Group 2 and specific Group 1 capability. The system utilizes the natural buoyancy of the steam/hot air inside the powerhouse to induce a chimney effect and draw cold air at lower elevations and exhaust the hot mixture at higher elevations (section 6.7.4 of Part 2 of the Safety Report). In addition, as described in section 2.6.2 of Part 2 of the Safety Report, the scope for the environmental qualification program includes all components, which are essential to provide a safety function consistent with the assumptions and requirements documented in the accident analysis, in accordance with the design and licencing basis established for the station.</p> <p>The Environmental Qualification of Safety Related Equipment for the Bruce B Nuclear Generating Station [NK29-DG-03650-003] contains the detailed requirements for each of the systems subject to environmental qualifications. As noted in Safety Factor 3 this design guide was used for the environmental qualification of the original Bruce B design, and is a historical document that has not been updated to current requirements. This design guide identifies the DBAs that result in global harsh environments, the safety related systems and structures that maintain the basic nuclear safety functions when exposed to harsh environments, and the system functional requirements necessary to maintain the basic nuclear safety functions when exposed to harsh environments. In addition Bruce B EQ Room Conditions Manual [B-STQ-03651-10001, Rev. 001] provides a single source of the normal service and post-accident environmental conditions for use in establishing and</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
		maintaining EQ of essential safety related equipment.	
7.11	<p>The design authority shall define the guaranteed shutdown state (GSS) that will support safe maintenance activities of the NPP.</p> <p>The design shall provide two independent means of preventing recriticality from any pathway or mechanism when the reactor is in the GSS.</p> <p>The shutdown margin for GSS shall be such that the core will remain subcritical for any credible changes in the core configuration and reactivity addition. Where possible, this shall be achieved without operator intervention.</p> <p>Guidance</p> <p>A GSS is where the reactor remains in a stable, sub-critical state, independent of any perturbation in reactivity produced by any change in core configuration, core properties, or process system failure.</p> <p>The design should describe the GSSs that are expected to be used over the life of the facility, including steps for GSS placement and removal,</p>	<p>There is no change in the requirements.</p> <p>The guaranteed shutdown states are defined in the Clause 63.13 of the Bruce B OP&amp;Ps [BP-OPP-00001, R019]. The primary function of the Moderator system during outages is to ensure that the reactor remains in a Guaranteed Shutdown State. The control parameter specifications applicable during GSS are specified in Moderator System Units 1-8 [B-SYS-32000-00001]. The requirements for guaranteed shutdown state are specified in Operational Safety Requirements for Moderator System [NK29-OSR-32000-00001, R000]. The Moderator System OSRs present the safety limits applicable to Over-Poisoned Guaranteed Shutdown State and Drained Guaranteed Shutdown State. A minimum poison concentration, in addition to the minimum level requirement, is required to prevent recriticality while the reactor is shut down and special safety systems and regulating systems may be out of service.</p> <p>As describes in sections 1.2.3 and 1.2.4 of Moderator Systems OSRs, the over-poisoned guaranteed shutdown state (OPGSS) requires that:</p> <p>" There is sufficient poison in the moderator such that the reactor cannot credibly become critical</p> <p>" Operational procedures are in place to prevent poison removal</p> <p>The determination of the required poison concentration is derived from a safety assessment and the resultant Safety Analysis Limit (SAL) for this parameter is documented in section 4.0 (Table 4.1-1) of this OSR. The required</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	and functional tests to be performed.	<p>operational procedures to prevent removal of poison are documented in the appropriate operating procedures.</p> <p>The drained guaranteed shutdown state (DGSS) is the ultimate safe state since it is not credible to achieve criticality without heavy water in the Calandria. DGSS requires that:</p> <p>" Sufficient D2O must be drained from the Calandria such that the reactor cannot credibly become critical.</p> <p>" Operational procedures are in place to isolate all sources of D2O from entering the Calandria and to depressurize the PHT so that an in-core LOCA is not credible.</p> <p>" A drain hole must be guaranteed such that if the isolation from the single largest potential addition source should fail, the addition rate would be drained without increasing the level of D2O in the Calandria.</p> <p>The determination of the required hole size and location is an engineering calculation and the SAL for this parameter is documented in section 5.0 (Table 5.1-1) of the OSR. The required operational procedures to drain the Calandria and to prevent D2O addition are documented in the appropriate operating procedures.</p> <p>The safety analysis [Appendix 9 Main Moderator and Moderator Auxiliary System Failures, Part 3 of Safety Analysis] considers pressure tube and Calandria tube failures that occur when the reactor is in the OPGSS. These result in HTS coolant diluting the dissolved poison in the moderator. The limiting accident of this type defines the minimum poison concentration required to ensure the reactor does not become critical again. The probabilistic risk assessments</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>also consider accidents during OPGSS, however these include very low probability events considered to be beyond the design basis and do not impose specific operational requirements on the Moderator System. [Moderator System OSRs]. The minimum poison concentration during OPGSS must be sufficient to ensure the reactor remains in a sub-critical state following any credible accident. The limiting accident is an in-core LOCA which results in the dilution of poisoned moderator with HTS coolant. Safety analysis calculated minimum required poison concentrations of 11.9 and 14.9 mg/kg (ppm) D2O with adjusters locked in-core and out-of-core respectively. These represent the minimum Safety Analysis Limits.</p> <p>The CNSC expressed concerns with the calculation methodology and has required that higher concentrations be used. As a result, the currently implemented limits for OPGSS are 19.1 and 21.8 mg/kg (ppm) D2O with adjusters locked in-core and out-of-core respectively.</p> <p>All sources of D2O are isolated from the Calandria while in the Drained Guaranteed Shutdown State. The design calculation assumes an appropriate location (e.g., maximum elevation) for the guaranteed hole and determines its required size to ensure that D2O inadvertently entering the Calandria will drain out, avoiding a recriticality event. DGSS is achieved by preventing D2O addition and providing a hole in the moderator piping of sufficient size and in a location such that the Calandria would not refill even if one of the isolations failed.</p> <p>The chemistry specification for the moderator system [B-</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		CYS-32000-00001] includes results of testing that has shown that self-shielding by gadolinium hydroxide, precipitate formed at typical OPGSS concentrations is small and that gadolinium hydroxide suspends for many hours. Typically the test frequency is determined by safety assessments, probabilistic risk assessment and unavailability analyses. The functional tests to be performed on the equipment associated with GSS (e.g., auxiliary pumps needed to run for poison, sampling and recirculation) are not reflected in the design documentation; therefore this is assessed as a gap (Gap).	
7.12	The design of the NPP, including that of external buildings and SSCs integral to plant operation, shall include provisions for fire safety.	<p>There is no change in the text. This is introductory clause; hence no assessment is required.</p> <p>As discussed in Safety Factor 7 guidance for documenting protection against fire hazard is provided in DPT-PDE-00027, DPT-PDE-00028 and DPT-PDE-00029.</p> <p>The extent to which the Bruce B design achieves all objectives detailed in sub clauses 7.12.1 to 7.12.3 is documented in NK29-REP-71400-00004, NK29-REP-71400-00003 and NK29-REP-71400-00002.</p>	C
7.12.1	<p>Suitable incorporation of operational procedures, redundant SSCs, physical barriers, spatial separation, fire protection systems, and design for fail-safe operation shall achieve the following general objectives:</p> <p>1. prevent the initiation of fires</p>	<p>There are no changes in the requirements.</p> <p>The Fire Safety Assessments performed for Bruce B consists of three separate assessments:</p> <p>1. The Fire Hazards Assessment [NK29-REP-71400-00004 R04] reviewed all areas of the plant with respect to the in situ and transient fire hazards, installed fire protection features, building construction and layout, and potential impediments to manual fire response. The FHA is conducted in accordance with the provisions of CSA N293 and</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2. limit the propagation and effects of fires that do occur by:</p> <p>a. quickly detecting and suppressing fires to limit damage</p> <p>b. confining the spread of fires and fire by-products that have not been extinguished</p> <p>3. prevent loss of redundancy in safety and safety support systems</p> <p>4. provide assurance of safe shutdown</p> <p>5. ensure that monitoring of safety-critical parameters remains available</p> <p>6. prevent exposure, uncontrolled release, or unacceptable dispersion of hazardous substances, nuclear material, or radioactive material, due to fires</p> <p>7. prevent the detrimental effects of event mitigation efforts, both inside and outside of containment</p> <p>8. ensure structural sufficiency and stability in</p>	<p>evaluates the conditions of the plant as operated.</p> <p>2. Fire Safety Shutdown Analysis [NK29-REP-71400-00003, Rev. 3] evaluates the capability to shut down and maintain the reactor in the shutdown state with respect to postulated fire damage. Using fire protection defence in depth philosophy described in clauses 5.3 and 11.6 of CSA N293, evaluations were carried out to either justify existing plant configurations or make recommendations for adjustments in physical plant hardware, administrative controls, and procedures to ensure the performance goals can be met.</p> <p>3. Fire Protection Code Compliance Review [NK29-REP-71400-00002-R03] evaluated the existing Bruce B fire protection features that are incorporated into the Fire Hazards Assessment portion of the FSA. It is performed to validate that installed fire protection features will perform their intended functions at the time of a postulated fire and to identify fire protection feature vulnerabilities that may have been created through historical plant modifications. The review provides the assurance that installed fire protection features can be credited in the FSA and that personnel safety with respect to fires has been maintained.</p> <p>The Code Compliance Review includes a detailed line-by-line review of CSA N293-07 to demonstrate documented compliance statements for each applicable section of the operational requirements. The CCR evaluated the as-found station conditions against the applicable fire protection portions of the National Building and Fire Codes.</p> <p>The Fire Safety Assessment and supporting documentation provides the basis for the development and implementation</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>the event of fire</p> <p>Buildings or structures shall be constructed using non-combustible or fire retardant and heat resistant material.</p> <p>Fire is considered an internal hazard. The essential safety functions shall be available during a fire.</p> <p>Fire suppression systems shall be designed and located such that rupture, or spurious or inadvertent operation, will not significantly impair the capability of SSCs important to safety.</p> <p>Guidance</p> <p>Effective fire protection is achieved by:</p> <ul style="list-style-type: none"> <li>• fire protection features such as programs and procedures, fire prevention, fire detection, fire warning, emergency communication, fire by-product management, fire suppression and fire containment, non-combustible construction, seismic and environmental qualification of fire protection equipment</li> </ul>	<p>of an efficient Fire Protection Program, as required by CSA N293.</p> <p>Separate assessments of N293, National Building Code and National Fire Code have been performed and documented.</p> <p>Details about the design of Fire Protection System are presented of the Safety Report 11.5.1 of Part 2 of the Safety Report. The results of fire protection assessment are presented in Safety Factor 7.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>the use of physical barriers to segregate redundant SSCs important to safety</li> </ul> <p>The design should address protection from fire by demonstrating that a defence in depth approach has been implemented. Supporting documents are expected to include a comprehensive design report, code compliance review, a fire hazard assessment, fire safe shutdown analysis, and a fire protection program.</p> <p>An independent third-party review of the design assessing compliance against the applicable fire codes and standards used in the design for protection from fires and explosions should be performed. The review should provide a definitive statement that the design conforms to the identified codes and standards, meets good engineering practices, and achieves fire protection objectives.</p> <p>The design should comply with the requirements of the following codes and standards:</p> <ul style="list-style-type: none"> <li>CSA Group, N293, Fire protection for nuclear power plants, Toronto, Canada.</li> <li>NRC, National Building Code of Canada,</li> </ul>		



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Ottawa, Canada, 2010.</p> <ul style="list-style-type: none"> <li>NRC, National Fire Code of Canada, Ottawa, Canada, 2010.</li> </ul> <p>Although CSA N293 is considered acceptable to provide technology-neutral design criteria, it does not fully address some fire safety aspects, such as:</p> <ul style="list-style-type: none"> <li>operator-initiated manual actions</li> <li>associated fire safe shutdown circuit analysis</li> <li>multiple spurious operations</li> </ul> <p>Guidance on the above fire safety aspects is provided in:</p> <ul style="list-style-type: none"> <li>U.S. NRC, NUREG-1852, Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire, 2007.</li> <li>Nuclear Energy Institute, NEI 00-01, Guidance for Post-Fire Safe Shutdown Circuit Analysis, Washington, D.C., 2005.</li> </ul> <p>Additional information</p>		



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>• IAEA, NS-G-2.1, Fire Safety in Operation of Nuclear Power Plants, Vienna, 2000.</li> <li>• IAEA, Safety Report Series No. 8, Preparation of Fire Hazard Analysis for Nuclear Power Plants, Vienna, 1998.</li> <li>• IAEA, NS-G-1.7, Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants, Vienna, 2004.</li> <li>• National Fire Protection Association (NFPA), Fire Protection Handbook, Quincy, Massachusetts, 2008.</li> <li>• NFPA, 805, Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants, Quincy, Massachusetts, 2010.</li> <li>• NFPA, 804, Standard for Fire Protection for Advanced Light Water Reactor Electric Generating Plants, Quincy, Massachusetts, 2010.</li> <li>• NEI, 00-01, Guidance for Post-Fire Safe Shutdown Circuit Analysis, Washington, D.C., 2005.</li> <li>• NEI, 04-02, rev. 1, Guidance for Implementing a Risk-Informed, Performance-</li> </ul>		



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design


File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Based Fire Protection Program under 10 CFR 50.48(c), Washington, D.C., 2005.</p> <ul style="list-style-type: none"> <li>• Society of Fire Protection Engineers (SFPE), SFPE Handbook of Fire Protection Engineering, Bethesda, Maryland, 2008.</li> <li>• U.S. NRC, NUREG/CR-6850, EPRI 1011989, Fire Probabilistic Risk Assessment Methods Enhancements, Washington, D.C., 2010.</li> <li>• U.S. NRC, NUREG-0800, section 9.5.1.1, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR edition - Fire Protection Program, Washington, D.C., 2009.</li> <li>• U.S. NRC, Regulatory Guide 1.189, Fire Protection for Operating Nuclear Power Plants, Washington, D.C., 2009.</li> <li>• U.S. NRC, NUREG-1852, Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire, Washington, D.C., 2007.</li> </ul>		
7.12.2	<p>The design shall provide protection to workers and the public from event sequences initiated by fire or explosion in accordance with established radiological, toxicological, and human factors criteria so that the following objectives are achieved:</p> <p>1. Persons not intimate with the initial event</p>	<p>The text is modified to read "a low probability" instead of "a decreased risk" in item 2. The change is editorial and does not affect the intent of the requirement.</p> <p>A review of the same clause in RD-337 indicated that the Bruce A and B design does not fully meet this requirement, as documented in [NK21-CORR-00531-11005 / NK29-CORR-00531-11397]. Compliance with the provisions of this requirement is in practice accomplished through compliance</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>(including the public, occupants, and emergency responders) are protected from injury and loss of life.</p> <p>2. Persons intimate with the initial event have a low probability of injury or death.</p> <p>To demonstrate that the above life safety objectives have been achieved, the design shall provide:</p> <p>1. effective and reliable means of fire detection in all areas</p> <p>2. effective and reliable means of emergency notification, including the nature of the emergency and protective actions to be taken</p> <p>3. multiple and separate safe egress routes from any area</p> <p>4. easily accessible exits</p> <p>5. effective and reliable identification and illumination of egress routes and exits</p>	<p>with the CSA standard for fire protection [CSA N293-12], the National Fire Code [NFCC], and relevant parts of the National Building Code [NBCC]. As stated in the LCH, compliance verification criteria for licence condition 10.2 Fire Protection Program, Bruce Power is compliant with the programmatic and operational requirements of CSA N293-12. The requirements for a revised Code Compliance Review, Fire Hazard Assessment and Fire Safety Shutdown Analysis did not change from CSA N293-07 to N293-12; N293-12 simply provided additional clarification on the requirements. Due to the date of construction of the Bruce facilities versus the date of issuance of the codes (1970's vs. 2007) a number of historical design related non-conformances were identified. Bruce Power has submitted a revised Code Compliance Review, Fire Hazard Assessment and Fire Safety Shutdown Analysis to the CNSC, as well as implementation dates for the remaining plant upgrades to address these design non-conformances. The 7-year implementation plan to complete this work was submitted to CNSC staff in October 2014 and has been accepted by CNSC staff. Bruce Power will provide CNSC staff with semi-annual updates until such time as the transition plan is implemented.</p> <p>CSA N293 requires that a utility perform a Fire Safety Assessment (FSA) which evaluates each of its stations against the requirements of the Standard. As discussed in Section 7.12.1 the Standard suggests that the FSA be documented in the form of three separate complementary documents:</p> <p>" A Code Compliance Review (CCR)</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>6. sufficient exiting capacity for the number of workers (taking into account the emergency movement of crowds)</p> <p>7. protection of workers from fires and fire by-products (i.e., combustion products, smoke, heat etc.) during egress and in the areas of refuge</p> <p>8. protection of workers performing plant control and mitigation functions during or following a fire</p> <p>9. adequate supporting infrastructure (lighting, access etc.) for workers to perform emergency response, plant control, and mitigation activities during or following a fire</p> <p>10. sufficient structural integrity and stability of buildings and structures to ensure the safety of workers and emergency responders during and after a fire</p> <p>11. protection of workers from the release or dispersion of hazardous substances, radioactive material, or nuclear material as a result of fire</p>	<p>" A Fire Hazard Assessment (FHA)</p> <p>" A Fire Safe Shutdown Analysis (FSSA)</p> <p>Bruce B has a Fire Safety Assessment (FSA), consisting of a Code Compliance Review (CCR) [NK29-REP-71400-00002, Rev.2], Fire Hazard Assessment (FHA) [NK29-REP-71400-00004, Rev. 4] and First Safe Shutdown Analysis (FSSA) [NK29-REP-71400-00003, Rev.3].</p> <p>The CNSC response in NK21-CORR-00531-10758 / NK29-CORR-00531-11139 noted that based on the review, Bruce Power submissions were deemed acceptable. Furthermore, the revised FSSA, FHA and CCR are considered acceptable to meet the requirements of CSA N293-07 and the PROL and associated Licence Conditions Handbook.</p> <p>Safety Factor 7: Hazard Analysis, performs an assessment against CSA N293-12. Other fire protection-related standards (NFCC and NFPA-805) are discussed in the following sections of this report:</p> <p>CSA N293: As discussed in Section 3.2 of this Safety Factor Report, "Bruce Power's reviews of the updated version of CSA N293-12 concluded that the existing fire protection plans, programs, procedures and response capabilities are generally in full compliance with the standard. Administrative and editorial updates to documentation will be required to change references to the revised standard and, in some cases, to add the new terminology it contains. These actions will be completed in a timely manner in accordance with Bruce Power's document change control procedures. No transition plan is required. The administrative and editorial documentation updates to Fire Protection plans, programs and procedures to address the requirements of the 2012</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Guidance</p> <p>The National Building Code of Canada (NBCC) and the National Fire Code of Canada (NFCC) are objective-based national model codes. The provisions of the NBCC and NFCC are considered the minimum acceptable measures for meeting the objectives of safety, health, structural protection, and fire protection of buildings. As such, additional fire protection measures may be required to meet the regulatory requirements detailed in this regulatory document. Additional fire safety provisions are usually assessed and documented in the code compliance and fire hazard assessment, as required by CSA N293, Fire protection for nuclear power plants.</p>	<p>edition of this standard are targeted for the end of November 2017."</p> <p>NBCC and NFCC: As discussed in Section 3.6 of this Safety Factor Report, the NFCC contains technical requirements designed to provide an acceptable level of fire safety. It complements the NBCC, and both must be considered when constructing, renovating or maintaining buildings. The NFCC, as well as fire protection related portions of the NBCC were reviewed as part of the CSA N293 Gap Assessment, since the provisions of CSA N293 are considered to be bounding those of the NFCC.</p> <p>NFPA 805: As discussed in Section 3.5 of this Safety Factor Report, the results of the review performed in Section A.6 state "high-level review of those clauses in NFPA 805 which provide guidance cited in CSA Standard N293-12 indicates that Bruce Power is compliant".</p> <p>As committed in [Letter, F. Saunders to K. Lafrenière, "Action Item 1207-3890: CSA N293 Transition Summary Report", October 3, 2014, NK21 -CORR-00531 -11574 / NK29-CORR-00531 -11955] Bruce Power provides annual update on fire protection related capital projects. Seven Year Implementation Plan of Prioritized Fire Protection Capital Projects, risk prioritization for the Fire Protection Capital Projects as well as summary of low risk fire protection items are included in the latest update [NK21-CORR-00531-12304/NK29-CORR-00531-12735]. As per the CSA N293-07 requirements, Operations staff review of Bruce B FSSA Operator Action Recommendations for operator manual action has been performed and submitted to CNSC as Enclosure 2 to [Letter F. Saunders to K. Larfeniere, Action 1207-3890: Provide Annual Update for the Fire Protection</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		Capital Projects, NK21-CORR-00531/NK29-CORR-00531-12735, November 30, 2015]. For each room where the FSSA contains recommended actions, walk downs were performed to assess feasibility and access given the postulated fire. The review supports crediting operator action for the postulated fires. No gaps were identified in the required operator response to hazards identified in the FSSA.	
7.12.3	<p>The design shall minimize the release and dispersion of hazardous substances or radioactive material to the environment, and shall minimize the impact of any releases or dispersions, including those resulting from fire.</p> <p>Guidance</p> <p>As indicated in section 7.12.2, the NBCC and the NFCC cover the minimum fire safety and fire protection features that must be incorporated at the time of building design and construction. Additional fire protection measures may be required to meet the regulatory requirements detailed in section 7.12.3. Additional fire safety provisions are usually assessed and documented in the code compliance, fire hazard assessment and fire safe shutdown analysis, as required by CSA N293.</p>	<p>There are no changes to the requirements in this clause.</p> <p>Bruce Power, in its Fire Safety Management Plan [BP-PLAN-00008, R004, September 14, 2015], sets the objectives of its program and describes the fire management aspects. The objective of fire safety management is to oversee the planning, implementation and control of activities related to fire safety, which are conducted by various contributing organizations in order to:</p> <ol style="list-style-type: none"> <li>1. Ensure that fires do not increase the risk to nuclear safety objectives of control, cool and contain the radioactive materials from the reactor.</li> <li>2. Protect plant operating personnel from the hazards of fires in accordance with applicable building codes and fire codes.</li> <li>3. Minimize interruption of power generation due to fires.</li> <li>4. Minimize economic loss resulting from the fire damage to structures, systems and supplies in accordance with acceptable industrial fire protection practices.</li> <li>5. Protection of the environment is supported by Fire Safety Management but is implemented by BP PROG 00.02</li> </ol>	C



 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		[R009, October 22, 2014], Environmental Safety Management.	
7.13	<p>The seismic qualification of all SSCs shall meet the requirements of Canadian national or equivalent standards.</p> <p>The design shall include instrumentation for monitoring seismic activity at the site for the life of the plant.</p>	<p>There are no changes in the text of this requirement.</p> <p>Seismic qualification of all SSCs is reviewed against requirements of Canadian national or equivalent standards, and is therefore not assessed further in this clause.</p> <p>As identified in Safety Factor 3: Equipment Qualification; the current governing documents do not address the need for recording equipment to be installed in the plant to satisfy the intent of clause 6.5.6 of CSA N289.1-08 and the specific requirement stated in clause 6.5.6.3 of CSA N289.1-08 to record all significant earthquake data. It would not be possible to satisfy the overall intent of these clauses (i.e., impact on fatigue usage factor and loss of service life) without earthquake recording equipment in the plant, so this is also identified as a gap. Clause 6.5.6.4 of CSA N289.1-08 requires data collected from monitoring instruments installed at different levels in the plant to be compared with the design floor response spectra to assess if the design stress levels have been exceeded. As identified in Safety Factor 3 (see SF3-4 and SF3-2) a free field accelerometer has not been installed on the site to confirm a seismic event has occurred. Additionally, earthquake monitoring instrumentation is not installed that would provide accurate earthquake records to confirm that the plant is fit for continued operation following an earthquake (Gap).</p> <p>Bruce A and B do not have any seismic instrumentation. However, Bruce Power relies on a regional seismic monitoring network called the Southern Ontario Seismograph Network (SOSN). One station is provided to detect ground</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>motion within 20 km of the Bruce site. The process for identifying seismic activity is outlined in the Bruce B Abnormal Incidents Manual [NK29-AIM-03600.1, Rev. 056]. In addition, Bruce Power has arrangements with the Geological Survey of Canada to be informed should an earthquake greater than magnitude 5 occur within 500 km, the reporting requirement of CNSC regulatory document S-99. (REGDOC 3.1.1, which supersedes S-99 states that "The licensee shall report on ...the occurrence of any unusual external events (flood, fires, earthquakes, etc.) at or near the site that require further inspection to verify its effect on NPP structures, systems and components.")</p>	
7.13.1	<p>The design authority shall ensure that seismically qualified SSCs important to safety are qualified to a design-basis earthquake (DBE), and ensure that they are categorized accordingly. This shall apply to:</p> <ol style="list-style-type: none"> <li>1. SSCs whose failure could directly or indirectly cause an accident leading to core damage</li> <li>2. SSCs restricting the release of radioactive material to the environment</li> <li>3. SSCs that assure the subcriticality of stored nuclear material</li> </ol>	<p>A new requirement for a beyond design basis earthquake (BDBE) that meets the requirements for identification of DEC is introduced.</p> <p>Seismic qualification of Bruce B components is assessed in Safety Factor 3 : Equipment Qualification.</p> <p>The primary procedure identified in Design Management (Clause 4.9.1) [BP-PROC-00335, Rev.7], that implements the seismic qualification process is the Bruce Power Seismic Qualification Standard [DPT-PDE-00017, Rev. 5]. This procedure describes the engineering and administrative processes for preserving the seismic qualification of the systems, structures and components. It outlines the basis of qualification of Bruce B, noting in section 4.1.2 that "The original seismic qualification of the Bruce B followed the criteria of Seismic Qualification of Safety-related Systems, [NK29-DG-03650-002] which invokes CSA N289.3 and CSA N289.4.</p> <p>In accordance with the Bruce Power Seismic qualification</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>4. SSCs such as radioactive waste tanks containing radioactive material that, if released, would exceed regulatory dose limits</p> <p>The design of these SSCs shall also meet the DBE criteria to maintain all essential attributes, such as pressure boundary integrity, leak-tightness, operability, and proper position in the event of a DBE.</p> <p>The design shall ensure that no substantive damage to these SSCs will be caused by the failure of any other SSC under DBE conditions.</p> <p>Seismic fragility levels shall be evaluated for SSCs important to safety by analysis or, where possible, by testing.</p> <p>A beyond-design-basis earthquake (BDBE) shall be identified that meets the requirements for identification of DEC as described in section 7.3.4. SSCs credited to function during and after a BDBE shall be demonstrated to be capable of performing their intended function under the expected conditions. Such demonstration shall provide high confidence of low probability of failure (HCLPF) under BDBE conditions for these SSCs. This demonstration need not be seismic</p>	<p>standard [DPT-PDE-00017, Rev. 2], clause 3.1.1, for Bruce B, the Design Basis Earthquake (DBE) is expressed in the form of a generic response spectra (90th percentile) derived from a study of response spectra recorded of large earthquakes and normalized to a site-specific peak ground acceleration. The peak ground acceleration of 0.05g was selected to correspond to an occurrence rate of less than 1E-3 per year. The current peak ground acceleration does not appear to satisfy guidance provided in this clause (7.13.1 of REGDOC-2.5.2), which defines a Design Basis Earthquake (DBE) with a "probability of occurrence of 1E-4/y by a design factor defined in the standard ASCE 43-05". This DBE definition is consistent with CSA N289.3-10, clause 3.1 which states the DBE states "an engineering representation of potentially severe effects at the site due to earthquake ground motions having selected probability of exceedance of 1E-4/y or such a probability level as is acceptable to the authority having jurisdiction". To further this, the minimum design ground response spectra is defined in CSA N289.3-10 clause 4.2 which states the standard-shape ground response spectrum anchored to a peak ground acceleration of 0.1g on rock. Bruce Power has received a formal interpretation of Clause 4.2 of CSA Standard N289.3-10 which states that the intent of the clause is applicable only to the design of SSCs of new nuclear power plants [NK29-CORR-00531-12453]. However, given the purpose of the PSR is to assess the plant against modern requirements, this is considered a gap against the guidance in this clause (Gap 1). It is recommended in Safety Factor 3 (Gap SF3-6) that the governing procedure [DPT-PDE-00017, Rev.2] and its implementing documents [NK29-DG-03650, Rev.7] be updated to reflect the latest requirements of CSA N289.1 (i.e. the 1E-4 requirement for the definition of the DBE), including</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>qualification by testing.</p> <p>Guidance</p> <p>The seismic design of an NPP should account for:</p> <ul style="list-style-type: none"> <li>technical safety objectives and corresponding load categories</li> <li>seismic input motion</li> <li>seismic classification</li> <li>structural layout criteria</li> <li>seismic analysis and design of structural systems, subsystems and equipment</li> <li>seismic testing and instrumentation</li> </ul> <p>Design and beyond design load categories are defined to demonstrate structural performance in operational states, DBAs and DECs. In addition, beyond design load categories are considered for structural performance in DECs. Earthquake load is not part of the normal load category corresponding to normal operation. Site design earthquake load, according to the CSA N289 series on seismic design and qualification, is defined under the severe load category</p>	<p>the 2014 update (see Safety Factor 3 for further details).</p> <p>Guidance for conduct of seismic qualification is provided in Bruce Power Seismic Qualification Standard [DPT-PDE-00017, R005, July 04, 2012]. This procedure describes the engineering and administrative processes for preserving the seismic qualification of the systems, structures and components. It outlines the basis of qualification of Bruce B, noting in section 4.1.2 that "The original seismic qualification of the Bruce B followed the criteria of Seismic Qualification of Safety-related Systems, NK29-DG-03650-002 [NK29-DG-03650-002-R007], which invokes CSA Standards CAN3-N289.3 and N289.4. The general scope of seismic qualification is described in the Bruce B Safety Report. Bruce Power is committed to preserving seismic qualification for Bruce B in accordance with NK29-DG-03650-002."</p> <p>The general safety requirements for, identified for the seismic qualification of safety related systems, per section 2.0, of the Bruce B design guide [NK29-DG-03650-002, Rev.7] states the general philosophy for common mode incidents. This design guide requires that:</p> <ol style="list-style-type: none"> <li>(1) The capability to shut down the reactor is maintained;</li> <li>(2) The capability to ensure the reactor remains shutdown be maintained;</li> <li>(3) The capability to remove decay heat be maintained;</li> <li>(4) The capability to limit release of radioactivity from containment be maintained;</li> <li>(5) The capability to monitor the status of the nuclear steam supply be maintained;</li> </ol>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>corresponding to AOO. A DBE is defined as a part of the abnormal or extreme load category corresponding to DBA. BDBE load should be considered under DEC.</p> <p>Seismic input motion, derived from the DBE, should be based on seismicity and geologic conditions at the site and expressed in such a manner that it can be applied for the qualification of SSCs. The DBE is defined by multiplying the mean site specific uniform hazard spectrum with a probability of occurrence of 1E-4/yr by a design factor, defined in the standard ASCE 43-05, Seismic Design Criteria for Structures, Systems and Components in Nuclear Facilities. The probability of occurrence of the defined DBE is therefore equivalent to the probability of DBAs. A minimum seismic input motion, consistent with national or international standards, should be considered in the design phase for the DBE. The minimum seismic input motion should take into account frequencies of interest for SSCs.</p> <p>Structural layout criteria, including structural separation, should follow best engineering practices and lessons learned from past earthquakes.</p> <p>Modelling of soil-structure interaction (SSI) should</p>	<p>(6) Systems other than the reactor proper containing significant amounts of radioactivity must not be damaged to such an extent as to lead to radioactive releases above allowable limits; and</p> <p>(7) A seismically induced loss-of-coolant accident be prevented.</p> <p>The above capabilities must be retained in the event of an earthquake.</p> <p>DPT-PDE-00017 also calls up equipment specification B-SPEC-01370-00001 and B-SPEC-01370-00002 for seismic qualification of equipment. A more recent specification, B-SPEC-01370-00003, has also been produced that includes qualification for different mounting conditions (where this is known) and is referenced in the first two specification documents in this series.</p> <p>The other main procedure is BP-PROC-00500, Control of Unsecured Equipment in Seismically Qualified Areas [B-SPEC-01370-00002], which is used during plant operations and maintenance to ensure that any equipment used is properly secured so it would not damage nearby qualified equipment should an earthquake occur.</p> <p>The seismic design philosophy is presented in section 2.5.2 of Part 2 of the Safety Report. Dynamic analyses of structures were done based on both lumped mass and finite element models to determine the predominant frequencies and modal displacements of the structures. The seismic response of the structures was determined by modal analysis using both the artificial time history and the response spectra method as seismic input. An artificial time history motion, whose response spectra curve envelopes the design ground</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>be based on geotechnical investigation and taking into account the random nature of soil material properties and inherent uncertainties incorporated in soil constitutive models used in the analysis. To account for uncertainties in soil properties a range with at least three values (upper limit, best estimate and lower limit) should be taken into account in the analysis according to CSA N289.3, Design procedures for seismic qualification of nuclear power plants, clause 5.2.3.</p> <p>The analysis of SSI should take into account all effects due to kinematic interaction (effect of applied seismic ground motion on massless structure) and inertial interaction (inertial forces developed in the structure due to the seismic ground motion). The detail and sophistication of soil-structure models should be in accordance with the purposes of the analyses. The frequency range of interest determines aspects of the structure model and the SSI model parameters.</p> <p>The frequency range of interest should be based on the combination of the frequency range of the earthquake input, the soil properties, the frequency range of building response (including response of subsystems modelled in the main building or structure model), and the frequency range of the response parameter of interest.</p>	<p>response spectra curves, was developed. This time history ground motion was applied as input in the seismic analyses of the nuclear structures to produce acceleration floor response spectra. These floor response spectra were applied as input for the seismic qualification of seismically qualified equipment and systems. Details of seismic analysis and qualification of the reactor assembly are provided in section 2.5.2.3 of Part 2 of the Safety Report. Specific safety related systems that are necessary for the orderly shutdown of the reactor, for the maintenance of the reactor in the safe shutdown state for an indefinite period, and for the removal of decay heat from the fuel for an indefinite period, have been designed and constructed to withstand the specified earthquake. In addition, non-qualified systems whose failure could cause the failure of qualified systems have been seismically restrained. The list of systems and structures specified as seismically qualified and their level of qualification is provided in Seismic Qualification of Safety-Related Systems Design Guide, NK29-DG-03650-002. The Design Guide also specifies the basic design approach. Since the HT system is designed to withstand a DBE, a DBE will not cause a loss of coolant accident. A loss of coolant accident coincident with a DBE is not part of the design basis.</p> <p>A Probabilistic Seismic Hazard Assessment was done for the Bruce B site in 2011 [NK29-03500.8 P NSAS, Rev.1] which does provide information about earthquakes beyond the DBE level. The Seismic Hazard Assessment does not however identify a specific BDBE or identify requirements for DEC's, as required by this clause. Compliance with the new requirement for a BDBE introduced in this clause cannot be confirmed. Therefore, it is assessed as gap (Gap 2).</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Refined finite element meshes and increased analytical rigor are required to transmit higher frequencies through the analytical models.</p> <p>Damping ratios for structural systems and sub-systems should be taken into account according to recognized standards such as ASCE 43-05 and CSA N289.3. For generating the in-structure response spectra to be used as input to the structure mounted systems and components, Response Level 1 damping of the structure is more appropriate unless the structure response generally exceeds demand over capacity factor given in ASCE 43-05.</p> <p>The seismic design of structural systems should be categorized according to seismic design category (SDC) 1 to 5 as per ASCE 43-05.</p> <p>SDC 1 and 2 structural systems should be in accordance with the National Building Code of Canada, Division B, Part 4. According to the Code, SDC 1 should be as normal and SDC 2 as post-disaster.</p> <p>All structures important to safety are classified as SDC 5. However, the designer may still classify some structures as SDC 3, 4 and 5 provided that</p>	<p>Although it is noted, in accordance with clause 5.2.4.2 CSA N289.1-08 (R2013) and clause 8.2 of CSA N289.3-10 to evaluate beyond design basis events as being applicable to new plants, not existing plants.</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>they include proper justification. Guidance on SDC 3, 4 and 5 (if SDC 3 and 4 are used) structural systems are provided as follows:</p> <ul style="list-style-type: none"> <li>for concrete containment, the design should be based on the American Society of Civil Engineers, ASCE 43-05 (SDC 5, limit state D) and CSA N287.3, Design Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants</li> <li>for steel containment, the design should be based on ASCE 43-05 (SDC 5), 2010 ASME Boiler and Pressure Vessel Code, Section III: Rules for Construction of Nuclear Power Plant Components, Division 1, Subsection NE: Class MC Components and U.S. NRC Regulatory Guide 1.57, Design Limits and Loading Combinations for Metal Primary Reactor Containment System Components</li> <li>for concrete and steel safety related structures the design should be based on ASCE 43-05 (SDC 5, limit state D) and CSA N291, Requirements for Safety-Related Structures for CANDU Nuclear Power Plants</li> </ul> <p>For all safety design categories in an NPP, ductility requirements should be in accordance with CSA-A23.3, Design of Concrete Structures for concrete structures and CSA S16, Design of</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Steel Structures for steel structures assuming that the structures are ductile or type D. These ductility requirements should provide margins for the BDBE.</p> <p>Sub-system analysis should follow the guidance presented for structural systems with the following criteria specific to sub-system supports:</p> <ul style="list-style-type: none"> <li>• in-structure response spectra</li> <li>• in-structure time response histories</li> </ul> <p>The methods of defining in-structure response spectra or in-structure time-histories as well as application of this seismic input to sub-systems and components should be in accordance with ASCE 04, Seismic Analysis for Safety-Related Nuclear Structures.</p> <p>Multiple support seismic input of sub-systems and components should take into account their inertial and kinematic components. The analysis should follow ASCE 04 or CSA N289.3, Design procedures for seismic qualification of nuclear power plants.</p> <p>Determination of the number of earthquake cycles</p>		



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>for sub-system analysis should be in accordance with U.S. NRC NUREG-0800, Standard Review Plan, section 3.7.3, Seismic Subsystem Analysis as well as seismic analysis of above-ground tanks.</p> <p>Seismic design of sub-systems and components should be in accordance with ASCE 43-05 section 8.2.3 which follows ASME Code.</p> <p>For equipment qualified by testing, multi-axis, multi-frequency testing is acceptable for the DBE in accordance with the requirement of IEEE 344-2004 – IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations and that the testing response spectrum should be at least a factor of 1.4 times the required response spectrum throughout the frequency range. Any deviation from this should be conservatively justified on a case-by-case basis.</p> <p>Any evaluation for BDBE should utilize the methodology in the Electrical Power Research Institute, (EPRI) TR-103959, Methodology for Developing Seismic Fragilities to determine if a HCLPF goal is met.</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Seismic instrumentation design should follow CSA-N289.5, Seismic Instrumentation Requirements for Nuclear Power Plants and Nuclear Facilities which itemizes the requirements for single and multiple unit site seismic instrumentation.</p> <p>Beyond-design-basis margin should be such that seismically induced SSC failure probabilities do not contribute to the total core damage frequency and small and large release frequency to the extent that they do not meet the safety goals. To support meeting the safety goals, the acceptance criterion for BDBE should demonstrate that the plant HCLPF is at least 1.67 times the DBE.</p> <p>Assessment and validation of margins for beyond-design-basis earthquakes should be considered, including the metric HCLPF.</p> <p>The seismic isolation of SSCs is an acceptable design approach to limit seismic demand. Seismic isolation devices should be designed, manufactured and installed to withstand a seismic action defined by a DBE without any failure, preserving its mechanical resistance and full load bearing capacity during and after the earthquake. Moreover, the devices and the whole structural system should be designed to withstand a BDBE</p>		



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>up to 2 times the spectral accelerations of the DBE without major damage and preserving its function. It includes the provisions to accommodate the structural displacements up to 2 times the displacements under DBE conditions.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"><li>• American National Standards Institute (ANSI)/American Nuclear Society (ANS) Standard 2.26, Categorization of Nuclear Facility Structures, Systems, and Components for Seismic Design, La Grange Park, Illinois, reaffirmed 2010.</li><li>• American Society of Civil Engineers (ASCE), 04-98, Seismic Analysis of Safety-Related Nuclear Structures, Reston, Virginia, 2000.</li><li>• ASCE/Structural Engineering Institute, 43-05, Seismic Design Criteria for Structures, Systems and Components in Nuclear Facilities, Reston, Virginia, 2005.</li><li>• American Society of Mechanical Engineers (ASME), Boiler and Pressure Vessel Code Section III, Division 1- Subsection NE, Rules for Construction of Nuclear Facility</li></ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Components, New York, 2010.</p> <ul style="list-style-type: none"> <li>• CSA Group, N287 series on requirements for concrete containment structures for CANDU nuclear power plants.</li> <li>• CSA Group, N289 series on seismic design and qualification of nuclear power plants.</li> <li>• CSA Group, A23.3, Design of Concrete Structures, Toronto, Canada.</li> <li>• CSA Group, S16, Design of Steel Structures, Toronto, Canada.</li> <li>• CSA Group, N291, Requirements for Safety-Related Structures for CANDU Nuclear Power Plants, Toronto, Canada.</li> <li>• Electric Power Research Institute, TR-103959, Methodology for Developing Seismic Fragilities, Palo Alto, California, 1994.</li> <li>• European Standard, EN-15129, Anti-seismic Devices, European Committee for Standardization: Brussels, 2009.</li> <li>• European Standard, EN-1337-3, Structural Bearings – Elastomeric Bearings, European Committee for Standardization: Brussels, 2000.</li> <li>• European Standard, EN 1337-1, Structural Bearings – General Design Rules, European Committee for Standardization: Brussels, 2000.</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>IEEE, 344, IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, Piscataway, New Jersey, 2004.</li> <li>NRC, National Building Code of Canada, Ottawa, Canada, 2010.</li> <li>U.S. NRC, Regulatory Guide 1.57, Design Limits and Loading Combinations for Metal Primary Reactor Containment System Components, Washington, D.C., 2007.</li> <li>U.S. NRC, Regulatory Guide 1.91, Evaluations of Explosions Postulated to Occur on Transportation Routes Near Nuclear Power Plants, Washington, D.C., 1978.</li> <li>U.S. NRC, NUREG-0800, section 3.7.3, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR edition- Seismic Subsystem Analysis, Washington, D.C., 2007.</li> </ul>		
7.14	<p>In order to maintain the NPP within the boundaries of the design, the design shall be such that the SSCs important to safety can be calibrated, tested, maintained and repaired (or replaced), inspected, and monitored over the lifetime of the plant.</p> <p>These activities shall be performed to standards commensurate with the importance of the</p>	<p>A new requirement has been added to have design provisions to gather baseline data in order to support maintenance ...etc.</p> <p>Each process and nuclear measurement loop that is essential for the operation of a special safety system is redundantly designed, usually triplicated, such that a single loop component or power supply failure will not incapacitate or spuriously invoke operation of the special safety system. This triplication and redundancy also allows each channel to be tested or repaired as necessary without tripping the</p>	IC



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>respective safety functions of the SSCs, with no significant reduction in system availability or undue exposure of the site personnel to radiation.</p> <p>SSCs that have shorter service lifetimes than the plant lifetime shall be identified and described in the design documentation.</p> <p>In cases where SSCs important to safety cannot be designed to support the desirable testing, inspection, or monitoring schedules, one of the following approaches shall be taken:</p> <ol style="list-style-type: none"> <li>1. Proven alternative methods, such as surveillance of reference items, or use of verified and validated calculation methods, shall be specified.</li> <li>2. Conservative safety margins shall be applied, or other appropriate precautions shall be taken, to compensate for possible unanticipated failures.</li> </ol> <p>Details of alternate approaches to SSC monitoring shall be provided in the design documentation.</p> <p>The design shall provide facilities for monitoring</p>	<p>system.</p> <p>Bruce B has extensive testing programs to demonstrate that the special safety systems meet their ongoing reliability requirements. Section 03.5 of the Bruce B Operating Policies &amp; Principles (OP&amp;Ps) [BP-OPP-00001, R019] specifies that the testing program is required on any system which is not normally operating but is required to function, in the event of a system failure, to control reactor power, cool the fuel, or contain radioactivity. The testing programs for these systems are consistent with reliability objectives established in system design.</p> <p>The process for development of Life Cycle Management Plans for Systems, Structures, or Components is outlined in Life Cycle Management for Critical SSCS [BP-PROC-00400, R002]. The relevant technical information (e.g., age-related degradation mechanisms, replacement and major overhaul tasks/frequencies, current conditions, etc.) from the Technical Basis Assessments (TBA), Performance Monitoring Plans (PMP), Health Reports and other data sources and use this information to document the recommended long-term mitigation options for the SSCs. The recommended options will then be included in the Asset Life Projections &amp; Options document (ALP&amp;O). The ALP&amp;O process adds to the recommended long-term options key information needed in business strategy decisions and implemented through the LCMPs. Critical components are listed on the Performance Monitoring Equipment List within the approved Performance Monitoring Plan [System and Component Performance Monitoring Plans DPT-PE-00008, R007, February 18, 2016; /System and Component Performance Monitoring Walkdowns DPT-PE-00009, R002, September 30, 2015;</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>chemical conditions of fluids, and of metallic and non-metallic materials. In addition, the means for adding or modifying the chemical constituents of fluid streams shall be specified.</p> <p>The design shall identify the needs for related testing when specifying the commissioning requirements for the plant.</p> <p>The design shall provide the means to gather baseline data, in order to support maintenance-related testing, inspection and monitoring.</p> <p>Guidance</p> <p>While in-service testing, maintenance, repair, inspection and monitoring take place primarily during the operating phase of the plant's lifecycle, the NPP is designed to permit the effective implementation of these activities during operation. In particular, the reactor core should be designed to permit the implementation of a material surveillance program to monitor the effects of service conditions on material properties throughout the operating life of the reactor.</p>	<p>System Health Reporting, DPT-PE-00010, R007, March 3, 2016] and meet the criteria specified in Component Categorization [BP-PROC-00666, R004, October 1, 2015]. Life Cycle Management is one of the key elements of BP-PROG-11.01 [R005, December 16, 2015, Equipment Reliability Program. The Performance Monitoring procedure [BP-PROC-00781] provides the basis and expectations for the Equipment Performance Monitoring Process at Bruce Power.</p> <p>Design provisions are implemented to minimize the radiation doses to workers as well as access to components and systems that require periodic inspections per N285.4, N285.5 and N287.7 which also covers gathering baseline data through inaugural inspections before the components are put in service. As much of the equipment, both safety and process, as possible was placed outside containment to allow on-power maintenance and testing. All safety system equipment that requires testing or maintenance is accessible on-power from outside containment (e.g., SDS1 and SDS2 instrumentation, poison tank sampling, shutoff rod drives, etc.). In general, for systems or structures that cannot be tested, inspection or monitoring programs are in place. For example, corrosion in systems is not measured directly but is done through chemical sampling, irradiation of material samples in the core. In order to detect any leakage from the pressure tubes into the calandria tubes, the annulus gas system, humidity is continuously monitored. If testing or monitoring is not feasible, calculations are performed. For example, reactor vault atmosphere mixing is used as a basis for the adequacy of the hydrogen ignition system. Systems that require sampling during their normal usage are provided with sampling systems, e.g., heat transport sampling and</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design should establish a technical basis of SSCs that require in-service testing, maintenance, repair, inspection and monitoring.</p> <p>The development of strategies and programs to address in-service testing, maintenance, repair, inspection and monitoring is a necessary aspect of the plant design phase. The strategies and programs to be implemented for these in-service activities should be developed so as to ensure that plant SSCs remain capable and available to perform their safety functions. The design should incorporate provisions recognizing the need for in-service testing, maintenance, repair, inspection and monitoring, as well as to permit the repair, replacement and modification of those SSCs likely to require such actions, due to anticipated operating conditions. In addition, activities which need to be carried out during the construction and commissioning phases should be identified, in order to provide a meaningful baseline data of the plant, at the outset of its operating life.</p> <p>The strategies should include well-planned and effective programs for evaluating and trending SSCs performance, coupled with an optimized preventive maintenance program. The strategies and programs should demonstrate consideration of the following:</p>	<p>moderator sampling as described in Section 11.2.2 of Part 2 of the Safety Report.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>the intended design life, design loading conditions, operational requirements and safety significance of SSCs</li> <li>the requirements of applicable codes, standards and regulations</li> <li>the responsibilities of the designer, vendor, construction organization, operating organization and contractors</li> <li>interdependence of SSCs important to safety and possible effects of failures of SSCs of lower safety significance on SSCs of higher safety significance</li> <li>plant design, layout and the accessibility of SSCs during construction, commissioning, and during the intended service life</li> <li>monitoring, inspection and testing programs used during the construction, commissioning and service for NPPs of similar or identical design and layout</li> <li>technologies and methodologies available for monitoring, inspection and testing, as well as for the repair, replacement or modification of SSCs</li> <li>research and development activities</li> <li>operating experience</li> <li>human factors</li> <li>training and qualification of personnel</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>availability of adequately trained and qualified personnel</li> <li>availability of required laboratory or testing facilities and equipment</li> </ul> <p>If risk informed in-service inspection methodologies are used when defining the scope of an inspection program, the methodology should be clearly documented.</p> <p>SSCs important to safety should be designed and located to make surveillance and maintenance simple, to permit timely access, and in case of failure, to allow diagnosis and repair, and minimize risks to maintenance personnel.</p> <p>Means provided for the maintenance of SSCs important to safety should be designed such that the effects on the plant safety are acceptable.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>ASME, Boiler and Pressure Vessel Code-2010, Section XI, Rules for Inservice Inspection of</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Nuclear Power Plant Components, New York, 2010.</p> <ul style="list-style-type: none"> <li>• CNSC, RD-334, Aging Management for Nuclear Power Plants, Ottawa, Canada, 2011.</li> <li>• CNSC, RD/GD-210, Maintenance Programs for Nuclear Power Plants, Ottawa, Canada, 2012.</li> <li>• CSA Group, N287.7, In-service Examination and Testing Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, Toronto, Canada.</li> <li>• CSA Group, N285.4, Periodic inspection of CANDU nuclear power plant components, Toronto, Canada.</li> <li>• CSA Group, N285.5, Periodic inspection of CANDU nuclear power plant components, Toronto, Canada.</li> <li>• CSA Group, N291, Requirements for Safety-Related Structures for CANDU Nuclear Power Plants, Toronto, Canada.</li> <li>• IAEA, Safety Guide NS-G-2.6, Maintenance, Surveillance and In-Service Inspection in Nuclear Power Plants, Vienna, 2002.</li> </ul>		
7.15.1	The NPP design shall specify the required performance for the safety functions of the civil structures in operational states, DBAs and DEC's.	A new requirement for DEC's is added. The design requirement for civil structures important to safety to meet the serviceability, strength and stability requirements for all possible load combinations under operational states and	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Civil structures important to safety shall be designed and located so as to minimize the probabilities and effects of internal hazards such as fire, explosion, smoke, flooding, missile generation, pipe whip, jet impact, or release of fluid due to pipe breaks.</p> <p>External hazards such as earthquakes, floods, high winds, tornadoes, tsunamis, and extreme meteorological conditions shall be considered in the design of civil structures.</p> <p>Settlement analysis and evaluation of soil capacity shall include consideration of the effects of fluctuating ground water on the foundations, and identification and evaluation of potential liquefiable soil strata and slope failure.</p> <p>Civil structures important to safety shall be designed to meet the serviceability, strength, and stability requirements for all possible load combinations under the categories of normal operation, AOO, DBA and DEC conditions, including external hazards. The serviceability considerations shall include, without being limited to, deflection, vibration, permanent deformation, cracking, and settlement.</p>	<p>DBAs is extended to include DEC's (new requirement).</p> <p>As discussed in section 7.4.1, the current design documentation does not consider internal events as leading to AOOs, DBAs and DEC's. This includes the design documentation for civil structures, and is therefore considered a gap (Gap).</p> <p>Section 2.5.3 of Part 2 of the Bruce B Safety Report [NK29-SR-01320-00001, R005] shows that features incorporated into the Bruce B design provide an adequate level of protection against any credible turbine generator missile. Features are incorporated into the Bruce B design provide an adequate level of protection against any credible turbine generator missile. These features include:</p> <ol style="list-style-type: none"> <li>1. Separation of the 600 V Class II switchgear, such that a single missile cannot disable both halves of the system.</li> <li>2. Reinforced concrete barriers, such that a turbine generator missile cannot strike the HT pump motors.</li> <li>3. Adoption of separation measures [NK29-DG-03650-005] such that a single missile cannot disable sufficient equipment to prevent safe shutdown, monitoring, or decay heat removal.</li> </ol> <p>It has been demonstrated by accident analyses that, after postulated pipe failures, the reactor would be safely shut down, decay heat removal capability would be available and adequate containment integrity would be maintained. Bruce Power External Hazards Assessment [K-449958-REPT-007, R01]; [NK21-CORR-00531-09809 / NK29-CORR-00531-10287] presents analysis of turbine generated missiles</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design specifications shall also define all loads and load combinations, with due consideration given to the probability of concurrence and loading time history.</p> <p>Environmental effects shall be considered in the design of civil structures and the selection of construction materials. The choice of construction material shall be commensurate with the designed service life and potential life extension of the plant.</p> <p>The plant safety assessment shall include structural analyses for all civil structures important to safety.</p> <p>Guidance</p> <p>The design authority should provide the design principles, design basis requirements and criteria, and applicable codes and standards, design and analysis procedures, the assumed boundary conditions and the computer codes used in the analysis and design.</p> <p>All internal and external hazard loads are specified in section 7.4. Earthquake design input</p>	<p>considered as potential external hazard. Phase 2 External Hazards Detailed Assessment includes turbine generated missiles analysis as documented in [K-449958-REPT-00009] and submitted to the CNSC [NK21-CORR-00531-10848 / NK29-CORR-00531-11226]. The assessment considers the potential of turbine generated missiles for damaging safety-related structures, systems, and components of the plant. The potential consequences of turbine missiles include direct effects (e.g., damage to the PHT Pump/Motor) as well as Indirect effects (e.g., impairment of vital control room functions). The missile analysis for Bruce B considered the new rotors replaced by GE during the period 2004 - 2006. The GE methodology for evaluating the probability of wheel missile generation for nuclear turbines manufactured by GE considers two fundamental failure modes that can lead to missile generation, (a) brittle fracture failures and (b) ductile tensile failures. As presented in section 4.3 of K-449958-0009, R02 [Enclosure 1 of NK21-CORR-00531-10848 / NK29-CORR-00531-11226], the potential consequences of turbine missiles include direct effects (e.g., damage to the PHT Pump / Motors) as well as indirect effects (e.g., impairment of vital control room functions). In either case, it is necessary to show that the risk from turbine missiles is acceptably small, either because design features are provided to prevent damage or because the probability of a strike by a turbine missile is sufficiently low. For Bruce B, due to the lack of protection around the electrical equipment, it is assumed that a credible turbine generator missile could strike the battery room and associated equipment, and the electrical protection relay room; consequently all Group 1 systems will be lost. The Bruce NGS B Safety Report Part 2, section 2.5.3 confirms that there is an adequate level of protection against any credible turbine generator missile that</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>loads and impacts of malevolent acts, including large aircraft crash can be found in sections 7.13 and 7.22, respectively.</p> <p>Load categories corresponding to the plant states are defined in this section so as to demonstrate structural performances as follows:</p> <ul style="list-style-type: none"> <li>• normal condition loads which are expected during the assumed design life of the NPP</li> <li>• AOO loads (or severe environmental loads)</li> <li>• DBA loads (or abnormal or extreme environmental loads)</li> <li>• DEC loads (or beyond-design loads)</li> </ul> <p>The design should identify all DEC loads considered in the structure design and provide the assessment methodology and acceptance criteria.</p> <p>The structural design should withstand, accommodate or avoid foundation settlement (total and differential), according to its performance requirements.</p> <p>The structural design should consider the impact</p>	<p>could strike on the PHT pump/motors and/or the reactivity mechanism deck area in the reactor building. Therefore, this particular scenario was screened out in Bruce NGS B during Phase I assessment. The bounding calculation of Core Damage Frequency (CDF) associated with turbine missiles striking Group 1 electrical equipment for Bruce NGS B (Section 4.3.5) showed larger value of <math>1.61\text{E-}6</math> occ./yr in comparison to Bruce A (<math>5.43\text{E-}8</math> occ./yr for Bruce A). Even though the estimated CDF (<math>1.61\text{E-}6</math> occ./yr) is higher than the screening criteria (Screening Frequency Level <math>\text{SFL} = 1\text{E-}6</math>) this specific event is a low risk contributor at Bruce NGS B compared with the internal events PRA (<math>1.6\text{E-}5</math>). In addition, the estimated CDF incorporates a significant level of conservatism in the missile probability evaluation as described in section 4.3.8 of K-449958-REPT-0009.</p> <p>The seismic qualification basis for Bruce B is provided in the Bruce Power Seismic Qualification Standard [DPT-PDE-00017, Rev. 5]. As discussed in Clause 7.13, the seismic qualification of Bruce B followed the Seismic Qualification of Safety Related Systems [NK29-DG-03650-002, Rev.7]. For Bruce B non-safety related structures, systems and components do not have to be seismically qualified for safety reasons. However, these are designed to the requirements of the National Building Code of Canada as being consistent with normal industrial standards. As noted in Part 2 of the Safety Report [NK29-SR-01320-00001, Rev.5] the effective dates of Codes and Standards (Section 1.1.5.4), the station structures have been designed and built in accordance with the requirements of the National Building code of Canada, 1975.</p> <p>Bruce B Containment Operational Safety Requirements are</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>of aging on the structure and its material. The design should include sufficient safety margins for the buildings and structures that are important to safety.</p> <p>The physical and material description of each civil structure and its base slab should include:</p> <ul style="list-style-type: none"> <li>the type of structure, and its structural and functional characteristics</li> <li>the geometry of the structures, including sketches showing plan views at various elevations and sections (at least two orthogonal directions)</li> <li>the relationship between adjacent structures, including any separation or structural ties</li> <li>the type of base slab and its arrangement with the methods of transferring horizontal shears (such as those seismically induced) to the foundation media</li> </ul> <p>Containment structure</p> <p>The design should specify the safety requirements for the containment building or system, including, for example, its structural strength, leak tightness,</p>	<p>presented in NK29-OSR-34200-00001, R000. Therefore, DEC's loads are not considered in the original structure design.</p> <p>Structural design considers the impact of ageing on structures and materials through the Plant Design Basis Management Program, BP-PROG-10.01 and its implementing procedures. In addition, the Life Cycle Management Plan for Civil Structures, B-PLAN-20000-00001, [R000, July 5, 2010] describes how system performance monitoring, which includes a review of the original design and subsequent modifications, is used to monitor ageing degradation for civil structures.</p> <p>An evaluation of the structural response of the IFB structure to temperatures in excess of the design temperature, including an assessment of the maximum credible leak rate following any predicted structural damage was performed. The IFB structural analysis was submitted to the CNSC on March 26, 2013 [NK21-CORR-00531-10341 / NK29-CORR-00531-10750] and this FAI (FAI 1.6.1) was closed following CNSC's review of the analysis [NK21-CORR-00531-10565 / NK29-CORR-00531-10965]. The analysis demonstrated that the heatup (to boiling) and subsequent cooldown cycle of the IFBs will not result in through-wall cracking of the concrete and thus will not result in draining of the IFBs. The analysis recommended that cooling mitigation measures should be initiated within the first few hours of an accident, to control the propagation of any cracks. Bruce Power noted that mitigation measures to supply water to the IFB during a BDBE have been completed, and the CNSC concluded this FAI is closed.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>and resistance to steady-state and transient loads (such as those arising from pressure, temperature, radiation, and mechanical impact) that could be caused by postulated internal and external hazards. In addition, the design should specify the safety requirements and design features for the containment internal structures, (such as the reactor vault structure, the shielding doors, the airlocks, and the access control and facilities).</p> <p>The design of the containment structure should include:</p> <ul style="list-style-type: none"> <li>• base slab and sub-base</li> <li>• containment wall and dome design</li> <li>• containment wall openings and penetrations</li> <li>• pre-stressing system</li> <li>• containment liner and its attachment method</li> </ul> <p>The design pressure of the containment building should be determined by increasing by at least 10% the peak pressure that would be generated by the DBA (refer to clause 4.49 of IAEA NS-G-1.10, Design of Reactor Containment Systems for</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Nuclear Power Plants).</p> <p>Ultimate internal pressure capacity should be provided for the containment building structures including containment penetrations.</p> <p>If the containment building foundation is a common mat slab which is not separated from the other buildings foundation, the impact should be evaluated.</p> <p>Concrete containment structures should be designed and constructed in accordance with the CSA N287 series, as applicable:</p> <ul style="list-style-type: none"> <li>• N287.1, General Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, for general requirements in documentation of design specification and design reports</li> <li>• N287.2, Material Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, for material</li> <li>• N287.3, Design Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants for design</li> <li>• N287.4, Construction, Fabrication and</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Installation Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, and N287.5, Examination and Testing Requirements for Concrete Containment Structures for Nuclear Power Plants, for containment construction and inspection</p> <ul style="list-style-type: none"> <li>N287.6, Pre-operational proof and leakage rate testing requirements for concrete containment structures for nuclear power plants, for pressure test before operation</li> </ul> <p>Steel containment structures should be designed according to the ASME Boiler and Pressure Vessel Code, Section III, Division 1, Subsection NE, Class MC Components or equivalent standard. Stability of the containment vessel and appurtenances should be evaluated using ASME Code Case N-284-1, Metal Containment Shell Buckling Design Methods, Section III, Division 1, Class MC.</p> <p>For other requirements on the design of containment structures, refer to section 8.6.2 of this regulatory document.</p> <p>Safety-related structures</p> <p>The safety-related structures other than the</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>containment should be designed and constructed in accordance with CSA N291, Requirements for safety-related structures for CANDU nuclear power plants.</p> <p>The design of other safety-related structures should include:</p> <ul style="list-style-type: none"> <li>• internal structures of reactor building</li> <li>• service (auxiliary) building</li> <li>• fuel storage building</li> <li>• control building</li> <li>• diesel generator building</li> <li>• containment shield building, if applicable</li> <li>• other safety-related structures defined by the design</li> <li>• turbine building (for boiling water reactor)</li> </ul> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>• American Concrete Institute (ACI), 349-06, Code Requirements for Nuclear Safety-</li> </ul>		





Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Related Concrete Structures &amp; Commentary, Farmington Hills, Michigan, 2007.</p> <ul style="list-style-type: none"> <li>ASME, Boiler and Pressure Vessel Code (BPVC) Section III, Division 2, Section 3, Code for Concrete Containments, New York, 2010.</li> <li>IAEA, NS-G-1.10, Design of Reactor Containment Systems for Nuclear Power Plants, Vienna, 2004.</li> <li>U.S. NRC, NUREG/CR-6486, Assessment of Modular Construction for Safety-Related Structures at Advanced Nuclear Power Plants, Washington, D.C., 1997.</li> <li>U.S. NRC, Regulatory Guide 1.76, Design Basis Tornado and Tornado Missiles for Nuclear Power Plants, Washington, D.C., 2007.</li> <li>U.S. NRC, Regulatory Guide 1.91, Evaluations of Explosions Postulated to occur on Transportation Routes near Nuclear Power Plants, Washington, D.C., 1978.</li> <li>U.S. NRC, NUREG-0800, Section 3.8.1, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Concrete Containment, Washington, D.C., 2007.</li> </ul>		
7.15.2	The design shall enable implementation of periodic inspection programs for structures important to safety in order to verify that the as-	The change is to clarify that the constructed structures meet their functional and performance requirements.	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>constructed structures meet their functional and performance requirements.</p> <p>The design shall also facilitate in-service monitoring for degradations that may compromise the intended design function of the structures. In particular, the design shall permit monitoring of foundation settling.</p> <p>Pressure and leak testing shall be conducted on applicable structures to demonstrate that the respective design parameters comply with requirements.</p> <p>The design shall facilitate routine inspection of sea, lake, and river flood defences and demonstrate fitness for service.</p> <p>Guidance</p> <p>For concrete containments, it is important to accommodate the structural integrity inspection and pressure testing for pre-operational and in-service phases. The inspection and pressure testing programs should be provided and meet the applicable requirements listed in CSA N287.6, Pre- operational proof and leakage rate testing</p>	<p>CSA N287.7-08 Periodic Inspection Program for Bruce NGS B Concrete Containment Structures and Appurtenances (excluding Vacuum Building) [NK29-PIP-21100-00001, R003, September 2014] details the Periodic Inspection Program for visual inspection of containment structures, test and inspection procedures, the inspection frequency, the components and areas to be inspected, the acceptance criteria and evaluation results. The Periodic Inspection Program for Units 0, 5-8 is comprised of the following concrete containment structures: Reactor Vaults. Fueling Machine Duct, Central Fueling Area, Pressure Relief Ducts, Pressure Relief Valve Manifold and East Service Area. Specific details of the areas to be inspected including the containment current inspection dates are presented in the corresponding appendices of NK29-PIP-21100-00001.</p> <p>CSA N287.7-08 Periodic Inspection Program for Bruce NGS 'B' Concrete Vacuum Building, NK29-PIP-25100-00001, R002, September 2014 provides the framework for visual inspection of components in the Vacuum Building. The containment side (inside) of the Vacuum Building is normally inaccessible; therefore the Internal and external inspections are conducted during Vacuum Building outages. The current period between inspections is 12 years. Deformation and distortion are monitored in terms as cracks as per BP-PROC-00815, R000 [November 16, 2012] Visual Inspection of Containment Boundary Components.</p> <p>Monitoring of foundation settlement does not appear to be a requirement in the N287 codes reviewed. However, part of the regular inspection program requires checking for misalignment and distortion, which are signs of settling. The foundations of Bruce B are constructed on bedrock that</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>requirements for concrete containment structures for nuclear power plants, and CSA N287.7, In-service examination and testing requirements for concrete containment structures for CANDU nuclear power plants.</p> <p>Special design provisions should be made to accommodate in-service inspection and pressure testing of concrete containments (e.g., providing sufficient physical access, providing alternative means for identification of conditions that can lead to degradation in inaccessible areas, or providing remote visual monitoring of high-radiation areas). Programs should be implemented for the examination of inaccessible areas, monitoring of ground water chemistry, and monitoring of settlements and differential displacements. The design should also provide for equipment and instrumentations, for example a strain gauge, to monitor stress, strain and any deformation of the structures.</p>	<p>minimizes the likelihood of any significant settling of the structures. As described in section 3.0 of Part 2 of the Safety Report, all major building and structures of the station are built on bedrock. Further details are presented in section 2.6.1 of Part 2 of Safety Report.</p> <p>As presented in Sections 6.5.1 and 6.5.2 of Part 2 of the Safety Report, an important criterion for determining the effectiveness of the containment envelope is the integrated leak rate for the period of the pressure excursion. To meet the design leakage requirements, two measures are employed. The first involves stringent design requirements to minimize the leak rate. The second is to prevent the design pressure within the containment envelope from being exceeded following a LOCA. The containment system quickly reduces the containment pressure pulse to subatmospheric level following a large energy release within the containment envelope and hence minimizes uncontrolled releases to the outside environment. A detailed performance assessment of the containment system is given in Part 3 of the Safety Report. The pressure in the vacuum building is normally maintained at 6.9 to 13.8 kPa(a) (1.0 to 2.0 psia) and at slightly sub-atmospheric in the rest of the containment envelope.</p> <p>The containment structures were subjected to the positive proof test (as well as negative proof test) pressures to confirm the structural integrity of containment. These proof tests were performed, in stages, as subsequent units were completed and commissioned in one time pre-operational tests. Containment integrity is also tested in periodic in-service elevated pressure tests. The acceptance leakage rate</p>	



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00


Article No.	Clause Requirement	Assessment	Compliance Category
		<p>for the containment envelope, except for the vacuum building, is set at 2% of the contained air mass per hour at 82.7 kPa(g) (12 psig). The vacuum building acceptance leakage rate is set at 2% of contained air mass per hour at 48.3 kPa(g) (7 psig). Operational targets are set at lower values. Leakage rate tests for the vacuum building and upper chamber are conducted periodically at 7 kPa(a) (1 psia). The acceptance leakage rates at metric standard conditions for the main volume of the vacuum building is 200 kg/hr (100 scfm) and for the upper chamber 6 kg/hr (3 scfm).</p> <p>The pressure and leak testing requirements for containment envelope are provided in section 2.4 of Negative Pressure Containment System Design Manual NK29-DM-34200-001.</p> <p>Bruce B Periodic Inspection Plan for Unit 0 and Units 5 to 8 Containment Components [NK29-PIP-03642-00001, R002, October 2015] outlines the inspection plan for containment boundary components at Bruce B as required by the PROL 18.00/2020, Licence Condition 6.1, the Licence Conditions Handbook, LCH-BNGS-R000, Section 6.1 and CSA N285.5-08 Clause 4.6 Program Documents. Following the issue of CSA Standard N285.5-08, updates were made to comply with the requirements of the new edition in March 2009. Based on the comments received from Regulator on the initial issue (R001A) of the inspection plan, further changes were made to comply with the CNSC request to include the effects of thermal stresses in functional loads. Bruce B is now in the third ten-year inspection cycle for containment boundary components and Bruce Power intends to revisit this plan at the end of this cycle to further optimize inspection selections and make necessary changes based in inspection experience. This revision incorporates inspection locations</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>from the modification of new connection points in the Emergency Filtered Air Discharge System as communicated in NK29-CORR-00531-12335 and addition/removal of several components for Bruce B based on implementation experience obtained to date which has resulted changes to locations selected for periodic inspections. This document complies with CSA N285.5-08 Periodic inspection of CANDU nuclear power plant containment components. The components and systems subject to inspection are identified in section 3 and section 4 of the plan. The periodic inspection plan establishes the requirements for common systems (Unit 0) and reactor specific systems (Units 5 to 8). Unit 0 comprises of all containment systems and components that are common to Units 5, 6, 7, and 8, i.e., the failure of which will simultaneously affect the containment integrity of all four units or the common pressure suppression and filtered venting systems. These components are associated with the Vacuum Building; the Pressure Relief Valve Manifold; the Pressure Relief Duct; the Fuelling Duct; the Central Service Area and the Fuelling Facilities Auxiliary Areas, and include systems such as the Emergency Cooling Water Systems, Vacuum System, Water Spray Dousing System, Emergency Filtered Air Discharge System, etc. The inspection areas for systems and components that affect only one unit are covered under the unit-specific Periodic Inspection Plans for Units 5, 6, 7, or 8. The appendices list systems and components that are subject to inspection, their locations, items selected for periodic examination, inspection categories, loadings where applicable and inspection methods to be used [NK29-PIP-03642-00001].</p> <p>The Operational Safety Requirements for Bruce B Containment System [NK29-OSR-34200-00001, R000]</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		describes the operational requirements for containment system. The bases of the OSR are the Safety Analysis Limits which are derived from the safety analysis and supporting documents. The Safety Analysis Limits define the minimum hardware functional and performance requirements and limiting process parameter values in the hardware subsystems, and are used to ensure there is sufficient margin to the nominal automatic actuation setpoints to account for instrument loop uncertainty.	
7.15.3	<p>The lifting and handling of large and heavy loads, particularly those containing radioactive material, shall be considered in the NPP design. This shall include identification of the large loads, traversing routes and situations where they need to be lifted over areas of the plant that are critical to safety. The design of all cranes and lifting devices shall, therefore, incorporate large margins, appropriate interlocks, and other safety features to accommodate the lifting of large loads.</p> <p>The drop of large loads lifted and handled in areas where there are systems and components that are important to safety shall be taken into account in the design. The potential load due to the large load drop shall be taken into account in the analysis of DBAs.</p>	<p>A new requirement for consideration of drop of large loads in areas where there are systems and components important to safety is introduced.</p> <p>The design of Bruce A and B recognizes the need for lifting heavy loads in a variety of locations and suitable cranes have been installed to perform these lifts as described in Part 2 of the Safety Report. However identification of traversing routes together with justification for safety is not available in the design documentation. Therefore, it is assessed as a gap. (Gap 1)</p> <p>The requirements for safe, efficient and effective execution of rigging and lifting activities at all Bruce Power Facilities are described in BP-PROC-00586 [R006, August 6, 2014] Control of Lifting Activities.</p> <p>A description of the lifting and handling of large and heavy loads together with the traversing roads is presented in Part 2 of the Safety Report as follows:</p> <p>A 75-ton seismically qualified crane serves the HT pumps and the reactivity control units. The crane operates on rails that extend about 9.2 m (30 ft) beyond the reactor building. In</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>the north end of the building, the crane has access to grade level.(Section 3.2.3)</p> <p>Two seismically qualified 10.5 ton cranes located in the reactor vault, one at each end of the reactor, can be used during reactor shutdown to move heavy equipment such as fuel channel maintenance tooling and fuelling machine components removed for maintenance. (Section 3.2.3)</p> <p>An 18 Mg (20 ton) crane serves to move irradiated fuel within the receiving and secondary bays. Irradiated fuel from the primary irradiated fuel storage bay is conveyed through the fuel transfer duct and received in the receiving bay. From here, it is moved by the 18 Mg (20 ton) crane into the secondary irradiated fuel storage bay. A 90 Mg (100 ton) crane operates on the rails to handle irradiated cobalt rod shipping flasks and dry fuel storage casks. (Section 3.7.2.2).</p> <p>A 90 Mg (100 ton) bridge crane serves the north, deep section of the bay for irradiated fuel shipping cask handling and loading, and spans an adjacent area for loading these casks onto road vehicles. The crane is also used to move the casks into a cask decontamination area before and after loading with irradiated fuel. The south end of the irradiated fuel bay is served by a 1.8 Mg (2 ton) crane that is used in defected fuel inspection and canning operations. (Section 10.2.2.2.2)</p> <p>In the secondary irradiated fuel bay a jib crane and tray handling tool are used to lower the trays onto a cable driven cart. The secondary irradiated fuel bay has a purification and cooling system and is serviced by a bridge crane that travels over the length of the bay. The tray handling tools on the bridge crane pick up and transfer trays from the receiving bay</p>	



 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>to stacks in the stacking frames in the secondary irradiated fuel storage bay. The cranes can handle flask decontamination and loading of fuel shipping flasks. (Section 10.2.5.2.4)</p> <p>The cranes are appropriate for the tasks and incorporate large margins and interlocks.</p> <p>Limited fuel handling system failures are discussed in Appendix 1 of Part 3 of the Safety Report, i.e., fuel storage tray drop in the primary irradiated fuel bay. The summary of total doses for fuel handling failures is provided in Table 1-26 of Part 3 of the Safety Report [NK29-SR-01320-00002, Rev.5]. The accident scenarios listed are analyzed to determine the timing and extent, if any, of fuel overheating and fission product release to containment, as well as corresponding public doses. Transportation accidents within the plant structures and away from the plant have been analyzed and documented in Bruce Power External Hazards Assessment [K-449958-REPT-0007, R01]; [NK21-CORR-00531-09809 / NK29-CORR-00531-10287]; however the assessments are limited to transportation vehicles.</p> <p>Due to the absence of an analyzed safe load path, lifting restrictions have been imposed with regards to lifting heavy loads over some areas of the plant [Memorandum from F. Wolsey to D. Andrews "lifting Restrictions: Powerhouse Cranes, Bruce A&amp;B", File #76100, May 24, 2013] [Memorandum from R. Dunn to D. Andrews "Reactivity Deck Crane Restriction, Bruce A&amp;B", File #:76112-CR3, Oct. 31, 2013]. The stress reports for Bruce A and Bruce B reactivity decks to calculate their capacities do not include accidental dropping of PHT pump motors during craning operations.</p>	



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>The reactivity deck above the Calandria in Bruce B was analyzed for its perforation and dynamic adequacy with no catastrophic collapse to bear the impact caused by accidental dropping of a PHT pump motor during craning operations over the reactivity deck [NK29-CALC-31360-00001, R00, October 23, 2013]. The focus was on the possibility of perforation through the Bruce B reactivity deck and its response to the impact. This calculation is carried out to establish the maximum drop height of 110,000 lb PHT pump motor. The analysis in this calculation is based on the existing AECL calculation carried out for the 55000 lb Cobalt flask with 27 feet drop height. The focus is on the possibility of perforation through the reactivity deck and its response to the impact. The drop height of the 110,000 lb (66 inch contact diameter) motor is concluded to be 20 feet with no through perforation and without any catastrophic collapse due to the impact. There would be permanent deformations throughout the deck and their determination is beyond the scope of this calculation. This analysis is limited to the reactivity deck only without any examination of the impact's effect on the shield tank support below the deck or at any other structure, system or component. The deck required to be analyzed for the impact of the accidental dropping of the 110,000 lb PHT motor. The purpose of this calculation is to determine the safe limit on drop height in terms of through perforation and structural integrity of the reactivity deck with no catastrophic collapse. No catastrophic collapse of the reactivity deck is expected by the impact caused by dropping of the 110,000 lb PHT pump motor with 66 inches contact diameter from 20 feet height. However there would be permanent deformations with no through perforation. The dropped motor's bottom portion would be damaged with permanent deformations. The damage to the reactivity deck may be extensive. The drop</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>height to cause elastic impact is 2m. No analysis is carried out for the elastic behavior which may cause the dropped object to bounce back and hit the deck repeatedly until it comes to rest. As a result of the calculations lifting of the pump motor should be restricted to 20 feet over the reactivity desk [BB Reactivity Deck PHT Pump Motor Drop Analysis, NK29-CALC-31360-00001, R00, October 23, 2013]. It is noted that the analysis is limited only to the reactivity deck. Its impact on the supporting or supported SSCs including the shield tank extension or piping below is not carried out. Interference of the drop by the other objects on top of the reactivity deck is not analyzed. However, the analysis is limited to the reactivity deck without any examination of the impacts on the shield tank support below the deck or at any other structure, system and component. The Bruce B design does not consider the drop of large loads in areas where systems and components important to safety are located. There is no documented corresponding analysis to justify safe operation when such loads are present. Therefore, it is assessed as a gap. (Gap 2).</p> <p>For the Bruce A design, the reactivity deck has one horizontal plate with vertical plates below spanning along its length with stiffeners in the transverse direction. There is concrete filling on top of this deck. It is noted that for Bruce B design the deck has top and bottom horizontal plates with web plates, stiffeners and concrete in between the two plates; whereas the absence of the bottom plate makes the Bruce A reactivity deck weaker than the one at Bruce B [NK21-CALC-31360-00003 R00, October 24, 2013].</p>	
7.16	SSCs important to safety shall be designed so that they can be manufactured, constructed,	New requirements related to construction, commissioning	IC


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>assembled, installed and erected in accordance with established processes that ensure the design will achieve the required level of safety.</p> <p>All plant systems shall be designed such that, to the greatest extent practicable, commissioning tests can be performed to confirm that design requirements have been achieved.</p> <p>The design shall include provisions to facilitate the commissioning activities. In particular, the design of the I&amp;C systems shall make provisions for start-up neutron sources and dedicated start-up instrumentation for conditions in which they are needed.</p> <p>The design shall specify commissioning requirements including data to be recorded and retained. In particular, the design shall clearly identify any non-standard or special commissioning requirements, which shall be specified in design documentation.</p> <p>Guidance</p> <p>Due account should be taken of relevant experience that has been gained in the</p>	<p>etc. are introduced in the first and the last two paragraphs.</p> <p>The original reactor systems were designed by AECL while Ontario Hydro Design and Construction Branch designed the balance of plant. From the earliest stages of the design, operating staff was assigned to the design organizations to make sure that appropriate input was provided to ensure that operating needs were dealt with. The design organization provided appropriate System Design Manuals to the operations staff prior to start up. From these manuals the operating staff developed Commissioning Plans and Procedures, Operating Manuals and Maintenance Manuals, and undertook the full commissioning of the station. The system design manuals provided operational limits for the various system components and the safety analysis provided safety limits for incorporation into the Operating Policies and Principles (OP&amp;P) and Impairment Manual (IM).</p> <p>The Bruce Power Engineering Change Control Program [BP-PROG-10.02, R010], Section 4.5 Commissioning Modifications and Projects process, as documented in BP-PROC-00615 R001, specifies how commissioning is to be carried out for Bruce Power Structures, Systems, Components and significant Tools. It includes requirements for commissioning planning, specification, execution, and reporting.</p> <p>The expectation is that commissioning will demonstrate that:</p> <p>" Installed systems, equipment and components will perform in accordance with specifications and design intent before they are placed into service.</p> <p>" Systems, equipment and components, which were altered to facilitate a change, are returned to their original</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>construction and commissioning of other similar plants and their associated SSCs. Where best practices from other relevant industries are adopted, such practices should be shown to be appropriate to the specific nuclear application.</p> <p>The design should include preliminary plant commissioning requirements for both pre-operational and initial start-up tests:</p> <ul style="list-style-type: none"> <li>• Pre-operational tests consist of those tests conducted following completion of construction and construction-related inspections and tests, but before fuel loading. Such tests demonstrate, to the extent practicable, the capability of SSCs to meet performance requirements and design criteria.</li> <li>• Initial start-up tests include those test activities scheduled to be performed during and following fuel-loading. Testing activities include fuel loading, pre-critical tests, initial criticality, low-power tests, and power ascension tests, which should confirm the design bases and demonstrate, to the extent practicable, that the plant will operate in accordance with its design and is capable of responding as designed to AOOs, DBAs and DECAs.</li> </ul> <p>The design authority should provide general</p>	<p>configuration.</p> <p>" Commissioning results are properly documented.</p> <p>" Systems, equipment and components are ready for turnover.</p> <p>The Engineering Change Control Program is implemented by the following procedures:</p> <p>" BP-PROC-00539, Design Change Package</p> <p>" BP-PROC-00542, Configuration Information Change</p> <p>" BP-PROC-00615, Commissioning Modifications and Projects</p> <p>" BP-PROC-00743, Site Services Engineering Change Control</p> <p>" BP-PROC-00877, Modification Installation Quality Assurance</p> <p>It is noted that these requirements are targeting new reactors.</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>guidance to control commissioning activities, including administrative controls that will be used to develop, review and approve individual test procedures, coordination with organizations involved in the test program, participation of plant operational and technical staff, and the review, evaluation and approval of test results.</p> <p>The design should include general guidance about how (and to what extent) the test program will use and test the plant's operating, surveillance and emergency procedures.</p> <p>The design should include test abstracts of SSCs and unique design features, which will be tested to verify that SSCs performance is in accordance with the design. These test abstracts should</p> <p>include the objectives, pre-requisites, test methods, and acceptance criteria that will be included in the test procedures.</p> <p>The design should include the acceptance criteria of commissioning activities that are necessary and sufficient to provide reasonable assurance that, if these commissioning activities are performed and the acceptance criteria met, the as-built facility will conform to the approved plant design and</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>applicable regulations.</p> <p>The scope of the acceptance criteria should be consistent with the SSCs that are in the design descriptions. In general, each system should have sufficient acceptance criteria that verify the information in the design descriptions. The level of detail specified in the acceptance criteria should be commensurate with the safety significance of the functions and bases for that SSC.</p> <p>The acceptance criteria should be objective and unambiguous, match the design commitments, and be able to be verified by adequate inspections, tests, and analyses during the construction and commissioning stages.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>IAEA, Safety Standards Series No. NS-G-2.9, Commissioning for Nuclear Power Plants, 2003.</li> <li>IAEA, SSR 2/2, Safety of Nuclear Power Plants: Commissioning and Operation, 2011.</li> </ul>		



 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>U.S. NRC, NUREG-0800, Chapter 14, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition, 2007.</li> </ul>		
7.17	<p>The design shall take due account of the effects of aging and wear on SSCs. For SSCs important to safety, this shall include:</p> <ol style="list-style-type: none"> <li>an assessment of design margins, taking into account all known aging and wear mechanisms and potential degradation in operational states, including the effects of testing and maintenance processes</li> <li>provisions for monitoring, testing, sampling, and inspecting SSCs so as to assess aging mechanisms, verify predictions, and identify unanticipated behaviours or degradation that may occur during operation, as a result of aging and wear</li> </ol> <p>Additional requirements are provided in RD-334, Aging Management for Nuclear Power Plants.</p> <p>Guidance</p>	<p>A new sentence referring to additional requirements defined in RD-334 is added to this clause. (Note: REGDOC-2.6.3 Fitness for Service: Aging Management, March 2014 superseded RD-334 Aging Management for Nuclear Power Plants, June 2011)</p> <p>As part of Bruce Power's submission for the 2015 renewal application for the Bruce A and Bruce B Operating Licences, Bruce Power reviewed additional new or revised CNSC regulatory documents and transition plans were provided in [Letter F, Saunders to M. Leblanc, Bruce Power: Requests and Supplemental Information for Licence Renewal, NK21-CORR-00531-11715 / NK29-CORR-00531-12105, November 28, 2014]. The development and implementation of effective aging management programs, procedures and processes has been an industry priority for several years and is being monitored by the CNSC under CANDU Safety Issue GL 3: Aging of Equipment and Structures. As part of this initiative, Bruce Power completed and submitted a gap analysis that compared the requirements of CNSC Regulatory Document RD-334, Aging Management for Nuclear Power Plants, against existing governance [NK21-CORR-00531-11715 / NK29-CORR-00531-12105]. After the publication of REGDOC-2.6.3, a gap assessment of Bruce Power governance against REGDOC 2.6.3 has been completed, which confirmed that existing governance largely aligns with the requirements of REGDOC-2.6.3. Some areas for requiring clarification have been identified, for example, in</p>	IC

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design should also consider the following:</p> <ul style="list-style-type: none"> <li>• identification of all SSCs subject to aging management</li> <li>• use of advanced materials with greater aging resistant properties</li> <li>• need for materials testing programs to monitor aging degradation</li> <li>• need to incorporate online monitoring, particularly where this technology would provide forewarning of degradation leading to failure of SSCs, and where the consequences of failure could be significant to safety</li> </ul>	<p>the requirements for periodic reviews of aggregate effects of aging, as well as governance considerations of aging management during all phases of the lifecycle of the plant. These identified areas for clarification are being addressed as part of the ongoing governance review and revision activities. Bruce Power plans to re-issue the affected documents in second quarter of 2016, thus completing the transition plan to REGDOC-2.6.3. The transition plan milestones for REGDOC-2.6.3 implementation are documented in Attachment A to [Letter F. Saunders to K. Lafreniere, Transition Plan for REGDOC-2.6.3 Implementation, NK21-CORR-00531-11763 / NK29-CORR-00531-12158, December 12, 2014].</p> <p>Bruce B design meets the requirement, as documented in the Equipment Reliability Program [BP-PROG-11.01, R005]. The program is to ensure that all systems important to safety meet their design intent and performance criteria. Current SSC life cycle and ageing management governance and processes meet the current regulatory requirements.</p> <p>Bruce Power is utilizing an Asset Management approach to ensure safe plant operations throughout its life cycle. A PSR process is being used to demonstrate and improve safety throughout the plant operating life. Bruce Power is utilizing an Asset Management approach to ensure safe plant operations throughout its life cycle. This Asset Management approach is being integrated with the PSR process, which is being used to demonstrate and improve safety throughout the plant operating life. Improvements identified in the PSR process are ranked, commensurate with the degree to which they support the cardinal objective of Bruce Power (i.e., safe and reliable production of electricity) and their safety</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>significance and time to become effective.</p> <p>An Assessment of Systems Important to Safety for the Safety &amp; Licensing Portion of the Nuclear Asset Management Program [B-REP-00701-21Oct2013-058] presents the various system groupings at Bruce Power that rank the importance of SSCs based on safety and production. These groupings can be used to establish the overall list of SSCs to be in scope of the Nuclear Safety &amp; Licensing portion of the Nuclear Asset Management Program. As indicated in section 3.2 of B-REP-00701-21Oct2013-058, tables of Bruce A and Bruce B systems and their relative placement in the hierarchy of importance in the definition of the scope of the performance and condition monitoring program are included in BP-PROC-00781, "Performance Monitoring" [R003, September 11, 2015].</p> <p>Bruce Power has established the Asset Life Projection and Options (ALPO) process described in BP-PROC-00899 Asset Life Projections and Options and BP-PROC-00936 Asset Management Planning.</p> <p>The scoping and identification of critical SSCs is part of the Equipment Reliability Program implementation. BP-PROC-00778 Scoping and Identification of Critical SSCs [R002, September 3, 2015] describes the process for the Responsible System Engineer (RSE), with support from Reactor Safety, Corporate &amp; Station Component Engineers and Design Engineering (including Environmental Qualification), to identify SSCs important to maintaining safe, reliable power operation. All aspects of nuclear safety (reactor safety, industrial safety, environmental safety and radiation safety) are addressed. This procedure includes a</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>functional criticality analysis and identifies:</p> <ul style="list-style-type: none"> <li>" Scoping criteria.</li> <li>" Functions related to safety and reliability.</li> <li>" Components included in Operational Safety Requirements (OSR) in support of Safe Operating Envelope (SOE)</li> <li>" Critical structures and components that support these functions.</li> <li>" Non-critical components.</li> <li>" Run to Maintenance components.</li> </ul> <p>Structures important to maintaining safe, reliable power operation will include those identified in the safety related system list [BP PROC 00169]. Systems important to maintaining safe, reliable power operation will include those identified as systems important to safety [DPT RS 00012, Systems Important to Safety (SIS) Decision Methodology]. Components important to maintaining safe, reliable power operation will include components on the Master Equipment List (MEL) identified as critical or significant to plant operation. This will include:</p> <ul style="list-style-type: none"> <li>" Components important to safety in systems important to safety.</li> <li>" Components that are Single Points of Vulnerability (SPVs).</li> </ul> <p>Scoping and Identification of Critical SSCs [BP-PROC-00778, R002, September 03, 2015] uses the Master Equipment List (MEL) as a basis. Components and structures not on the</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>MEL (such as piping, cables, and supports), shall also be reviewed to identify any that are important to maintaining safe, reliable power operation. Components and structures not on the MEL (such as piping, cables and supports will also be reviewed to identify any that are important to maintaining safe, reliable power operation. Data stewardship and governance of the MEL is described in BP-PROC-00584, R008, October 19, 2015] PASSPORT Equipment Data Management. The BP-PROC-00584 procedure establishes the standard basis and process requirements to add, modify, retire, remove or delete existing equipment data in PASSPORT. This procedure sets guidelines for maintaining accurate Master Equipment List (MEL) record information and summarizes the relationships between equipment data and processes.</p> <p>DPT-RS-00012, [R001, September 24, 2013] Systems Important to Safety (SIS) Decision Methodology, determines which plant systems meet the criteria of 'Systems Important to Safety' (SIS). This determination is based on screening criteria which assesses probabilistic risk assessment (PRA) based risk significance, and on non PRA-based system importance for preventing fuel damage and release of radioactivity. The SIS list is used as one of the inputs into the scoping and identification of critical systems as part of AP-913.</p> <p>Long Term Planning and Life Cycle Management are discussed in Section 4.1.6 of Equipment Reliability Program [BP-PROG-11.01, R005].</p>	
7.18	The design shall provide for the detection, exclusion and removal of all foreign material and	There is no change in the requirement; the text is modified to provide clarification only.	C

Article No.	Clause Requirement	Assessment	Compliance Category
	corrosion products that may have an impact on safety.	<p>Bruce Power has a Chemistry Management control program [BP-PROG-12.02, R006, June 8, 2015] whose objective is to establish the optimum conditions for system chemistry and to mitigate conditions that could lead to an adverse effect on plant systems. The chemistry program is designed to embrace the fundamentals of nuclear safety as defined in BP-MSM-1. The program embraces the fundamentals of strong nuclear safety principles and recognizes that reactor safety, industrial safety, radiation safety and environmental safety are essential to long-term success of the chemistry program.</p> <p>BP-PROC-00197 [R006, February 12, 2015] Chemistry Control Event Management describes the process for defining, documenting and reacting to conditions where chemistry specifications are out of control limits, or when sampling violations have occurred.</p> <p>Bruce Power has a Foreign Materials Exclusion Program to ensure that no material inadvertently enters, for example, the HTS during outage maintenance activities.</p>	
7.19	The design shall incorporate appropriate features to facilitate the transport and handling of new fuel, irradiated fuel, and radioactive waste in accordance with the requirements of the Packaging and Transport of Nuclear Substances Regulations. Related considerations shall include facility access, as well as lifting and packaging capabilities.	<p>The addition of Packaging and Transport of Nuclear Substances Regulation is for clarification.</p> <p>The regulation is a legal requirement and is part of the licensing basis, i.e., applicable regulations under the NSCA.</p> <p>The facilities for transporting and handling of fresh fuel, spent fuel and radioactive wastes have been designed into the Bruce B plant and are described in Section 10 of Part 2 of the Safety Report.</p>	C
7.20	The design shall provide a sufficient number of	The change is for clarification only; "operational states, DBAs	C

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>safe escape routes that will be available in operational states, DBAs and DEC's, including seismic events. These routes shall be identified with clear and durable signage, emergency lighting, ventilation and other building services essential to their safe use.</p> <p>Escape routes shall be subject to the relevant Canadian requirements for radiation zoning, fire protection, industrial safety, and plant security, which include assurance of the ability to escape from containment regardless of the pressure in containment.</p> <p>Suitable alarm systems and means of communication shall be available at all times to warn and instruct all persons in the plant and on the site.</p> <p>The design shall ensure that diverse methods of communication are available within the NPP and in the immediate vicinity, as well as to offsite agencies, in accordance with the emergency response plan.</p> <p>Additional information</p>	<p>and DEC's" replaces "all plant states".</p> <p>As per the National Building Code and National Fire Code requirements, exits are generally signed by the usual illuminated exit signs (either powered or tritium lit). Exit routes have either Class 2 lighting or local emergency battery lights. The usual building code requirements about the number of exits per square footage of floor area etc. apply. Some specific anomalies have been identified which accommodated by adding an additional exit. There has recently also been a program to strengthen exit signage from the sixth floor admin area.</p> <p>Bruce B stairwells have fire doors, emergency lighting, and exit signs but in some cases, exiting by the staircases leads to outside doors bypassing monitors and takes the individual from Zone 2 or 3 to the outside unzoned area around the powerhouse. Generally, there are signs on the door saying that the exit is only to be used in an emergency without monitoring. These are not into the public domain though and individuals would only exit to the public domain via the security gatehouse, which is a monitored pathway.</p> <p>All areas of the station are served by a public address system, and provision is made to dial into the systems from the direct dialing system. As presented in Section 11.5.2.4 of Part 2 of the Safety Report, provision is made for the operator to make emergency announcements and to initiate emergency warning tones for fire and other emergencies from the control room, using the public address system. When the emergency tones are sounded a beacon system is activated in noisy areas of the plant where the public address system might not be heard.</p>	




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>• CSA Group, N293, Fire protection for nuclear power plants, Toronto, Canada.</li> <li>• CNSC, G-225, Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills, Ottawa, Canada, 2001 or successor document.</li> <li>• IAEA GS-R-2, Preparedness and Response for a Nuclear or Radiological Emergency, Vienna, 2002.</li> <li>• NRC, National Building Code of Canada, Ottawa, Canada, 2010.</li> <li>• NRC, National Fire Code of Canada, Ottawa, Canada, 2010.</li> </ul>	<p>The communication systems are described in Part 2, Section 11.5.2 of the Safety Report.</p>	
7.21	<p>The design shall include a human factors engineering program plan. Relevant and proven systematic analysis techniques shall be used to address human factors issues within the design process.</p> <p>Human factors considerations:</p> <p>1. reduce the likelihood of human error as far as reasonably achievable</p>	<p>A new requirement is added for the design to identify the type of information that facilitates the operator's ability to readily assess the general state of plant in DEC's.</p> <p>Bruce Power has a Human Factors Engineering Program Plan [DPT-PDE-00013, R008, June 16, 2014 that outlines the procedure for applying Human Factors site wide.</p> <p>This procedure provides direction in implementing Human Factor processes into changes performed under the Design Change Package procedures [BP-PROC-00539, R016, June 23, 2015]. This procedure may also be applied to projects outside of the modifications procedures where it is deemed that a Human Factors review will provide added benefit. For</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2. provide means for identifying the occurrence of human error, and methods by which to recover from such an error</p> <p>3. mitigate the consequences of error</p> <p>The human factors engineering program shall also facilitate the interface between the operating personnel and the plant by promoting attention to plant layout and procedures, maintenance, inspection, training, and the application of ergonomic principles to the design of working areas and working environments.</p> <p>Appropriate and clear distinction between the functions assigned to operating personnel and those assigned to automatic systems shall be facilitated by systematic consideration of human factors and the human-system interface. This consideration shall continue in an iterative way throughout the entire design process.</p> <p>The human-system interfaces in the main control room, the secondary control room, the emergency support facilities, and in the plant, shall provide operators with necessary and appropriate information in a usable format that is compatible</p>	<p>changes outside of BP-PROC-00539 the determination as to whether HF review is required will be made by the department manager or above of the line requesting the work in conjunction with the Manager, Plant Design Engineering. The Section Manager responsible for Human Factors, will provide input to the decision as required.</p> <p>The procedure outlines, using a graded approach, a systematic process for the application of Human Factors with the intent of:</p> <ol style="list-style-type: none"> <li>1. reduce the likelihood of human error as far as reasonably achievable</li> <li>2. provide means for identifying the occurrence of human error, and methods by which to recover from such an error</li> <li>3. mitigate the consequences of error</li> </ol> <p>This procedure is based upon NUREG-0711, Human Factors Engineering Program Review Model, and conforms to CNSC documents G-276, Regulatory Guide for Human Factors Engineering Program Plans and G-278, Regulatory Guide for Verification and Validation Plans. Appendix B of the procedure outlines the key elements of the NUREG-0711 model. The technical review elements identified in NUREG-0711 and G-276 promote the consideration of procedures, maintenance, inspection, training and the application of ergonomic principles to the design of work areas.</p> <p>Consequently, the processes and Bruce Power guidelines</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>with the necessary decision and action times.</p> <p>Human factors verification and validation plans shall be established for all appropriate stages of the design process so as to confirm that the design adequately accommodates all necessary operator actions.</p> <p>To assist in the establishment of design criteria for information display and controls, each operator shall be considered to have dual roles: that of a systems manager (including responsibility for accident management) and that of an equipment operator. Verification and validation activities shall be comprehensive, such that the design conforms to human factors design principles and meets usability requirements.</p> <p>The design shall identify the type of information that facilitates an operator's ability to readily:</p> <ol style="list-style-type: none"> <li>1. assess the general state of the plant, whether in operational states, DBAs or DEC's</li> <li>2. confirm that the designed automatic safety actions are being carried out</li> </ol>	<p>outlined DPT-PDE-00013 include considerations for such technical elements. Appendix B of DPT-PDE-00013 describes the technical review elements for procedures, training, and Human-System Interface (HSI) design. These technical review elements are also identified for consideration in DPT-PDE-00001, [R004, September 3, 2014] Human Factors Minor Change.</p> <p>Appropriate and clear distinction between functions assigned to operating personnel and those assigned to automatic system is reviewed for modifications through the function allocation component of a functional analysis described DPT-PDE-00013, Appendix B (Human Factor Plan Elements and Application) and Appendix E (Function Analysis and Function Allocation for Major Products). Function allocation is further considered during task analyses, HSI design, Human Reliability Analysis (where applicable), and finally as a part of validation.</p> <p>The main control room displays are based on the concept that the operators must have sufficient information available to allow them to control the units safely from the main control room [Bruce B Safety Report, Part 2, Section 7.1.5]. Moreover, the MCR has been in operation for approximately 30 years and has undergone modifications throughout the operating life of the plant. Based on this, it can be concluded that appropriate information is provided in the MCR. Any on-going system changes that necessitate changes in the MCR are addressed through the Human Factors program described in DPT-PDE-00013. The Bruce B has four unit Secondary Control Areas and one common Secondary Control area located in the Emergency Water and Power Supply (EWPS) Building. The SCAs are a part of the original</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>3. determine the appropriate operator-initiated safety actions to be taken</p> <p>The design shall provide the type of information that enables an equipment operator to identify the parameters associated with individual plant systems and equipment, and to confirm that the necessary safety actions can be initiated safely.</p> <p>Design goals shall include promoting the success of operator action with due regard for the time available for response, the physical environment to be expected, and the associated psychological demands made on the operator.</p> <p>The need for operator intervention on a short time scale shall be kept to a minimum. Where such intervention is necessary, the following conditions shall apply:</p> <p>1. the information necessary for the operator to make the decision to act is presented simply and unambiguously</p> <p>2. the operator has sufficient time to make a</p>	<p>design of the station. The SCA requirements are documented in the Bruce B Generating Station Safety Related System and the Two Group Separation Philosophy Design Manual [R00, February 26, 1979]. According to the requirements the SCA must have sufficient monitoring and control devices necessary to carry out three safety functions independently from the MCR in the event of a common mode failure, which may render the MCR uninhabitable:</p> <p>" Shut down the reactor and maintain it shut down.</p> <p>" Remove the decay heat and thus prevent any subsequent process failure which might lead to the release of radioactivity to the public in excess of allowable limits.</p> <p>" Supply necessary information for post-accident monitoring to permit the operator to assess the state of the nuclear steam supply system.</p> <p>The design requirements and the fact that the SCA instrumentation and controls are tested regularly to ensure their functionally and availability suggests that the SCA provides operators with necessary and appropriate information.</p> <p>Bruce Power has five emergency response facilities as discussed in the assessment to Clause 8.10.3. Four of the current response facilities are on site. The facilities are:</p> <p>" Two Emergency Operations Centre (EOC) - one for each station. The EOC is where the centralized coordination of all on-site and off-site response will take place initially. The non-incident facility EOC is a back-up location for the incident facility's EOC.</p> <p>" Site Management Centre (SMC) - is the on-site</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>decision and to act</p> <p>3. following an event, the physical environment is acceptable in the main control room or in the secondary control room, and in the access route to the secondary control room</p> <p>Guidance</p> <p>This section applies to the design of all plant systems where there are human factors (HF) considerations. Human factors means “factors that influence human performance”, as defined in CNSC P-119 Policy on Human Factors. In practice, it is expected that most plant systems will require some consideration of HF.</p> <p>The systematic approaches and processes taken for HF in design should meet international standards and good practices. HF codes and standards that are used by the design authority for the plant design should be identified and evaluated for their suitability, applicability, sufficiency and adequacy.</p> <p>There should be sufficient authority in the management of HF in design to ensure that HF</p>	<p>facility where station management augmentation and technical staff assemble.</p> <p>" Corporate Emergency Support Centre (CESC) - coordinates and manages the overall corporate office response to a nuclear emergency. CESC is the primary contact for communications with the provincial, regional, and local municipal government centres.</p> <p>The SMC and CESC are back-up facilities to each other.</p> <p>Bruce Power has an Emergency Management Centre (EMC) off-site and has unified the existing Site Management and Corporate Emergency Support Centres into a single, modern command centre. The activities in the EMC were integral to the Huron Challenge IV conducted on October 2012 and described in Bruce Power's After Action Report (AAR) Exercise Huron Challenge 2012, B-REP-03491-19OCT2012.</p> <p>Where appropriate, Human Factors verification and validation plans for design changes are developed based on a graded approach and in accordance with the guidelines identified in DPT-PDE-00013 Appendix B (Human Factor Plan Elements and Application) and Appendix G (Validation for Major Projects). Verification activities are defined with reference to the applicable human factors design principles and guidelines in order to meet usability requirements.</p> <p>Operator intervention and the time needed to carry out tasks are associated with design changes are analyzed through task analyses for major projects as described in Human Factors Engineering Program Plan [DPT-PDE-00013, R008, June 16, 2014 Appendix F (Task Analysis for Major Projects) or for minor changes, Human Factors Minor Change [DPT-PDE-00001, R004, September 03, 2014] Section 4.7 - Step</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>considerations that influence safety are adequately taken into account. HF design requirements that will supplement the codes (e.g., concerning usability and human performance) should also be identified and specified early in the design stage process.</p> <p>The following areas should have interfaces with HF in design:</p> <ul style="list-style-type: none"> <li>• engineering design of specific SSCs</li> <li>• procedure development</li> <li>• training development</li> <li>• consideration of human actions in safety analyses</li> <li>• specifications of staffing and minimum shift complement</li> </ul> <p>The design expectations are provided below for use in different design stages.</p> <p>Planning</p> <p>A human factors engineering program plan demonstrates how HF considerations are</p>	<p>3, Tasks.</p> <p>Bruce Power undertook an Abnormal Incidents Manual (AIM) validation exercise with the goal of ensuring that all AIMs could be completed safely and within the required time, using the minimum staff complement. The analysis also verified the availability of the required controls, equipment and information. As a secondary goal, optimization of the AIMs and their associated field tasks was also considered during the analysis. This included consideration of available equipment and locations, methods of dispatch and other aspects of AIM implementation. The exercise is summarized in B-REP-06700-00002, Bruce Power Abnormal Incident Manual (AIM) Project Human Factors Engineering Summary Report (HFESR).</p> <p>In response to the events that occurred at the Fukushima Daiichi nuclear power station in March of 2011, Bruce Power reviewed its operational equipment and response capabilities. The review included confirmation of safety equipment functionality, up-to-date related procedures and training. In addition, a detailed analysis was undertaken that identified further enhancement activity to effectively respond to a Beyond Design Basis Accident Scenario.</p> <p>Based on these identified enhancement opportunities, Bruce Power participated in a provincially led exercise called Huron Challenge IV in October 2012. This exercise was a full scale exercise that tested the equipment and emergency response enhancements identified in the review of operations and detailed analysis of responding to Beyond Design Basis Accidents that was previously conducted by Bruce Power.</p> <p>The results and the improvement opportunities identified from</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>incorporated into the design activities. Further guidance on how to develop such a plan is provided in the CNSC G-276 Human Factors Engineering Program Plans and U.S. NRC NUREG-0711, Revision 2, Human Factors Engineering Program Review Model. The technical elements described in the plan should be supported by subsequent verification and validation activities for the resulting design, as described in CNSC G-278 Human Factors Verification and Validation Plans.</p> <p>The HF in design activities are effectively integrated in the overall engineering design process and incorporated early enough to make an effective contribution to safety. There should be a sufficient number of trained, qualified and experienced HF specialists to carry out the HF in design activities provided that established criteria pertaining to system complexity and importance to safety are met.</p> <p>Analysis</p> <p>Systematic analytical approaches are used to establish the HF inputs. Such analyses should be conducted from the earliest stages of design, to provide a strong foundation upon which the design solutions are based. The specific HF</p>	<p>the exercise are summarized in Bruce Power's After Action Report (AAR) Exercise Huron Challenge 2012, B-REP-03491-19OCT2012.</p> <p>DPT-PDE-00013 is based upon NUREG-0711, Human Factors Engineering Program Review Model, and conforms to CNSC documents G-276, Regulatory Guide for Human Factors Engineering Program Plans and G-278, Regulatory Guide for Verification and Validation Plans. Appendix B of the procedure outlines the key elements of the NUREG-0711 model. NUREG-0711 model is recognized internationally as a well-developed, comprehensive model for the review of HF. Inherently, the model proves very useful for design as well.</p> <p>The model that is outlined in NUREG-0711 and similarly in DPT-PDE-00013 is intended to ensure that the HF aspects of a design change to the plant are developed, designed, and evaluated via a structured analysis founded on HF principles. The methodology uses a top-down approach such that high level goals and functions of the modification are analyzed and the tasks associated with the functions are subsequently analyzed. The detailed design of the HSI, procedures, and training is the "bottom" of the top-down process. The technical elements and the application of the elements are depicted in Figure 1 and described in in Appendix B of DPT-PDE-00013:</p> <ul style="list-style-type: none"> <li>" HFE Program Management</li> <li>" Operating Experience Review</li> <li>" Functional Analysis and Function Allocation</li> <li>" Task Analysis</li> </ul>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>analyses should be:</p> <ul style="list-style-type: none"> <li>appropriate to the activities in question that they cover, considering the risk of the activities and the novelty of the design</li> <li>carried out throughout the development of the design</li> <li>use methods, techniques, and good practices that are considered acceptable by trained and experienced human factors specialists</li> <li>share the information produced between groups engaged in different parts of the design</li> </ul> <p>The HF analyses could include:</p> <ul style="list-style-type: none"> <li>function analysis</li> <li>task analysis</li> <li>human reliability analysis</li> <li>hazard analysis</li> <li>link analysis</li> <li>information requirements analysis</li> <li>staffing analysis</li> <li>usability analysis</li> </ul>	<p>" Staffing and Qualification</p> <p>" Treatment of Important Human Actions</p> <p>" Human System Interface Design</p> <p>" Procedure and Training Program Development</p> <p>" Design Verification</p> <p>" Design Validation</p> <p>" Design Implementation</p> <p>" Human Performance Monitoring</p> <p>Human Factors at Bruce Power resides within Plant Design Engineering and is integrated into Bruce Power's Design Change Package process described in BP-PROC-00539 and is invoked by BP-PROG-10.02, Engineering Change Control. Because Human Factors is integrated into the engineering change control process, Human Factors activities, depending on the scope of work, aligns with the process map identified in BP-PROC-00539, Appendix A and is invoked through the identification of stakeholder involvement (HF being a potential stakeholder) early on for the design change package. In addition, the nature of the NUREG-0711 model is structured to provide timely input to various design activities within the engineering design process intended by BP-PROC-00539.</p> <p>DPT-PDE-00013 describes interfaces with procedure development, training, and safety analysis (when credible human actions are concerned). The AIM Validation conducted and described in B-REP-06700-00002, Bruce Power Abnormal Incident Manual (AIM) Project Human Factors Engineering Summary Report (HFESR) was carried</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>operability and maintainability analysis</li> </ul> <p>The design should also provide research or study reports for any work carried out as part of the process of developing and testing any human-system interface technologies (e.g., displays and controls) that are new to NPP applications and that may have a bearing on safety.</p> <p>The design should demonstrate that steps have been taken in developing the design to reduce or eliminate, where practicable, the potential for human error; that there are acceptable means by which to identify error; that methods are provided by which to recover from the error; and that the consequences of error can be mitigated.</p> <p>Design</p> <p>There should be evidence that a systematic process exists for the design of work areas, work environments, and human-system interfaces for SSCs throughout the plant. The design should demonstrate consideration of HF issues for all aspects of the plant, not just control areas. HF aspects should be considered where off-the-shelf SSCs are specified and procured. Operating experience concerning HF issues gained from</p>	<p>out with the intent of providing input to the minimum staff complement.</p> <p>Bruce Power's site-wide HFEPP outlines the planning of activities in Section 4.1 and 4.2 of DPT-PDE-00013. The planning, along with the execution of Human Factors activities are based on a graded approach, which has already been described within this assessment.</p> <p>DPT-PDE-00013 also outlines the qualifications for the various individuals involved in providing Human Factors support and carrying out Human Factors related work.</p> <p>DPT-PDE-00013 provides guidance with respect to the application of various HF analyses and also provides for flexibility of analyses based on the scope of the work and the applicability of various analyses.</p> <p>Operations and maintenance departments are considered important stakeholders in the engineering change control process and as such they are always engaged in the design process as early as possible. This is evident in the implementation of Bruce Power's Engineering Change Control program.</p> <p>Any formal interfaces that are necessary are defined within a project specific Human Factors Engineering Program Plan in accordance with CNSC G-276.</p> <p>Elements of effective human factors verification and validation planning are described in CNSC G-278. This guidance is listed under the compliance verification criteria for Licence Conditions 2.2, and 5.1.</p>	



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>existing or similar systems should be considered in the design.</p> <p>A significant aspect of this systematic process is the use of modern human factors codes, standards, and good practices in developing the design. Guidance is provided in U.S. NRC NUREG-0700 Revision 2, Human-System Interface Design Review Guidelines.</p> <p>The design should demonstrate that operators (and any other potential users) in the main control room, the secondary control room, the emergency support facilities, and in the plant, are provided with the necessary and appropriate information in a format that is compatible with necessary decision and action times. The same kind of considerations should apply to other users of equipment (e.g., maintainers and technicians) elsewhere in the plant.</p> <p>Operating personnel</p> <p>Personnel who have operating experience from similar plants should be actively involved in the design process to ensure that consideration is given as early as possible to the future operation and maintenance of the SSCs.</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Formal interfaces should be defined between the HF in design group(s) and the various design engineering groups involved in the design process; this facilitates the interactions and sharing of information to achieve good integration of HF considerations in the design.</p> <p>Verification and validation</p> <p>Evaluations are an essential part of HF in the design process and include both verification and validation activities. Evaluation criteria (i.e., design requirements and standards) should be established prior to conducting these evaluations.</p> <p>HF verification activities should be carried out (generally by vendor and licensee) to confirm that the design conforms to HF design standards and has been implemented as intended in the plant.</p> <p>Validations should be carried out iteratively at various stages of the design process, ensuring that the task fidelity is appropriate. Data from the validation activities should be analysed and the results should be used to improve the design. Validation should confirm that the system, including the human components and procedures</p>		



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>to support the tasks, meets the specified system and usability requirements. Validations should also demonstrate that operations and maintenance personnel can successfully carry out their tasks in a safe manner.</p> <p>Guidance on evaluations is provided in CNSC G-278, Human Factors Verification and Validation Plans, and U.S. NRC NUREG-6393, Integrated System Validation: Methodology and Review Criteria.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>• ANSI/ANS, 58.8-1994, Time Response Design Criteria for Safety-Related Operator Actions, La Grange Park, Illinois, reaffirmed 2008.</li> <li>• CNSC, G-323, Ensuring the Presence of Sufficient Qualified Staff at Class I Nuclear Facilities – Minimum Staff Complement, Ottawa, Canada, 2007.</li> <li>• CNSC, G-276, Human Factors Engineering Program Plans, Ottawa, Canada, 2003.</li> <li>• CNSC, G-278, Human Factors</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Verification and Validation Plans, Ottawa, Canada, 2003.</p> <ul style="list-style-type: none"> <li>• CNSC, P-119, Policy on Human Factors, Ottawa, Canada, 2000.</li> <li>• CSA Group, N290.6, Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of an Accident, Toronto, Canada.</li> <li>• CSA Group, N290.4, Requirements for Reactor Control Systems of Nuclear Power Plants, Toronto, Canada.</li> <li>• IEC, 61839, Nuclear Power Plants – Design of Control Rooms – Functional Analysis and Assessment, Geneva, 2000.</li> <li>• IEC, 60964, Nuclear Power Plants – Control Rooms – Design, Geneva, 2009.</li> <li>• IEEE, 1289, IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations, Piscataway, New Jersey 1998.</li> <li>• IEEE, 1023, IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations, Piscataway, New Jersey, 2004.</li> <li>• U.S. NRC, NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on</li> </ul>		



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Nuclear Power Plant Applications- Final Report, Piscataway, New Jersey , 2011.</p> <ul style="list-style-type: none"> <li>• U.S. NRC, NUREG-0711, Human Factors Engineering Program Review Model, Washington, D.C., 2002.</li> <li>• U.S. NRC, NUREG-0700, Human System Interface Design Review Guidelines, Washington, D.C., 2002.</li> <li>• U.S. NRC, NUREG-6393, Integrated System Validation: Methodology and Review Criteria, Washington, D.C., 1997.</li> <li>• U.S. NRC, NUREG-6684, Advanced Alarm Systems: Revision of Guidance and Its Technical Basis, Washington, D.C., 2000.</li> <li>• U.S. NRC, NUREG/CR-6633, Advanced Information Systems Design: Technical Basis and Human Factors Review Guidelines, Washington, D.C., 2000.</li> </ul>		
7.22	<p>The design shall provide physical features such as protection against design-basis threats (DBTs), in accordance with the requirements of the Nuclear Security Regulations.</p> <p>Guidance on robustness against malevolent acts</p> <p>The engineering safety aspects of robustness and protection from malevolent acts should account</p>	Due to sensitivity of information the assessment is documented elsewhere.	RNA



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>for:</p> <ul style="list-style-type: none"> <li>• basic design approach</li> <li>• structural performance objectives</li> <li>• threat characterisation</li> <li>• loading development</li> <li>• material properties</li> <li>• principles of analysis and design</li> <li>• structural acceptance criteria</li> <li>• design of SSCs</li> </ul> <p>The basis for identifying malevolent acts considered in the design is the potential to cause a release of radioactivity to the public and the environment.</p>		
7.22.1	<p>The design shall be such that the NPP and any other onsite facilities with potential to release large amounts of radioactive material or energy are protected against malevolent acts.</p> <p>Threats from credible malevolent acts are referred to as design-basis threats (DBTs). More severe but unlikely threats are referred to as beyond-design-basis threats (BDBTs). Both types of</p>	<p>Due to sensitivity of information the assessment is documented elsewhere.</p>	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>threats shall be considered in the design.</p> <p>Threats identified as DBTs shall have credible attributes and characteristics of potential insider or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage against which a physical protection system is designed and evaluated.</p> <p>BDBTs are threats too unlikely to warrant incorporation into the design basis, but for which the consequences shall be assessed in order to establish means of mitigation to the extent practicable.</p> <p>Consistent with the concept of defence in depth, the design shall provide multiple barriers for protection against malevolent acts, including physical protection systems, engineered safety provisions, and measures for post-event management, as appropriate. The failure of a preceding barrier shall not compromise the integrity and effectiveness of subsequent barriers.</p> <p>Guidance</p> <p>The identification of vital areas involves the</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>identification and location of SSCs that require protection, in order to prevent significant radioactive releases. The vital areas include the reactor building and the spent fuel pool, including the structure housing the spent fuel pool. The protection measures for these identified vital areas should be assessed.</p> <p>Based on identified threats, the DBT and BDBT sets of load cases should be selected. Each load case selected should be the worst case scenario for a given threat.</p>		
7.22.2	<p>The design authority shall develop a methodology for assessing the challenges imposed by DBTs and evaluating the capabilities for meeting these challenges (e.g., as identified in an initial threat and risk assessment). The methodology shall apply conservative design measures and sound engineering practices.</p> <p>The plant design shall take into account the role of structures, pathways, equipment, and instrumentation in providing detection, delay, and response to threats.</p> <p>Vital areas shall be identified and taken into account in the design and verification of robustness. For vital areas, the design shall allow</p>	Due to sensitivity of information the assessment is documented elsewhere.	RNA



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>enough delay for effective intervention by the onsite or offsite response force, taking structures, detection and assessment into account. These areas shall, to the extent practicable, be protected from inadvertent damage while performing defensive actions.</p> <p>The design shall provide appropriate means for access control and detection, and for minimizing the number of access and egress points to protected areas. Such points shall include storm sewers, culverts, service piping, and cable routing that could be used to gain access to the facility.</p> <p>The design shall also take into account the placement of civil utilities to minimize access requirements for such activities as repair and maintenance, in order to reduce threats to the protected area and vital areas.</p> <p>The design authority shall also develop a methodology for assessing the challenges associated with BDBTs. This methodology shall be applied to determine the margins available for shutdown, fuel cooling and confinement of radioactivity. Significant degradation of engineering means may be permitted.</p>		



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Guidance</p> <p>Vital areas are designed according to the tiered approach related to the level of the threat as described below.</p> <p>For the loadings induced by DBT, the structural design methodology applies conservative design measures and sound engineering practices that meet codes and standards.</p> <p>For the first-tier BDBT (events more severe than DBT), sufficient structural integrity to protect important systems should be provided. The design code criteria may be relaxed; however, the design methodology should be followed.</p> <p>For the second-tier BDBT (extreme events), degradation of the containment barrier may be accepted; however, the degradation should be limited. The structures of vital areas should be designed for the second-tier BDBT that may exceed design code limits but within documented material and structural limits.</p> <p>The aircraft crash loading functions related to DBTs and BDBTs are “classified”, and are</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>available to licensees and applicants upon request to the CNSC.</p> <p>It is acceptable to model the whole aircraft as a load that impacts the structure. However, the design should be such that the loading functions due to the crash of the modelled aircraft against a rigid target envelope are acceptable.</p> <p>Two distinct types of structural failure modes should be reviewed: local (punching - brittle) failure and global (flexural-plastic) failure. The loading characteristics and structural behaviour for these two failure modes are different, and should be reviewed separately. However, it should be noted that, in some cases, these two failure modes (e.g., an aircraft crash) may act simultaneously or quasi-simultaneously.</p> <p>Local structural behaviours under a malevolent-act-induced loading case should be assessed. Local damage to the target can be defined using the following descriptions:</p> <ul style="list-style-type: none"> <li>• penetration – the depth of the crater due to the missile impact</li> <li>• spalling – the ejection of the target material from the front face of the target (impacted</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>face)</p> <ul style="list-style-type: none"> <li>• scabbing – the ejection of material from the rear face of the target</li> <li>• just perforation – the missile just penetrates the target with residual velocity equal to zero</li> </ul> <p>Most technical references consider engines, in the case of an aircraft crash, as the critical missiles. Such local damage modes would not, in general, result in structural collapse; but they may cause damage to safety-related systems or components. Application of empirical formulae for perforation and scabbing is an acceptable approach to assess structural behaviour under local, concentrated loading.</p> <p>Global structural response effects refer to the overall building behaviour in response to the applied impact loading. The global response can be characterized by major structural damage, such as significant perforation or collapse of large portions of the building walls, floors, and load carrying frames. The impact could also potentially induce significant vibrations or “shock loading” throughout the building.</p> <p>In the case of an aircraft crash, in the absence of adequate design measures, local damage associated with the impact of a missile into the</p>		



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>wall could result in scabbing of concrete from the rear face. Ultimately, it could result in local fracture of rebar, allowing perforation of the wall by the residual crushed engine mass and remaining portion of the shaft. Global structural damage, however, is generally associated with the deformation of the entire structural system. Adequate design measures should be provided to meet the acceptance criteria provided in section 7.22.3.</p> <p>The design of the facility's physical protection system should consider changes in threat, enhanced understanding of the potential vulnerabilities of the facility, its systems and structures as well as advances in physical protection approaches, systems, and technologies.</p>		
7.22.3	<p>All safety system functions and capabilities shall continue to be available for DBTs.</p> <p>The design shall provide for the ongoing availability of fundamental safety functions during BDBTs; these provisions will depend on the severity of the threat.</p> <p>For more severe events, there shall be a safe shutdown path that comprises at least one means</p>	Due to sensitivity of information the assessment is documented elsewhere.	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>for each of the following:</p> <ol style="list-style-type: none"> <li>1. reactor shutdown</li> <li>2. fuel cooling</li> <li>3. retention of radioactivity from the reactor</li> </ol> <p>There shall be sufficient structural integrity to protect important systems. Two such success paths shall be identified where practical.</p> <p>For extreme events, there shall be at least one means of reactor shutdown and core cooling. Degradation of the containment barrier may allow the release of radioactive material; however, the degradation shall be limited. In these cases, the response shall include onsite and offsite emergency measures.</p> <p>Guidance</p> <p>The acceptance criteria for both local and global behaviour should be satisfied simultaneously. The structural acceptance criteria for local behaviour</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>should include the following:</p> <ul style="list-style-type: none"> <li>For DBTs, there should be no scabbing of the rear face of structural elements, possibly with limited, easily repairable, superficial spalling of concrete.</li> <li>For severe BDBTs, there should be no scabbing of the rear face of structural element, or possible limited scabbing (concrete cover), if confined by the steel liner. The steel liner should remain leak-tight.</li> <li>For extreme BDBTs, there should be no perforation, according to the applicable formula with a corresponding increase factor of 1.2 applied to the calculated thickness.</li> </ul> <p>Further detailed guidance on structural analysis of containment structures is given in Appendix A. Further information on the design and construction for containment and other safety-related</p> <p>structures can be found in the CSA N287 series of standards, and in CSA N291, Requirements for Safety-Related Structures for CANDU Nuclear Power Plants, respectively.</p> <p>Additional information</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>• ACI, Standard 349, Code Requirements for Nuclear Safety-Related Concrete Structures and Commentary, Farmington Hills, Michigan, 2007.</li> <li>• ASCE, Ed. 2, Design of Blast-Resistant Buildings in Petrochemical Facilities, Reston, Virginia, 2010.</li> <li>• ASCE, 58, Manual and Reports on Engineering Practice, Structural Analysis and Design of Nuclear Plant Facilities, Reston, Virginia, 1980.</li> <li>• Communications Security Establishment, TRA-1, Harmonized Threat and Risk Assessment (TRA) Methodology, Ottawa, Canada, 2007.</li> <li>• CNSC, RD-321, Criteria for Physical Protection Systems and Devices at High-Security Sites, Ottawa, Canada, 2010.</li> <li>• CNSC, RD-363, Nuclear Security Officer Medical, Physical, and Psychological Fitness, Ottawa, Canada, 2008.</li> <li>• CNSC, G-274, Security Programs for Category I or II Nuclear Material or Certain Nuclear Facilities, Ottawa, Canada, 2003.</li> <li>• CNSC, RD-346, Site Evaluation for New Nuclear Power Plants, Ottawa, Canada, 2008.</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>• CNSC, G-208, Transportation Security Plans for Category I, II or III Nuclear Material, Ottawa, Canada, 2003.</li> <li>• CSA Group, N291, Requirements for Safety-Related Structures for CANDU Nuclear Power Plants, Ottawa, Canada.</li> <li>• IAEA, TECDOC-967, Rev.1, Guidance and considerations for the implementation of INFCIRC/225/Rev.5, The Physical Protection of Nuclear Material and Nuclear Facilities, Vienna, 2002.</li> <li>• IAEA, TECDOC-1276, Handbook on the Physical Protection of Nuclear Materials and Facilities, 2002.</li> <li>• IAEA, INFCIRC-225, Rev.5, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, Vienna, 2011.</li> <li>• NEI, 07-13, Methodology for Performing Aircraft Impact Assessments for New Plant Designs, Washington, D.C., 2011.</li> <li>• Unified Facilities Criteria, 3-340-02, Structures to Resist the Effects of Accidental Explosions, Washington, D.C., 2008.</li> <li>• United Kingdom Atomic Energy Authority, Guidelines for the Design and Assessment of Concrete Structures Subjected to Impact, Oxfordshire, United Kingdom, 1990.</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
7.22.4	<p>The design of computer-based I&amp;C systems important to safety shall provide a cyber security defensive architecture.</p> <p>Computer-based I&amp;C systems and components important to safety shall be protected from cyber attacks in order to maintain confidentiality, integrity and availability.</p> <p>A cyber security program shall be developed, implemented and maintained so as to achieve the security required in each phase of the computer-based I&amp;C systems' lifecycle.</p> <p>Cyber security features shall not adversely affect the functions or performance of SSCs important to safety.</p> <p>Guidance</p> <p>The security of computer-based I&amp;C systems is designed to provide a secure operational environment with defensive features, and to protect against cyber attacks. Applicable codes and standards should be used, and industry best practices should be consulted.</p>	<p>This is a new clause/section.</p> <p>Due to the sensitivity of information the assessment is documented elsewhere.</p>	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design of a cyber security program should consider:</p> <ul style="list-style-type: none"> <li>• documentation for how the design authority establishes, implements and maintains the program to provide high assurance that the systems subject to security protective measures are protected</li> <li>• application of defence in depth protective strategies to provide a high level of assurance that the program has adequate cyber security capability</li> <li>• addressing potential security vulnerabilities in each phase of the computer-based I&amp;C systems lifecycle for computer-based systems important to safety</li> <li>• inclusion of security controls for a secure development environment during the development phases</li> </ul> <p>A site specific program should include the following elements:</p> <ul style="list-style-type: none"> <li>• defensive strategy</li> </ul>		





Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"><li>• asset identification, and security controls</li><li>• roles and responsibilities</li><li>• policies and procedures</li><li>• awareness and training</li><li>• configuration management</li><li>• information protection</li><li>• coordination with other security programs</li><li>• incident reporting and recovery plan</li><li>• program maintenance</li></ul> <p>The defensive architecture should have cyber security defensive levels separated by security boundaries. The systems requiring the greatest degree of security should be located within the most secure boundaries.</p> <p>The design authority should identify the design features that provide a secure operational environment of the systems important to safety.</p> <p>Security design requirements for computer-based I&amp;C systems should be informed by vulnerability analyses. Vulnerabilities addressed in the design should include:</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>deficiencies in the design that may allow inadvertent, unintended, or unauthorized access or modifications to the systems (hardware and software), which may degrade the reliability, integrity or functionality of the systems during operations</li> <li>non-performance of the safety functions by the systems in the presence of undesired behaviour of connected systems</li> </ul> <p>The following should be considered for the protection of computer-based I&amp;C systems and components important to safety functions:</p> <ul style="list-style-type: none"> <li>the computer-based I&amp;C systems and components important to safety should be protected, along with those support systems and components which, if compromised, would adversely affect safety functions</li> <li>cyber attacks should include either physical or logical threats (with either malicious or non- malicious intent), originating from inside and outside of the perimeter of the system's facility</li> <li>computer-based systems and components should include computer hardware, software,</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>firmware, and interfaces</p> <ul style="list-style-type: none"> <li>both autonomous and non-autonomous computer-based systems or components subject to cyber security, should be protected</li> <li>computer-based systems and components for the functions of emergency preparedness system, physical security and safeguards, should be protected, if applicable for the design</li> </ul> <p>The computer-based I&amp;C systems important to safety should be protected from physical attacks and unauthorized physical or logical access, and should meet the following expectations:</p> <ul style="list-style-type: none"> <li>all systems, components and network cabling important to safety should be installed in a plant location that physically secures the equipment</li> <li>effective methods should be used, such as including appropriate combinations of programmatic controls and physical security measures (e.g., locked enclosures, locked rooms, alarms on enclosure doors)</li> <li>unnecessary or unauthorized access to the setpoint adjustments and calibration adjustments</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>should be limited</p> <ul style="list-style-type: none"> <li>connections needed for temporary use should be disabled when not in use (e.g., connection of maintenance and development computers)</li> <li>unused data connections should be disabled</li> <li>all data connections for systems and components should be placed within enclosures</li> <li>any remote access to the safety system from a computer located in an area with less physical security than the safety system should be limited</li> <li>access to the safety systems should be logged, and the security logs should be checked periodically</li> <li>wireless communication should not be implemented for safety systems</li> <li>safety systems should be designed such that virus protection software is not required</li> <li>dedicated communication of plant data between the plant and the emergency support facilities</li> </ul> <p>(either onsite or offsite) should be provided using secure protocols</p> <p>Security functions and security supporting</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>functions of I&amp;C systems should not adversely affect the functions of systems and components important to safety. The design should ensure that neither the operation nor failure of security measures implemented will adversely affect the ability of the systems important to safety.</p> <p>Implementation of any individual security control or function, or of the complete set of applied controls for safety systems, should consider the following:</p> <ul style="list-style-type: none"> <li>• implementation should not adversely impact performance, including response time, effectiveness or operation of safety functions</li> <li>• where practical, implementation directly in the safety system should be avoided</li> <li>• if implemented in safety system displays and controls, the security control should not adversely impact the operator's ability to maintain the safety of the plant</li> <li>• if implemented within a safety system, adequate measures should be taken to ensure that the security controls do not adversely affect the ability of the system to perform its safety functions</li> <li>• security controls within a safety system should be developed and qualified to the same</li> </ul>		



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>level of qualification as the system in which the control resides</p> <p>Provisions should be made for periodic and post-maintenance verification, to confirm that the security features are properly configured and operating.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>IAEA, Nuclear Security Series No. 17, Computer Security at Nuclear Facilities, Vienna, 2011.</li> <li>IEEE, 7-4.3.2, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, Piscataway, New Jersey, 2010.</li> <li>IEC, 61513, Nuclear Power Plant - Implementation and Control Important to Safety - General Requirements for Systems, Geneva, 2011.</li> <li>NEI, 08-09, rev.6, Cyber Security Plan for Nuclear Power Reactors, Washington, D.C., 2010.</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>NEI, 10-04, rev.2, Identifying Systems and Assets Subject to the Cyber Security Rules, Washington, D.C., 2012.</li> <li>U.S. NRC, Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, Washington, D.C., 2010.</li> </ul>		
7.23	<p>NPPs are subject to the obligations arising from Canada's international agreements, and to requirements pertaining to safeguards and non-proliferation.</p> <p>The design and the design process shall ensure compliance with the obligations arising from the safeguards agreement between Canada and the IAEA. These features allow for the permanent installation of safeguards equipment and the provision of services required for the ongoing operation of that equipment shall be provided.</p> <p>Guidance</p> <p>For the purposes of this document, the term "safeguards" denotes a system of inspection and other verification activities undertaken by IAEA in order to evaluate a state's compliance with its obligations, pursuant to its safeguards agreement with the IAEA, under the Treaty on the Non-</p>	Due to sensitivity of information the assessment is documented elsewhere.	RNA





Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Proliferation of Nuclear Weapons. The objective of the Canada-IAEA safeguards agreement is for the IAEA to provide annual assurance to Canada and to the international community that all declared nuclear material is employed in peaceful, non-explosive uses, and that there is no indication of undeclared nuclear material or activities.</p> <p>The CNSC is the governmental authority responsible for implementing the Canada-IAEA safeguards agreement.</p> <p>Safeguards considerations should be integrated during the early design phase of a new NPP. This approach is a well-established practice in the Canadian nuclear industry and can avoid the retrofitting of safeguards equipment after a design is completed, which could otherwise result in substantial cost increases in terms of redesign work, timeline extensions and additional demands on human resources. If there is a requirement to install IAEA safeguards equipment to monitor nuclear material flows and inventories, accurate plant layout requirements should be identified early in the process, so as to ensure that appropriate “design space” is allocated for critical safeguards installations equipment.</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>CNSC, RD-336, Accounting and Reporting of Nuclear Material, Ottawa, Canada, 2010.</li> <li>CNSC, GD-336, Guidance for Accounting and Reporting of Nuclear Material, Ottawa, Canada, 2010.</li> </ul>		
7.24	<p>Future plant decommissioning and dismantling activities shall be taken into account, such that:</p> <ol style="list-style-type: none"> <li>materials are selected for the construction and fabrication of plant components and structures with the purpose of minimizing eventual quantities of radioactive waste and assisting decontamination</li> <li>plant layout is designed to facilitate access for decommissioning or dismantling activities, including for plants with multiple units at a site, periods when some units are operating and some are under decommissioning</li> <li>consideration is given to the future potential</li> </ol>	<p>A new requirement for the plant layout design to consider plants with multiple units at site is introduced in item 2.</p> <p>At the time Bruce B was designed, no special considerations were given to decommissioning of the plant. However, based upon experience from NPD and Douglas Point materials were chosen to minimize the Cobalt production, thereby meeting the intent of the first requirement. Any materials now added to the plant are chosen with this objective in mind. In regard to item 3 there are adequate facilities on-site at the BNPD Waste management site to store radioactive waste that would result from decommissioning activities.</p> <p>Responsibility for decommissioning of the plant remains with Ontario Power Generation. Bruce Power however has a Preliminary Decommissioning Plan and other supporting documentation as indicated in Condition 11.2 of the Bruce A and B Operating Licence [PROL 18.00/2020].</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>requirements for storage of radioactive waste generated as a result of new facilities being built, or existing facilities being expanded</p> <p>Guidance</p> <p>Future plant decommissioning and dismantling activities considered at the design phase should include considerations of experience gained from the decommissioning of existing plants, as well as those plants that are in long-term safe storage. Experience suggests that the decommissioning of NPPs could be facilitated if it received greater attention at the design stage. The consideration of decommissioning at the design stage is expected to result in lower worker doses and reduced environmental impacts.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>• CNSC, G-219, Decommissioning Planning for Licensed Activities, Ottawa, Canada, 2000.</li> <li>• CSA Group, N294, Decommissioning of Facilities Containing Nuclear Substances, Ottawa,</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Canada.</p> <ul style="list-style-type: none"> <li>IAEA, TECDOC-1657: Design Lessons Drawn from the Decommissioning of Nuclear Facilities, Vienna, 2011.</li> <li>IAEA, Safety Guide WS-G-2.1, Decommissioning of Nuclear Power Plants and Research Reactors, Vienna, 1999.</li> <li>Nuclear Energy Agency (NEA), No. 6924, Applying Decommissioning Experience to the Design and Operation of New Nuclear Power Plants, Organization for Economic Cooperation and Development, Paris, 2010.</li> <li>NEA, No. 6833, Decommissioning Considerations for New Nuclear Power Plants, Organization for Economic Cooperation and Development, Paris, 2010.</li> </ul>		
8.1	<p>Reactor core parameters and their limits shall be specified. The design shall consider all foreseeable reactor core configurations for normal operation.</p> <p>The reactor core, including the fuel elements, reactivity control mechanisms, reflectors, fuel channel and structural parts, shall be designed so that the reactor can be shutdown, cooled and held subcritical with an adequate margin in operational states, DBAs and DEC's.</p>	<p>New requirements have been introduced in the first three paragraphs of this clause. Additional changes have been made in the design of the reactor core portion.</p> <p>The Operational Safety Requirements for Bruce B Fuel and Reactor Physics document NK29-OSR-31000-00001, R000] provides the definition of and the rationale for, the Operational Safety Requirements (OSRs) for Fuel and Reactor Physics. These requirements are developed based on Safety Analysis Limits, which are derived from the safety analysis and supporting documents. The Safety Analysis Limits define the minimum hardware functional and performance requirements and the limiting process parameter values in the hardware subsystems, and are used</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The anticipated upper limit of possible deformation or other changes due to irradiation conditions shall be evaluated. These evaluations shall be supported by data from experiments, and from experience with irradiation. The design shall provide protection against those deformations, or any other changes to reactor structures that have the potential to adversely affect the behaviour of the core or associated systems.</p> <p>The reactor core and associated structures and cooling systems shall:</p> <ol style="list-style-type: none"> <li>1. withstand static and dynamic loading, including thermal expansion and contraction</li> <li>2. withstand vibration (such as flow-induced and acoustic vibration)</li> <li>3. ensure chemical compatibility, including service-related contaminants</li> <li>4. meet thermal material limits</li> </ol>	<p>to ensure that there is sufficient margin to the nominal automatic actuation setpoints to account for instrument loop uncertainty. In general, the OSRs and Safety Analysis Limits for parameters associated with the Fuel and Reactor Physics Processes can be divided into three separate specifications based on physical characteristics: power, reactivity and core configuration.</p> <p>The normal operating conditions that were considered in the design, including those during SDS2 firing (not including emergency conditions) are listed in Table 4-4 of Part 2 of the Safety Report. The current values of the Bruce B licensing limits are provided in the Bruce B OP&amp;P [BP-OPP-00001, R019].</p> <p>The design limits and margins as required in the second paragraph of this clause (i.e., reactor core, including the fuel elements, reactivity control mechanisms, etc.) for DEC's cannot be confirmed in the existing design documentation. Therefore, it is assessed as a gap. (Gap).</p> <p>Section 4 of Part 2 of the Safety Report describes the mechanical and nuclear design of the reactor. Additional details are provided in the design manuals for different components of the reactor</p> <p>The allowable deflection limits are established by the ASME code such that the allowable stresses remain within elastic limits except where acceptance of some permanent strain is necessary to be compatible with the functional requirements (section 4.1.1.4.4 of Part 2 of the Safety Report). In this case, the permanent strain limits can be calculated by the use of Tables AHA-1, AHA-2, and AHA-3 of the ASME Code Section VIII, Division 2. Deflections are limited under design</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>5. meet radiation damage limits</p> <p>The reactor core design shall include provisions for a guaranteed shutdown state as described in section 7.11.</p> <p>The design of the core shall be such that:</p> <p>1. the fission chain reaction is controlled during operational states</p> <p>2. the maximum degree of positive reactivity and its maximum rate of increase by insertion in operational states and DBAs are limited by a combination of the inherent neutronic characteristics of the core, its thermal-hydraulic characteristics, and the capabilities of the control system and means of shutdown, so that no resultant failure of the reactor pressure boundary will occur, cooling capability will be maintained, and no significant damage will occur to the reactor core</p> <p>The shutdown margin for all shutdown states shall be such that the core will remain subcritical for any credible changes in the core configuration and reactivity addition.</p>	<p>and all service conditions such that the reactivity control units remain operable, except for where some of the reactivity control limits are assumed to be disabled as a result of a postulated accident and the number of such disabled units is shown to be acceptable. The calandria tubes and calandria shell are designed for limited deflection under external pressure [NK29-SR-01320-00001, R005].</p> <p>System and component design pressures and temperatures are tabulated in Table 5-1 of Part 2 of the Bruce B Safety Report. The component and system test pressures are established in accordance with the rules for the appropriate component Class of Section III of the ASME Code. The design of the HT circuit satisfies the rules of Section III of the ASME Code for Class 1 components as a minimum (section 5.2.1 of Part of the Safety Report). Relevant case interpretations of Section III of the ASME Code were applied in the design of the main circuits.</p> <p>Table 4-4 of Part 2 of the Bruce B Safety Report lists the operating conditions that were considered in the design. The stress analysis of all systems and major components in the HT system meets the requirements of Section III of the ASME Code. The types of stress analysis employed are tailored to the particular requirements for each system and component, and are identified in the stress reports produced for Class 1 systems and components. The faulted conditions considered in the pressure boundary analysis are identified in the stress reports produced for systems and components.</p> <p>The safety analysis for Bruce B has demonstrated that the systems provided are capable of shutting down and maintaining the reactor subcritical following the Canadian equivalent of Design Basis Accidents, as well as providing</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>If operator intervention is required to keep the reactor in a shutdown state, the feasibility, timeliness, and effectiveness of such intervention shall be demonstrated.</p> <p>Guidance on nuclear design</p> <p>The design of the reactor core should provide confidence that the permissible design limits, under operational states, DBAs and DECAs, are not exceeded, taking into account engineering tolerances and uncertainties associated with the calculations.</p> <p>The nuclear design deals with flux and power distribution within the reactor core, the design and use of reactivity control systems for normal operation and for shutting down the reactor, core stability, the various reactivity feedback characteristics, and the physics of the fuel.</p> <p>The design of the reactor core and associated coolant and fuel systems should take into account all practical means so that, in the power operating range, the net effect of the prompt inherent nuclear feedback characteristics tends to compensate for a rapid increase in reactivity and</p>	<p>adequate cooling. Any failures of internal components caused by the accident have been factored into the analyses. According to Section 10.1.4 of Part 2 of the Safety Report, Flow Straightening Inlet Shield Plugs, FSISPs, have been added in the region the inner cooling zone and selected outer zone channels which are suspected to have high acoustics. The FSISP decrease the axial gap between the fuel string and the inlet shield plug. Debris fretting flaw monitoring is included as part of the life-cycle inspection requirements and no unacceptable flaws have been detected based upon the full length fuel channel inspections completed to date. FSISPs reduce water turbulence, and consequently the vibration of the inlet bundles and the fretting. The transition to fuelling with the flow and the simultaneous reduction of the length of fuel strings from 13 to 12 bundles has eliminated the requirement for abnormally supported bundles in the inlet rolled joint area, although frets at the inlet rolled joint burnish mark are present in many channels from abnormally supported bundles before core conversion was completed. As defined in Section 4.1 of the Safety Report and Appendix B of Life Cycle Management (LCM) for Critical SSCs [BP-PROC-00400, R002] monitoring of pressure tube fretting wear will be captured by the Bruce B Fuel Channel Life Cycle Management. The LCMs and associated inspection programs ensure that the potential impact of vibration is monitored for components that may be affected.</p> <p>Plant Chemistry Management Program [Chemistry Management, BP-PROC-12.02, R006] has the objective to establish the optimum conditions for system chemistry and to mitigate conditions that could lead to an adverse effect on nuclear safety, radiological safety, personnel safety, environmental safety or plant condition. Further details of</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>power. The consequences of those accidents that would be aggravated by a positive reactivity feedback should be either acceptable, or be satisfactorily mitigated by other design features.</p> <p>The design should take into account measurements made in previous reactors and critical experiments and their use in the uncertainty analyses. The design should define the measurements to be made, including start-up confirmatory tests and periodically required measurements.</p> <p>The design should provide for I&amp;C to:</p> <ul style="list-style-type: none"> <li>maintain the variables and systems within prescribed operating ranges</li> <li>monitor variables and systems that can affect the fission process over anticipated ranges for operational states, DBAs and DEC's</li> </ul> <p>These I&amp;Cs should be demonstrated to be effective.</p> <p>Defence in depth</p>	<p>design provisions for chemical control are presented in Section 11.2.3 of Part 2 of the Safety Report and the Chemistry Design Manual. The Fuel Performance Management process [Fuel Performance Management, BP-PROC-01032, R000, December 24, 2015] is defined to manage fuel performance for the duration of the fuel design life with the objective to achieve and maintain failure-free nuclear fuel performance during its use in the reactor, handling and storage. As described in BP-PROC-01032, nuclear fuel shall be effectively designed, procured, transferred, stored, inspected, inserted, shifted and discharged in a manner that ensures optimum reactor core operation within regulatory, safe operating and nuclear fuel performance limits, minimizing radiation exposure and that protecting fuel from damage throughout the fuel life cycle. This is ensured through continuous evaluation of performance against the established fuel design basis and operating envelope, and adverse performance is fed back through the appropriate process for mitigation and/or correction in support of achieving a goal of operating with zero defects. The Design Authority for fuel is delegated to the Department Manager, NSAS per DIV-ENG-00009, Design Authority. All fuel design activities, including modifications and updates are the responsibility of the Fitness for Service Assessment section (FSA) within NSAS. Changes and modifications will be defined, planned, implemented and controlled consistent with BP-PROC-10.02, Engineering Change Control, and the implementing procedures, as deemed applicable, with FSA as the lead.</p> <p>As discussed in Bruce B Safety Report the Heat Transport system's main circuit provides reliable cooling of the fuel under all operating conditions for the life of the plant. The</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The nuclear design should incorporate inherently safe features to reduce the reliance on engineered safety systems or operational procedures. Defence in depth and related principles should be applied in the design of the reactivity control safety function, such that the fission chain reaction is controlled during operational states, and, when necessary, terminated for DBAs and DEC's.</p> <p>The nuclear design should provide for effective means to ensure success of the following safety functions to:</p> <ul style="list-style-type: none"> <li>• prevention of unacceptable reactivity transients</li> <li>• shutdown of the reactor as necessary to prevent progression of AOOs to DBAs, or DBAs to DEC's</li> <li>• maintain and monitor the reactor in a safe shutdown state</li> </ul> <p>Core power densities and distributions</p> <p>The design limits for the power densities and power distributions should be determined from an integrated consideration of fuel design limits,</p>	<p>reactor coolant system is a barrier to the release of radioactive fission products and is therefore designed to retain its integrity under normal and abnormal conditions. Main circuit pressure boundary design described in Section 5.2 of Part 2 of the Safety Report demonstrates the reliability of the HT system pressure boundary design and Section 5.3 presents details of how the fuel channel pressure boundary design meets the design objectives.</p> <p>The design provisions for achieving guaranteed shutdown state are presented in Section 7.11 of this assessment.</p> <p>The modified requirement for reactor core design in item 2 may be interpreted as a requirement for negative reactivity feedback as it refers to the combination of the inherent neutronic characteristics and its thermal-hydraulic characteristics and the capability of control system and means of shutdown (i.e., self-limiting capability as a result of negative power coefficient). The basic design features of CANDU reactors described in Section 1.2 of Part 2 of the Safety Report effectively mitigate the consequences of those accidents that would be exacerbated by a positive reactivity feedback.</p> <p>The reactor regulating system is designed to maintain overall reactivity control during normal operation and following a range of AOOs by controlling the light water level in the liquid zone controllers. Under certain transient conditions, i.e., AOOs, if the reactivity range of the liquid zone controllers is exceeded, then further control via the regulating system is through the use of the control absorbers. Analysis of the Bruce B core has shown that it meets the requirements for overpressure protection. The safety analyses have demonstrated that the fuel either remains cool or cooling is</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>thermal limits, decay heat limits, and AOO and accident analyses. For power distribution, the reactor core design should demonstrate the following:</p> <ul style="list-style-type: none"> <li>There is a high level of confidence that the proposed design limits can be met within the expected operational range of the reactor, taking into account:</li> <li>the analytical methods and data for the design calculations</li> <li>uncertainty analyses and experimental comparisons presented for the design calculations</li> <li>the sufficiency of design cases calculated covering times in fuel reload cycle, or during on-power fuelling (depending upon the reactor design, reactivity devices configurations, and load-follow transients)</li> <li>special problems (such as power spikes due to densification), possible asymmetries, and misaligned reactivity devices</li> <li>There is a high level of confidence that, during normal operation, the design limits will not be exceeded, based on consideration of information received from the power distribution monitoring instrumentation. The processing of that information should include:</li> </ul>	<p>re-established in the event of a LOCA such that the allowable release limits are met for all AOOs and DBAs. The safety analyses have shown that even for the largest LOCA the fuel damage is limited and no failure of pressure tubes is predicted. Thus, the reactor core remains intact. In the case of a single channel failure (PT/CT rupture) the dynamic forces resulting during the blow down cause some damage to the internal structures but enough shutoff rods remain intact to meet all the relevant requirements. The calandria vessel does not fail from the resulting over-pressure transient.</p> <p>As demonstrated in Part 3 of the Safety Report, the safety analyses have shown that for the most reactive accident, SDS1 can keep the reactor subcritical for at least 15 minutes, before operator action is required. This is consistent with the current CNSC requirements of 15 minutes for actions initiated in the MCR (Section 4.4.4.5 Guidance for operator action of CNSC REGDOC-2.4.1). SDS2 can keep the reactor shut down indefinitely without operator intervention.</p> <p>The safety analyses have demonstrated that the fuel either remains cool or cooling is re-established in the event of a LOCA such that the allowable release limits are met for all AOOs and DBAs. The safety analyses have shown that even for the largest LOCA the fuel damage is limited and no failure of pressure tubes is predicted. Thus, the reactor core remains intact. In the case of a single channel failure (PT/CT rupture) the dynamic forces resulting during the blowdown cause some damage to the internal structures but enough shutoff rods remain intact to meet all the relevant requirements. The calandria vessel does not fail from the resulting over-pressure transient.</p> <p>The on-going surveillance, inspection and maintenance and</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>calculations (instrument-calculation correlations) involved in the processing</li> <li>operating procedures used</li> <li>the requirements for periodic check measurements</li> <li>the accuracy of design calculations used in developing correlations when primary variables are not directly measured</li> <li>the uncertainty analyses for the information and processing system</li> <li>the requirements for instruments, the calibration and calculations involved in their use, and the uncertainties involved in conversion of instrument readings into power distribution</li> <li>the limits and set points for control actions, alarms, or automatic trip for instrument systems and demonstration that these systems can maintain the reactor within design power distribution limits (including the instrumentation alarms for the limits of normal operation (e.g., offset limits, control bank limits) and for abnormal situations (e.g., flux tilt alarms)</li> <li>measurements in previous reactors and critical experiments, including their use in the uncertainty analyses</li> <li>measurements needed for start-up confirmatory tests and the required periodical measurements</li> </ul>	<p>major component replacement programs, R&amp;D activities and the use of OPEX provides further confidence in robustness of the design, the adequacy of the safety margins and allows mitigation of impacts of ageing. In addition, extensive tests were undertaken both prior to and since the start of operation using the 37 element fuel bundles in Bruce A and Bruce B (section 10.1.4 of Part 2 of the Safety Report). As specified in Fuel Performance Management procedure [BP-PROC-01032, R000, December 24, 2015] all work groups whom participate in Fuel Performance Management are responsible for highlighting any observed adverse fuel performance issues by means of different processes such as Station Condition Records (SCRs), processing of external and internal operating experience, participation in the CANDU Owners Group Fuel Normal Operating Conditions Working Group, etc. Almost 30 years of successful operation with low fuel failure rates has confirmed that the fuel is capable of withstanding the majority of these conditions. The results of these tests and operating experience have been documented in various Bruce Power and Industry reports.</p>	



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The limiting power distributions should be determined such that the limits on power densities and peaking factors can be maintained in operation. These limiting power distributions may be maintained (i.e., not exceeded) administratively (i.e., not by automatic shutdown), provided a suitable demonstration is made that sufficient, properly translated information and alarms are available from the reactor instrumentation to keep the operator informed.</p> <p>The design should establish the correlation between design power distributions and operating power distributions, including instrument-calculation correlations, operating procedures used, and measurements that will be taken. Necessary limits on these operations should be established.</p> <p>The breakdown of design power distributions into the following components should be established:</p> <ul style="list-style-type: none"><li>• power generated in the fuel</li><li>• power generated directly in the coolant and moderator</li><li>• power generated directly in the core</li></ul>		



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>internals</p> <p>The reference design core power distributions (axial, radial, and local distributions and peaking factors) used in AOO and accident analyses should be established. In addition, power distributions within fuel pins should be established.</p> <p>The design limits for power densities (and thus for peaking factors) during normal operation should be such that acceptable fuel design limits are not exceeded during AOOs and that other limits are not exceeded during DBAs and DECAs. The design limits, along with related uncertainties, operating limits, instrument requirements, and set-points, should be incorporated into OLCs.</p> <p>Reactivity coefficients</p> <p>The design should establish and characterize the bounding reference values for reactivity coefficients. These reference values should be conservative.</p> <p>The range of plant states to be covered should include the entire operating range – from cold</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>shutdown through full power – and the extremes reached in AOOs, DBAs and DEC. It should include the full range of the fuelling cycle, and an appropriate range of reactivity device configurations.</p> <p>The design calculations of reactivity coefficients should cover the full applicable range of the variables and modelling approximations in AOO and accident analyses, including approximations related to modelling and nodalization of the reactor cooling system. Where applicable, the difference between intra- and inter-assembly moderator coefficients needs to be established.</p> <p>Conservatism should be considered based on:</p> <ul style="list-style-type: none"> <li>the use of a coefficient (i.e., the analyses in which it is important)</li> <li>whether state of the art tools have been used for calculation of the coefficient</li> <li>the uncertainty associated with such calculations, experimental checks of the coefficient in operating reactors</li> <li>any required checks of the coefficient in the start-up program following significant core reconfiguration</li> </ul>		



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design calculation should cover and be supported by the following:</p> <ul style="list-style-type: none"> <li>calculated nominal values for the reactivity coefficients, such as the coolant and moderator coefficients (temperature, void, or density coefficients), the Doppler coefficient and power coefficients</li> <li>uncertainty analyses for nominal values, including the magnitude of the uncertainty and the justification of the magnitude (by examination of the accuracy of the methods used in calculations), and comparison, where possible, with reactor experiments.</li> <li>combination of nominal values and uncertainties to provide suitably conservative values for use in reactor steady-state analysis (primarily control requirements), stability analyses, and the AOO and accident analyses</li> </ul> <p>For comparisons to experiments, it is important to show that the experiments are applicable and relevant, and the experimental conditions overlap the operating and anticipated accident conditions.</p> <p>It is recognized that reactivity coefficients of the design are important in determining the reactor</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>behavior and safety characteristics. This document does not have specific requirements on the sign or magnitude of the reactivity coefficients including the power coefficient of reactivity. Instead, this document requires a number of design provisions related to the nuclear design to ensure that the design is acceptable for reactor control, stability and plant safety. If a reactor design has a positive power coefficient of reactivity for any operating state, the design authority should demonstrate that operation with a positive power coefficient is acceptable, by showing:</p> <ul style="list-style-type: none"> <li>• a bounding value of power coefficient of reactivity has been calculated for all permitted operating states and used in control, stability, and safety analyses</li> <li>• measurements of the power coefficient of reactivity are conducted at start-up and periodically for certain operating limiting core conditions to demonstrate that measured values are bounded by calculated values with adequate margin</li> <li>• the reactor control system is designed with adequate reliability and has the capability to automatically accommodate for a positive power coefficient of reactivity for a wide range of AOOs</li> </ul>		



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design should ensure that the likelihood of exceeding specified criteria of the AOOs without shutdown is sufficiently small, by demonstrating either that the criteria are met, or that a diverse shutdown means is installed, which reduces significantly the probability of a failure to shutdown.</p> <p>Criticality</p> <p>The nuclear design should ensure that the criticality of the reactor during refuelling is controlled. If on-power refuelling is used to compensate for core reactivity depletion, the nuclear design should establish the values of core excess reactivity, maximum local powers, amount of fuel loaded per refuelling operation and frequency of refuelling load. The design should also ensure that the maximum core excess reactivity and predicted local power peaks will not exceed the control system capability and fuel thermal limits.</p> <p>Core stability</p> <p>Power oscillations that could result in conditions exceeding specified acceptable fuel design limits should be reliably and readily detected and</p>		



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>suppressed.</p> <p>Assessment of reactor core stability should include:</p> <ul style="list-style-type: none"><li>• phenomena and reactor aspects that influence the stability of the nuclear reactor core</li><li>• calculations and considerations given to xenon-induced spatial oscillations</li><li>• potential stability issues, due to other phenomena or conditions</li><li>• verification of the analytical methods for comparison with measured data</li></ul> <p>Analytical methods</p> <p>The analytical methods and database used for nuclear design and reactor physics analyses should be consistent with modern best practices. Also, the experiments used to validate the analytical methods should be adequate representations of fuel designs in the reactor and ranges of key parameters in the validation database should overlap those expected in design and safety analysis.</p>		



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design should be such that the analytical methods used in the nuclear design (including those for predicting criticality, reactivity coefficients, burnup and stability) as well as the database and nuclear data libraries used for neutron cross-section data and other nuclear parameters (including delayed neutron and photo neutron data and other relevant data) are adequate and fit for application, based on adequate qualification. The qualification should be based on proven practices for validation and verification, using the acceptable codes and standards.</p> <p>A validation or verification method can be proven either by meeting accepted verification and validation standards, or by established practice, or some combination of these. New method(s) are</p> <p>“proven” by performing a number of acceptance and demonstration tests that show the method(s) meets pre-defined criteria.</p> <p>Core internals and vessel</p> <p>The nuclear design should establish:</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>neutron flux spectrum above 1 million electron volts (MeV) in the core, at the core boundaries, and at the inside vessel wall, if applicable</li> <li>assumptions used in the calculations, these include the power level, the use factor, the type of fuel cycle considered, and the design life of the vessel</li> <li>computer codes used in the analysis</li> <li>the database for fast neutron cross-sections</li> <li>the geometric modelling of the reactor core, internals, and vessel(s)</li> <li>uncertainties in the calculations</li> </ul> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>CSA Group, N286.7.1, Guideline for the application of N286.7-99, Quality assurance of analytical, scientific, and design computer programs for nuclear power plants, Toronto, Canada.</li> <li>CSA Group, N286.7, Quality Assurance of Analytical, Scientific, and Design Computer</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Programs for Nuclear Power Plants, Toronto, Canada.</p> <ul style="list-style-type: none"> <li>• CSA Group, N290.4, Requirements for reactor control systems of nuclear power plants, Toronto, Canada.</li> <li>• CSA Group, CAN3-N290.1, Requirements for the Shutdown Systems of CANDU Nuclear Power Plants, Toronto, Canada.</li> <li>• IAEA, NS-G-2.5, Core Management and Fuel Handling for Nuclear Power Plants, Vienna, 2002.</li> <li>• IAEA, NS-G-1.12, Design of the Reactor Core for Nuclear Power Plants, Vienna, 2005.</li> <li>• U.S. NRC, Regulatory Guide 1.77, Assumptions Used for Evaluating a Control Rod Ejection Accident for Pressurized Water Reactors, Washington, D.C., 1974.</li> <li>• U.S. NRC, Regulatory Guide 1.203, Transient and Accident Analysis Methods, Washington, D.C., 2005.</li> </ul> <p>Guidance on core management and fuel handling</p> <p>The reactor design should be such that the plant will operate within the specified operating limits for the entire reactor lifecycle (including intermediate reactor core states).</p>		



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design should provide for functional tests to be performed periodically for monitoring the health of the reactor components.</p> <p>The design should provide for the capability to monitor online important core parameters, to ensure that the acceptable operating limits for the reactor are not exceeded during normal operation. The types of detectors and other devices used in monitoring the core parameters should be described.</p> <p>The reactor control strategy should be defined, to ensure that the reactor will be restored to an acceptable safe state if any reactor parameter deviates from its allowed domain. The control strategy should be such that fuel integrity will be maintained for all AOOs.</p> <p>The refuelling scheme should be developed to ensure that the intermediate refuelling configurations do not have more reactivity than the most reactive configuration approved in the design. The core parameters for the intermediate configurations should be within their approved limits.</p>		



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design should allow for data acquisition during reactor operation and record-keeping for later retrieval and analysis.</p> <p>The design should take into account the details of fuel management strategy including the loading of fuel into the fresh core, and the criteria for determining the location of fuel assemblies to be unloaded from the reactor and loaded with fresh fuel.</p> <p>For reactor designs where a significant fraction of the fuel is replaced or shuffled during fuelling, the design should provide for diagnostic tests at startup. These tests should verify that the core parameters are within their allowed range.</p> <p>Guidance on mechanical design of reactor internals</p> <p>The reactor internals classified as core support structures according to the ASME Boiler and Pressure Vessel Code (BPVC), Section III, Division 1, NG-1121, Core Support Structures, should be designed, fabricated, and examined in accordance with the provisions of ASME BPVC Section III Division 1, subsection NG.</p>		



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Those reactor internals not classified as ASME BPVC Code, Section III, Division 1, Core Support Structures should be classified as internal structures in accordance with ASME Code, Section III, Division 1, Subsection NG-1122. The design criteria, loading conditions, and analyses that provide the basis for the design of reactor internals (other than the core support structures) should meet the guidelines of ASME Code, Section III, Division 1, Subsection NG-3000, and be constructed so as to not adversely affect the integrity of the core support structures. If other guidelines (e.g., manufacturer standards or empirical methods based on field experience and testing) are the bases for the stress, deformation, and fatigue criteria, those guidelines should be identified and their use justified in the design.</p> <p>For non-ASME code structures, components and supports, design margins presented for allowable stress, deformation, and fatigue should be equal to or greater than margins for other plants of similar design with successful operating experience. Any decreases in design margins should be justified.</p> <p>Specific reactor internals of a high safety class should be designed, fabricated, and examined in accordance with the applicable codes and</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	standards, such as ASME Section III for light water reactors (LWR), and CSA N285.0, General Requirements for Pressure-retaining Systems and Components in CANDU Nuclear Power Plants for CANDU.		
8.1.1	<p>Fuel assembly design shall include all components in the assembly, such as the fuel matrix, cladding, spacers, support plates, movable rods inside the assembly etc. The fuel assembly design shall also identify all interfacing systems.</p> <p>Fuel assemblies and the associated components shall be designed to withstand the anticipated irradiation and environmental conditions in the reactor core, and all processes of deterioration that can occur in operational states. The fuel shall remain suitable for continued use after AOOs. At the design stage, consideration shall be given to long-term storage of irradiated fuel assemblies after discharge from the reactor.</p> <p>Fuel design limits shall be established to include, as a minimum, limits on fuel power or temperature, limits on fuel burnup, and limits on the leakage of fission products in the reactor cooling system. The design limits shall reflect the importance of preserving the fuel matrix and cladding, as these are first and second barriers to fission product release, respectively.</p>	<p>A new requirement is added in the second paragraph for the fuel to remain fit for service after AOOs.</p> <p>The fuel bundles design is described in Section 10.1.2 of Part 2 of the Safety Report and Fuel Design Manuals [NK29-SR-01320-00001, Rev.5]. The fuel assemblies are bundles of 37 cylindrical elements made up of compacted and sintered uranium dioxide pellets in zirconium alloy sheaths. These elements are the same as those used in Bruce A. The fuel channel cross-section and the 37-element fuel bundle cross-section are shown in Figures 4-23 and 4-24, respectively.</p> <p>A summary of the normal length fuel bundle specifications is given in Table 10-1, the summary of the fuel channel specifications in Table 10-2 [NK29-SR-01320-00001, Rev.5]. The fuel elements are held together in a bundle by end-plates and are separated from each other by spacers attached to the sheaths near the mid-plane of the bundle, as shown in Figure 10-1 [NK29-SR-01320-00001, Rev.5].</p> <p>The spacers are of the skewed split spacer type. One half of the spacer is attached to each of two neighbouring elements such that the half-spacers contact each other. The spacers are skewed from the element axis to reduce the possibility of becoming locked one against the other during handling. Fretting wear between the spacers is typically such that the average inter-element spacing at the end of the fuel life is not expected to be less than 1.0 mm (0.040 in). The fuel is</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design shall account for all known degradation mechanisms, with allowance being made for uncertainties in data, calculations, and fuel fabrication.</p> <p>Fuel assemblies shall be designed to permit adequate inspection of their structures and components prior to and following irradiation.</p> <p>In DBAs, the fuel assembly and its component parts shall remain in position with no distortion that would prevent effective post-accident core cooling or interfere with the actions of reactivity control devices or mechanisms. The design shall specify the acceptance criteria necessary to meet these requirements in DBAs.</p> <p>The requirements for reactor and fuel assembly design shall apply in the event of changes in fuel management strategy, or in operating conditions, over the lifetime of the plant.</p> <p>Fuel design and design limits shall reflect a verified and auditable knowledge base. The fuel shall be qualified for operation, either through experience with the same type of fuel in other reactors, or through a program of experimental</p>	<p>supported in the pressure tube on bearing pads located near the ends and middle of each outer fuel element (section 10.1.2.1 of Part 2 of the Safety Report [NK29-SR-01320-00001, Rev.5]).</p> <p>The design specifications of the long fuel bundles are the same as those for the normal length fuel bundles except for an increase in bundle length of 12.7 mm (0.5 in). Implementation of long fuel bundles makes a gradual increase in the length of a fuel string possible. This in turn allows control of the axial gap between the fuel string and fuel channel end components as the fuel channel elongates due to neutron induced creep. The location of the bearing pads relative to the fuel bundle end plates is unchanged. Since all channels have been reordered and converted to a 12 bundle fuel string, the axial gap is not a concern. There are no long bundles being fuelled into the reactor (section 10.1.2.2 of Part 2 of the Safety Report).</p> <p>Qualitative acceptance criteria have been established to assess fuel and fuel channel integrity fitness-for-service (FFS) following an AOO. The COG Report "AOO Fuel and Pressure Tube Fitness-For-Service Criteria for LOF, SLOCA and Slow LORC" [COG-12-2049/CG402-RP-001 R01] document assesses fuel and fuel channel behaviour during an AOO event. Demonstration that the fuel will remain fit for service after AOO cannot be confirmed in the current design documentation. Acceptance criteria and corresponding assessments, including inspection requirements, return to service requirements or further assessments are not available; therefore this is assessed as a gap (Gap).</p> <p>The design data related to the nuclear design are presented</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>testing and analysis, to ensure that fuel assembly requirements are met.</p> <p>Guidance</p> <p>The fuel design and qualification should provide assurance that the reactor core design requirements in section 8.1 are met.</p> <p>Acceptance criteria should be established for fuel damage, fuel rod failure, and fuel coolability. These criteria should be derived from experiments that identify the limitations of the material properties of the fuel and fuel assembly, and related analyses. The fuel design criteria and other design considerations are discussed below.</p> <p>Fuel damage</p> <p>Fuel damage criteria should be established for all known damage mechanisms in operational states (normal operation and AOOs). The damage criteria should assure that fuel dimensions remain within operational tolerances, and that functional capabilities are not reduced below those assumed in the safety analysis. When applicable, the fuel damage criteria should consider high burnup</p>	<p>in Section 4.2 of Part 2 of the Safety Report.</p> <p>Two fuel burnup envelopes are used in the design and licensing of the Bruce B reactor. The higher bundle power/burn-up envelope is the reference overpower envelope. The original peak bundle power of 1035 kW exceeds the nominal design bundle power of 900 kW by 15 percent. The margin allowance of 15 percent is sufficient to include most spatial and time ripples, operational flexibility and calculation uncertainty. The use of the power/burnup envelope ensures that for any element linear power the initial internal gas pressures are overpredicted, which results in the greatest driving force for sheath strain and thus the highest potential for sheath failure due to localized overstrain (Appendix 4.2.2.21 of Part 3 of the Safety Report).</p> <p>Measurements of bundle end flux peaking effects in 37-element fuel has shown that the fuel near the ends of a bundle operate at somewhat elevated power levels. The phenomenon is referred to as end flux peaking. For the 37-element fuel design, end flux peaking can result in a localized increase in outer element power of up to a maximum of 15 percent at the very ends of a fuel stack, and on average approximately 5 percent over the end 2 or 3 pellets, depending on the fuel ring considered. However, since this effect is highly localized, it does not significantly increment the challenge to channel integrity (section 5.5.4.2.1 of Appendix 5.5 Fuel Behaviour and Fission Product Release of Part 3 of the Safety Report).</p> <p>The calculated time averaged channel power distribution is shown in Figure 4-26 (Part 2, Section 4 of this report). Figure 10-2 illustrates the bundle power versus burnup envelope. The figure shows the reference overpower envelope, which</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>effects based on irradiated material properties data. The criteria should include stress, strain or loading limits, the cumulative number of strain fatigue cycles, fretting wear, oxidation, hydriding (deuteriding in CANDU reactors), build-up of corrosion products, dimensional changes, rod internal gas pressures, worst-case hydraulic loads, and LWR control rod insertability.</p> <p>Fuel rod failure</p> <p>Fuel rod failure applies to operational states, DBAs and DEC's. Fuel rod failure criteria should be provided for all known fuel rod failure mechanisms. The design should ensure that fuel does not fail as a result of specific causes during operational states. Fuel rod failures could occur during DBAs and DEC's, and are accounted for in the safety analysis.</p> <p>Assessment methods should be stated for, fuel failure mechanisms, reactor loading and power manoeuvring limitations, and fuel duty which lead to an acceptably low probability of failure. When applicable, the fuel rod failure criteria should consider high burnup effects, based on data of irradiated material properties. The criteria should include:</p>	<p>bounds the bundle power/burnup history of normal length and long fuel bundles, and the nominal design power envelope.</p> <p>The assumed peak bundle power of 1035 kW exceeds the nominal design bundle power of 900 kW by 15%. The margin of 15% is sufficient to allow for variations in the manufacturing process, and operational and computational uncertainties. The nominal design power envelope, normalized to a peak bundle power of 900 kW, is the reference for fuel design calculations. The resulting bundle design is then assessed against the reference overpower envelope (section 10.1.3.1 of Part 2 of the Safety Report).</p> <p>As described in section 10.1.4 of Part 2 of the Safety Report, the 37-element bundle design is supported by a comprehensive development and testing program. A significant number of tests have been successfully completed to verify design parameters and compatibility of fuel with operating conditions. Flow Straightening Inlet Shield Plugs (FSISPs) have been added in the region the inner cooling zone and selected outer zone channels to reduce water turbulence, and consequently the vibration of the inlet bundles and the fretting.</p> <p>The analysis of the wear due to loading 501 bundles at random angles has indicated that the pad sliding wear would reduce the minimum sheath-to-pressure tube separation from 1.220 mm to 1.143 mm, which is acceptable (section 10.1.4.2 of Part 2 of the Safety Report).</p> <p>The bundle mechanical strength tests show that the 37-element design is compatible with the maximum forces estimated to be encountered in the Bruce B reactors. Experiments were also conducted to establish whether the</p>	




Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>• hydriding</li> <li>• cladding collapse</li> <li>• cladding overheating</li> <li>• fuel pellet overheating</li> <li>• excessive fuel enthalpy</li> <li>• pellet-clad interaction</li> <li>• stress-corrosion cracking</li> <li>• cladding bursting</li> <li>• mechanical fracturing</li> </ul> <p>Fuel coolability</p> <p>Fuel coolability applies to DBAs and, to the extent practicable, DECAs. Fuel coolability criteria should be provided for all damage mechanisms in DBAs and DECAs. The fuel should be designed to ensure that fuel rod damage will not interfere with effective emergency core cooling. The cladding temperatures should not reach a temperature high enough to allow a significant metal- water reaction to occur, thereby minimizing the potential for fission product release. The criteria should include cladding embrittlement, fuel rod ballooning, structural deformation and, in CANDU, beryllium</p>	<p>impact of one or two 37-element bundles, flowed into the channel against a stationary 12 bundle fuel string, could lead to bundle deformation. No measurable deformations were observed; therefore the concerns about fuelling with the flow are eliminated.</p> <p>Many test reactor irradiations were conducted to test the bundles (section 10.1.4.4 of Part 2 of the Safety Report), including two at constant power in the NRU reactor at the Chalk River Nuclear Laboratories as follows:</p> <ol style="list-style-type: none"> <li>1. Bundle HS ran at an outer-element linear power of about 52 kW/m to a burnup of 200 MWh/kgU.</li> <li>2. Bundle GS ran at an outer-element linear power of about 70 kW/m to a burnup of 300 MWh/kgU. In addition, a large number of 37-element bundles have been irradiated by now at Bruce A and B, further confirming the fuel bundle design compatibility with operating conditions.</li> </ol> <p>Substantial out of reactor testing has been performed on normal length and long fuel bundles to qualify long fuel and to generally improve the understanding of fuel vibration. This testing concluded that there is no significant difference in the vibration response of a long fuel bundle compared to a normal length fuel bundle for all reactor operating conditions at Bruce B (section 10.1.4.5 of Part 2 of the Safety Report).</p> <p>In addition, Bruce Power has designed and implemented changes to the fuel bundle to support the ageing and margin management programs. The modified 37-element (37M) fuel bundle improves thermal hydraulic performance leading to a significant improvement in fuel cooling capability, with no appreciable negative impact, and increases the safety margins at Bruce A and Bruce B. The Modified 37- Element</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>brazing penetration.</p> <p>Other considerations</p> <p>The design should also include:</p> <ul style="list-style-type: none"> <li>all expected fuel handling activities</li> <li>the effects of post-irradiation fuel assembly handling</li> <li>cooling flow of other components of LWR fuel assembly (such as control rods, poison rods, instrumentation, or neutron sources)</li> </ul> <p>Testing, inspection, and surveillance programs</p> <p>Programs for testing and inspection of new fuel, as well as for online fuel monitoring and post-irradiation surveillance of irradiated fuel should be established.</p> <p>Fuel specification</p> <p>The design should establish the specification of fuel rods and assembly (including LWR control</p>	<p>(37M) Fuel Bundle Implementation at Bruce B [NK29-PLAN-37000-00001, Rev.000, February 5, 2014] covers the implementation of the fuel bundle design in Bruce B Units and covers activities from the delivery of the first 37M fuel bundles to the Bruce Station to the discharge of the last 37R bundle from the reactor.</p> <p>The 37-element CANDU fuel bundles used in Bruce A and B are readily inspectable in the new fuel storage area prior to loading and in the primary irradiated fuel storage bay after irradiation. The irradiated fuel inspection logic and technical basis is provided [B-REP-37040-00007, Rev.0]</p> <p>Bruce Power is implementing the installation of a modified 37-element fuel bundle to address the impact of heat transport system aging. The 37M bundle utilizes a smaller diameter centre element to improve flow in the inner sub-channels and counteract the flow bypass caused by pressure tube diametral creep. These changes result in improvements in critical heat flux margins and critical channel powers. The final assessment of safety analysis performed to demonstrate that it is safe to operate with 37M fuel in Bruce A reactors and to confirm the improvement in safety margin for accidents impacted by aging is documented in Enclosure 1 of NK21-CORR-00531-09574]. Fuelling of 37M bundles into the inner thermalhydraulic zone fuel channels began in March 2014 and the demonstration proceeded with the loading of four 37M bundles in the Unit 6 acoustic fuel channel K22 and ended on April 8, 2015 with the start of the Unit 6 planned outage. Following operation with 37M fuel bundles from March 2014 to April 2015, fuel channel K22 was re-inspected and the results were provided in Enclosure 2 of [Letter, F. Saunders to K. Lafreniere, "Bruce B Unit 6 2015 Inspection:</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>rods) in order to minimize design deviations and to determine whether all design bases are met (such as limits and tolerances).</p> <p>Reactor core thermal hydraulic design</p> <p>The thermalhydraulic design should be such that sufficient margin exists with regard to maintaining adequate heat transfer from the fuel to the reactor coolant system, to prevent fuel sheath overheating. The design requirements can be demonstrated by meeting a set of derived acceptance criteria, as required by REGDOC-2.4.1, Deterministic Safety Analysis.</p> <p>Critical heat flux (CHF) is defined as the heat flux at departure from nucleate boiling (DNB), commonly used in pressurized water reactors (PWRs), or at dryout, commonly used in CANDU designs.</p> <p>It should be noted that, although a thermal margin criterion is sufficient to demonstrate that overheating from a deficient cooling mechanism can be avoided; other mechanistic methods may be acceptable as CHF is not considered as a failure mechanism. In some designs, CHF conditions during transients can be tolerated if it</p>	<p>Pressure Tube Flaw Component Disposition", NK29-CORR-00531-12526, June 12, 2015]. It was determined that there are no new dispositionable flaws, and that there were no changes in the dimensions of dispositionable flaws observed in inspections prior to the demonstration in K22. Based on the inspection results of the demonstration pressure tube (Unit 6 K22), there is no evidence that operation of 37M fuel bundles in acoustic channels will pose an unacceptable risk to the structural integrity of the fuel channels [Letter F. Saunders to K. Lafreniere, Action Item 1314-4554: Phase 2 Implementation of 37M Fuel in the Bruce B reactors, NK29-CORR-00531-12595, August 26, 2015]. During Phase 1 of the implementation plan it was confirmed that the 37M modification did not materially impact fuel endurance and acoustic performance. Based on the completion of the 37M demonstration (Phase 1), the CNSC staff have approved Bruce Power to proceed with Phase 2 of the 37M fuel bundles [Letter K. Lafreniere to F. Saunders, Action Item 1314-4554 Closure: Phase 2 Implementation of 37 M Fuel in the Bruce B Reactors, NK29-CORR-00531-12968, December 10, 2015].</p> <p>The following mechanisms are identified to have the potential to cause fuel degradation under accident conditions [Modified Bruce 37 Element Fuel Bundle (Reduced Diameter Centre Element Design), B-DM-37000-001, R001, Unit 018, April 2014]:</p> <ul style="list-style-type: none"> <li>- Fuel sheath strain.</li> <li>- Fuel (pellet)/cladding mechanical interaction.</li> <li>- Fuel pellet fragment axial relocation.</li> </ul>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>can be shown by other methods that the sheath temperatures do not exceed well-defined acceptable limits. However, any other criteria than the CHF criterion should address sheath temperature, pressure, time duration, oxidation, embrittlement etc., and these new criteria should be supported by sufficient experimental and analytical evidence. In the absence of such evidence, the core thermal-hydraulic design is expected to demonstrate a thermal margin to CHF.</p> <p>The demonstration of thermal margin is expected to be presented in a manner that accounts for all possible reactor operational states and conditions, as determined from operating maps including all AOOs. The demonstration should also include long term effects of plant aging and other expected changes to core configuration over the operating life of the plant.</p> <p>The demonstration of thermal margin should thoroughly address uncertainties of various parameters affecting the thermal margin. The design should identify all sources of significant uncertainties that contribute to the uncertainty of thermal margin. The uncertainty for each of the sources should be quantified with supportable evidence.</p>	<ul style="list-style-type: none"> <li>- CANLUB degradation.</li> <li>- Iodine corrosion of the sheath.</li> <li>- Fuel element bowing and bundle deformation (including end plate deformation).</li> <li>- Fuel sheath collapse into axial gaps.</li> <li>- Lobe collapse or fuel sheath longitudinal ridging.</li> <li>- Sheath oxidation.</li> <li>- Hydride formation.</li> <li>- Hydride migration.</li> <li>- Pre-defected fuel element degradation (Fuel oxidation, sheath oxidation and embrittlement).</li> <li>- Sheath embrittlement or through-wall oxidation.</li> <li>- Beryllium assisted crack penetration.</li> <li>- Athermal strain.</li> </ul> <p>Service limits to prevent unacceptable fuel degradation are determined from design manuals, CANDU operating experience (OPEX), and experiments. For the majority of DBAs the safety analyses have shown that there is no threat to fuel cooling. The "Bruce B Integrated Safety Analysis and Assessment Report (ISAAR)" [NK29-REP-03503-00013, September 12, 2012] describes the assessment performed to demonstrate it is safe to operate with 37M fuel in the Bruce B reactors, and to assess the improvement in safety margin for accidents impacted by aging. Assessments were performed for design basis accidents and operational impacts for the reactors fully fueled with 37M fuel and for transition to the full</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>In addition to the demonstration of thermal margin, the core thermal-hydraulic design should also address possible core power and flow oscillations and thermal-hydraulic instabilities. The design should be such that power and flow oscillations that result in conditions exceeding specified acceptable fuel design limits are not possible or can be reliably and readily detected and suppressed.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>ANSI/ANS, 57.5, Light Water Reactor Fuel Assembly Mechanical Design and Evaluation, La Grange Park, Illinois, 1996.</li> <li>CNSC, G-144, Trip Parameter Acceptance Criteria for the Safety Analysis of CANDU Nuclear Power Plants, Ottawa, Canada, 2006.</li> <li>U.S. NRC, NUREG-0800, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Fuel System Design, Section 4.2, Washington, D.C., 2007.</li> </ul>	<p>37M core [NK29-REP-03503-00013, Rev.0].</p> <p>It was concluded that the introduction of 37M fuel to Bruce B reactors improves safety margins for events significantly affected by the Heat Transport System ageing without introducing appreciable negative impacts, therefore supporting continued high power operation [NK29-REP-03503-00013, Rev.0].</p> <p>The fuelling strategy in a CANDU is limited to the number of fuel bundles that can be shifted at one time in any channel. This in turn governs the maximum burnup the fuel can have when irradiated fuel is shifted from lower to higher flux regions along the fuel channel. Any changes in fuelling strategy must ensure that the bundle power limits are not exceeded or that the fuel bundle power change during any one shift does not exceed allowable limits. This is assured through Bruce Power's Core Management Procedure [BP-PROC-00452, Rev.0]. Bundle Powers are not measured; they are calculated with the computer code SORO.</p> <p>Operational Safety Requirements for Bruce B Fuel and Reactor Physics [NK29-OSR-31000-00001, Rev.0] provides the definition and rationale for the operational and safety requirements for fuel and reactor physics.</p> <p>The Safety Analysis Limits define the minimum hardware functional and performance requirements and the limiting process parameter values in the hardware subsystems, and are used to ensure that there is sufficient margin to the nominal automatic actuation setpoints to account for instrument loop uncertainty. The OSRs and Safety Analysis Limits are grouped into three specifications based on physical characteristics as follows: power, reactivity and core</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>configuration. The applicable analyses that were used to derive the safety analysis limits for reactor physics parameters are presented as well. The current values of Bruce B licensing limits are given in the Bruce B Operating Policies and Principles [BP-OPP-00001, R019].</p> <p>BP-PROC-00363, R003, "Nuclear Safety Assessment", takes into account the effects of ageing and ensures the safety analysis provides a basis for safe operation.</p> <p>As per above, the ISAAR concluded that the introduction of 37M fuel to Bruce B reactors improves safety margins for events significantly affected by the Heat Transport System ageing without introducing appreciable negative impacts, therefore supporting continued high power operation [NK29-REP-03503-00013, Rev.0].</p> <p>In addition, analysis of the main events impacted by ageing, are revised to reflect plant conditions applicable to the licence duration. The most recent ageing analyses to 2019 are documented in Letter F. Saunders to R. Lojk, Safety Analysis Submission in Support of Operation of Bruce A and Bruce B to 2019, NK21-CORR-00531-10943 / NK29-CORR-00531-11325, December 12, 2013.</p>	
8.1.2	<p>The design shall provide the means for detecting levels and distributions of neutron flux. This shall apply to neutron flux in all regions of the core during normal operation (including after shutdown and during and after refuelling states), and during AOOs.</p> <p>The reactor core control system shall detect and</p>	<p>A new requirement is introduced for the design to take account of wear-out of the effects of irradiation, burnup etc. in the design of the reactivity devices.</p> <p>As described in Sections 4 and 7 of Part 2 of the Safety Report, the Bruce B reactor control system is designed to control both core flux and process parameters to predetermined levels under normal operating conditions. The flux shapes in the core can be measured by detectors in the</p>	IC



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>intercept deviations from normal operation with the goal of preventing AOOs from escalating to accident conditions.</p> <p>Adequate means shall be provided to maintain both bulk and spatial power distributions within a predetermined range.</p> <p>The control system shall limit the positive reactivity insertion rate to a level required to control reactivity changes and power manoeuvring.</p> <p>The control system, combined with the inherent characteristics of the reactor and the selected operating limits and conditions, shall minimize the need for shutdown action.</p> <p>The control system and the inherent reactor characteristics shall keep all critical reactor parameters within the specified limits for a wide range of AOOs.</p> <p>In the design of the reactivity control devices, due account shall be taken of wear-out and of the effects of irradiation, such as burnup, changes in physical properties and production of gas.</p>	<p>regulating system (process system) and in both shutdown systems (special safety systems).</p> <p>Different types of detectors are used in the process and safety systems and they are totally independent of each other, thereby ensuring that common mode failure of all detectors is very unlikely. As described in section 4.1.2.2.2 of Part 2 of the Safety Report, the reactor has both vertical and horizontal in-core flux detectors. The vertical units house three types of detectors: Inconel, platinum clad Inconel, and vanadium. The Inconel and platinum clad Inconel detectors provide signals to SDS1 and the reactor regulating system, respectively. The vanadium flux detectors are no longer used for flux mapping but remain in-core. A typical vertical unit is shown in Figure 4-10. The vertical flux detector units are of the straight individually replaceable type. The horizontal units house platinum clad Inconel detectors that provide signals to SDS2. A typical horizontal unit is shown in Figure 4-11, section 4 of Part 2 of the Safety Report.</p> <p>The horizontal flux detector units are of the straight, individually replaceable type and form part of SDS2. Should an individual detector deteriorate or fail in-service, it can be withdrawn from the detector assembly into a special shielded flask, and a replacement can then be inserted. Since the assembly pressure boundary will have been broken, the flux detector assembly must then be purged with helium in situ through fittings, and then be resealed (section 4.1.2.2.3).</p> <p>Between 5-15% of full power, self-powered in-core flux detector measurements are phased in while ion chamber measurements are phased out because the ion chambers do not provide the necessary spatial flux information. Inconel detectors are provided for SDS1, and platinum clad Inconel</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Guidance</p> <p>Reactivity control</p> <p>The reactivity control should ensure that:</p> <ul style="list-style-type: none"> <li>the acceptable fuel design limits are not exceeded as a result of a wide range of AOOs</li> <li>no single malfunction of the reactivity control function can cause a violation of the acceptable fuel design limits</li> </ul> <p>The nuclear design reactivity control requirements and control provisions should:</p> <ul style="list-style-type: none"> <li>compensate for long-term reactivity changes of the core; this includes reactivity changes due to depletion of the fissile material in the fuel, depletion of burnable poison in some of the fuel rods (where applicable), and buildup of fission products and transuranic isotopes</li> <li>compensate for the reactivity change caused by changing the temperature of the reactor from the zero-power hot condition to the</li> </ul>	<p>detectors are provided for the reactor regulating system and SDS2. These detectors are characterized by sensitivity to both neutron and gamma fluxes. The platinum clad Inconel detectors have a prompt signal component of about 89%. The Inconel detectors have a prompt component of about 104%. Vanadium detectors have been disconnected from flux mapping but remain in-core. Vanadium detectors are mainly neutron sensitive but have a slow response to flux Changes (section 7.1.2.3).</p> <p>The automatic computer controlled regulating system maintains flux shape control in the core by adjusting the water level in the 14 light water filled individual zone control units. In responding to AOOs there are two types of scenarios that must be considered, those involving flux changes and those involving process parameters other than flux. The detectors described above control the flux levels. When the flux exceeds the predetermined normal level, the zones respond by filling to add negative reactivity. If the power continues to rise to the SETBACK setpoint, then liquid zones will further fill and, if necessary, the control absorbers drive into the core adding more negative reactivity. The setback routine is part of the reactor-regulating program, and monitors a number of inputs indicating the status of all setback parameters that are summarized in Table 7-1 of Part 2 of the Safety Report. All setback logic operations are performed by the control computers. The setback routine is part of the reactor control program, and monitors a number of inputs indicating the status of all setback parameters which are summarized in Table 7-1. If a parameter is out of limits and demand power setpoint exceeds the setback endpoint, demand power is ramped down at a suitable rate until either the condition clears or the endpoint is reached. Each setback</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>cold shutdown condition</p> <ul style="list-style-type: none"> <li>compensate for the reactivity effects caused by changing the reactor power level from full power to zero power</li> <li>assure reactivity management during the fuelling cycle, and intermediate times during the fuel cycle</li> <li>compensate for the effects on the power distribution and stability of the high cross-section neutron capture of the xenon-135</li> <li>cover uncertainties associated with the control rods, including: <ul style="list-style-type: none"> <li>manufacturing tolerances</li> <li>methods errors</li> <li>operation other than planned</li> <li>control element absorber depletion</li> <li>measurement uncertainty in shutdown margin demonstration</li> </ul> </li> </ul> <p>Reactivity devices configurations and reactivity worth</p> <p>The nuclear design should establish the following</p>	<p>parameter may have a unique setback rate and endpoint. A test facility is provided to simulate high moderator temperature conditions to test the setback routine at the software level (section 7.2.2.3.5 of Part 2 of the Safety Report). The STEPBACK routine monitors a number of parameters, summarized in Table 7-2 of Part 2 of the Safety Report, which indicate plant conditions requiring a reduction in reactor power much faster than the zone controllers can produce. If a parameter is out of limits, the program opens all four control absorber clutch contacts. If the second computer also opens its control absorber clutch contacts, the clutches will be de-energized, which will cause the absorbers to drop into the core. As the absorbers are dropping, the stepback routine continues monitoring the out-of-limits parameter as well as the extrapolated reactor power, and recloses the clutch contacts when the condition clears or extrapolated reactor power is less than the endpoint. This may result in a partial absorber drop. However, most stepback conditions will cause the absorbers to be fully inserted. There is a test facility to check the reliability of the stepback function. The facility enables the operator to simulate the computer inputs for some stepback parameters. Opening of the clutch contacts is indicated by light emitting diodes. The stepback function is tested from the computer inputs through the stepback routine to the clutch contacts. The absorbers are not actually dropped since each computer is tested separately (section 7.2.2.3.6 of Part 2 of the Safety Report).</p> <p>The list of SETBACK and STEPBACK parameters are listed in Table 7-1 and Table 7-2 of Section 7 of Part 2 of the Safety Report.</p> <p>A wide range of AOOs is covered by the control system as</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>for reactivity device configurations, including (where applicable) control rod patterns, and reactivity worth for:</p> <ul style="list-style-type: none"> <li>reactivity devices configurations expected throughout a fuel reload cycle, power manoeuvring, and load-following (where applicable), including operation of single rods, or of groups or banks of rods, rod withdrawal order, and insertion limits, as a function of power and core life</li> <li>predicted reactivity devices' worth and reactivity insertion rates. It should be reasonably bounded to values that may occur in the reactor. Note: These values are typically used in the safety analysis, and judgments as to the adequacy of the uncertainty allowances are made in the review of the safety analysis</li> <li>allowable deviations from the patterns indicated above, such as for misaligned rods, stuck rods, or rod positions used for spatial power shaping</li> <li>maximum worth of individual rods or banks as a function of position for power and lifecycle conditions appropriate to rod withdrawal, rod ejection (or drop) accidents and other conceivable failures of reactivity control components leading to positive reactivity insertions</li> </ul>	<p>required under these expectations. The control system in Bruce B was designed to cover those events as shown in Table 7-2. For the remainder of the AOOs, the protection is provided by the two shutdown systems as described earlier.</p> <p>The speed and depth of the shutdown systems are greater than that of either the SETBACK or STEPBACK so adequate protection is provided. As presented of the Safety Report 7.2.2.2.2 of Part 2 of the Safety Report In the high power range, above 15% full power, self-powered in-core detectors are used to provide accurate power information not available from the ion chambers. The response of the reactor regulating system ion chambers situated on top of the core is affected by flux tilts and by the concentration of poison in the moderator. The detectors are distributed in the core and can provide more accurate information on the bulk power level and its spatial distribution. The regulating system flux detectors are installed in 27 vertical detector assemblies mounted strategically in the core.</p> <p>Detailed design description of reactivity control mechanisms (i.e. zone control system; control absorbers and adjuster rods), is presented in Section 4.2.7 Part 2 of the Safety Report. The liquid Zone Control System is the primary means for regulating the reactor power level and the spatial distribution of power in the core. It is designed to perform two main functions: (1) to provide short-term reactivity control to maintain reactor power at demanded level during normal operation and (2) to control spatial power distributions by suppressing regional power transients associated with reactivity perturbations. The simultaneous adjustment of water level in all zone control compartments provides bulk reactivity control. The differential adjustment of the water</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>maximum rates of reactivity increase associated with reactivity device withdrawals and any other conceivable change in the configuration of reactivity devices, due to failures in the reactivity control system. It should also include experimental confirmation of rod worth, or other factors justifying the reactivity increase rates used in control rod accident analyses, as well as equipment, administrative procedures and alarms which may be employed to restrict potential rod worth</li> <li>trip (or scram) rundown reactivity, as a function of time after trip (scram) initiation and other pertinent parameters, including methods for calculating the rundown reactivity</li> <li>equipment, operating limits, and administrative procedures necessary to restrict potential rod worth or reactivity insertion rates</li> </ul>	<p>level in individual zone compartments is designed to control the spatial power distribution. The four Control Absorbers are used by the regulating system to initiate rapid power reductions and to provide reactivity override for the negative fuel temperature effect. The required reactivity worth of these control absorbers is determined mainly by the increase in reactivity associated with a decrease in power from 100% full power to zero power hot with fresh fuel conditions. For a given setback in power, the increase in reactivity is significant only at low fuel burn-ups but could be higher than the negative reactivity range provided by the zone control system. Since the control absorbers can be dropped in by gravity, they also can provide a much faster reduction of system reactivity than is possible with the zone control system. The reactivity load provided by the control absorbers will be used to augment the zone control absorber worth (section 4.2.7.2 of Part 2 of the Safety Report). Adjuster Rods are cobalt rods, which are normally fully inserted in the core. There are 24 adjuster units in Bruce B arranged in three axial rows of eight units. The central row is located along the axial mid-plane of the reactor and the two outer rows are located symmetrically at 0.8 m on either side of the central row. The adjusters are designed to perform two main functions: (1) When withdrawn from the core, the rods provide positive reactivity shim either for overriding xenon transients or for compensating the reactivity loss due to fuel burn-up in the event of fuelling machine unavailability. (2) In their normal, fully inserted positions, they provide both radial and axial flattening of the flux, thereby reducing the maximum bundle and channel powers at full power operation. (Section 4.2.7.3 of Part 2 of the Safety Report).</p> <p>The control system is designed to ensure that serious</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>process failures are limited to less than 1 in 3 years, in accordance with the Siting Guide to which the Bruce A and B reactors are licensed. The inherent characteristics of Bruce B are discussed in Sections 6.1 and 4.1.2.1 of Part 2 of the Safety Report. The combination of these characteristics and the effectiveness of the control system minimize the need for shutdown system actions.</p> <p>Historically, the original design of reactivity control devices has not taken into account the wear-out and the effects of radiation as required in this clause. The reactor simulation techniques take into account these effects as discussed in Safety Report.</p>	
8.2	<p>The design shall provide the reactor coolant system (RCS) and its associated components and auxiliary systems with sufficient margin to ensure that the appropriate design limits of the reactor coolant pressure boundary are not exceeded in operational states or DBAs.</p> <p>The design shall ensure that the operation of pressure relief devices will not lead to significant radioactive releases from the plant, even in DBAs. The RCS shall be fitted with isolation devices to limit any loss of radioactive coolant outside containment.</p> <p>The material used in the fabrication of the component parts shall be selected so as to</p>	<p>New requirements have been introduced in this clause - (1) the selection of the material used in the fabrication of the component parts to be selected as to minimize corrosion and (2) the design to take into account all conditions of the boundary material including DEC's.</p> <p>Loss of pressure control, both high and low, is analyzed in Section 3.5 of Appendix 3 Control Failures of the Bruce B Safety Report [NK29-SR-01320-00002, R005]. Pressure relief from the heat transport system is provided by two steam bleed valves and two steam relief valves on the pressurizer, two liquid relief valves on the heat transport system and one relief valves on the bleed condenser tube side. One relief valve on the heat transport feed line through the bleed condenser reflux tube side protects the tube bundle, and one relief valve on the discharge from the bleed cooler protects the purification system from over-pressurization. In the solid mode, the pressurizer steam relief valves provide overpressure protection of the isolated</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>minimize corrosion and activation of the material.</p> <p>Operating conditions in which components of the pressure boundary could exhibit brittle behaviour shall be avoided.</p> <p>The design shall take into account all conditions of the boundary material in normal operation (including maintenance and testing), AOOs, DBAs and DECAs, as well as expected end-of-life properties affected by aging mechanisms, the rate of deterioration, and the initial state of the components.</p> <p>The design of the moving components contained inside the reactor coolant pressure boundary, such as pump impellers and valve parts, shall minimize the likelihood of failure and associated consequential damage to other items of the reactor coolant system. This shall apply to operational states and DBAs, with allowance for deterioration that may occur in service.</p> <p>The design shall provide a system capable of detecting and monitoring leakage from the reactor coolant system.</p>	<p>pressurizer. Operation of the pressure relief devices from the heat transport system and its auxiliaries are such that the discharged coolant is collected in the bleed condenser and is not discharged to the atmosphere. In cases where the bleed condenser relief valves may lift, the discharge is into containment and this fact has been considered in the safety analysis. Per the Derived Design Requirements (section 6.2 of [NK29-DG-03650-006, Rev.4]) the general nuclear safety and design philosophy for extensions to Containment Atmosphere PHTS and Moderator system is to provide barriers having redundancy, reliability and performance capabilities with reflect the importance of the barrier in meeting the fundamental safety function "contain" requirement. A single barrier that is closed and is not significantly leaking is sufficient to ensure release limits within prescribed limits. However, to meet the general philosophy, dual isolation is usually provided in the design. Two noted exceptions to the dual isolation were reviewed in the design guide supplements are provided, with the rationale for below:</p> <p>(1) the D20 recovery system (line 33330-L11D6) which was exempt from the dual automatic isolation valve requirement, as noted in design guide supplement [NK29-DGS-29-03650, Rev.0]. The reason for acceptance is that valve MV3 is normally closed, fails closed and has limit switches which provide alarms in the control room when the valve is not closed.</p> <p>(2) the 3/8 inch vent lines (3433L11D3/8, and 3433L14D3/8) connect the PHT system to the D20 collection system and do not meet the containment isolation requirements since only one normally closed valve is provided on this line [NK29-DGS-29-03650 Rev.0]. The reason for acceptance is the</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Guidance</p> <p>The design should have adequate provisions with regards to RCS and reactor auxiliary systems. The design should meet design limits for the worst conditions encountered in normal operation, AOOs and DBAs, including pressurized thermal shock and water hammer loads. The RCS and reactor auxiliary systems should meet – or contribute to meeting – the following objectives:</p> <ul style="list-style-type: none"> <li>maintain sufficient reactor coolant inventory for core cooling both in and after all postulated initiating events considered in the design basis</li> <li>remove heat from the core after a failure of the reactor coolant pressure boundary, in order to limit fuel damage</li> <li>remove heat from the core in appropriate operational states, DBAs and DECAs with the reactor coolant pressure boundary intact</li> <li>transfer heat from other safety systems to the ultimate heat sink</li> </ul> <p>The design of each reactor auxiliary system should ensure that automatic action by the system cannot impair a safety function.</p>	<p>vent valves will not be opened unless the reactor is shutdown and depressurized, and leaked through the closed valve.</p> <p>For the Bruce B design, each material that forms a part of the reactor coolant pressure boundary has been chosen to be compatible with the expected service and environmental conditions at the location at which it is used (section 5.2.3 of Part 2 of the Safety Report).</p> <p>As described in section 5.2.3 of Part 2 of the Safety Report, each material, which forms a part of the reactor coolant pressure boundary, has been chosen to be compatible with the expected service and environmental conditions at the location where it is used. Table 5-6 in Part 2 of the Bruce B Safety Report, lists the materials used for the major components in the HT system. The cobalt content is given in the table, where the requirement is to be less than that specified in the applicable material specification. Low cobalt content is required to keep radiation doses as low as possible.</p> <p>The major materials exposed to the reactor coolant are zirconium alloys, 400 series steels, carbon steel, Inconel and Incoloy. Part 2, Subsection 5.3.3 of the Safety Report contains details on the zirconium alloy and 400 series steels. Carbon steel is used for the main circulation piping, feeders and headers. The coolant chemistry has been chosen to give acceptable low carbon steel corrosion rates. The use of carbon steel gives low cobalt and nickel concentrations in the coolant and so assists in the objective of minimizing the quantities of Co-58 and Co-60 in the HT system.</p> <p>Inconel-600 was chosen as the steam generator and preheater tubing as it was believed at that time to combine a</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design authority should demonstrate the adequacy of the following:</p> <ul style="list-style-type: none"> <li>• flow rate and pressure drops across major components</li> <li>• major thermalhydraulic parameters, such as operating pressure and temperature ranges</li> <li>• valve performance (flow, pressure drop, opening and closing times, stability, water-hammer)</li> <li>• pump performance (head, flow, two-phase flow, seal performance)</li> <li>• vibration of components and pipes</li> <li>• control of gas accumulation (in particular, prevention of combustible gas accumulation)</li> <li>• maximum allowable heat-up and cool-down rates</li> <li>• consideration of pressurized thermal shock due to operation (including inadvertent operation) of auxiliary systems</li> <li>• flow stability, including loop-to-loop stability and void-enthalpy oscillations (CANDU)</li> <li>• design of instrumentation taps</li> </ul>	<p>high corrosion resistance to pitting, cracking and localized attack with a low corrosion product release rate in both the HT and secondary side water. Industry experience has demonstrated that I600 steam generator tubes have better primary side resistance to attack than secondary side. Incoloy-800 was used for the pressurizer heaters.</p> <p>The design intent of the Bruce B Heat Transport System in regard to crack propagation is documented in Part 2 of the Safety Report as follows. Fracture Toughness of Heat Transport Circuit Components (Section 5.2.4) specifies that as a minimum, the materials in the HT circuit meet the fracture toughness requirements for Class 1 components on Section III of the ASME Code. As noted in section 5.2.4.3, austenitic stainless steels are not used as part of the reactor coolant pressure boundary. Wherever austenitic stainless steel is used, for example in the gland seal systems for the HT pumps, great emphasis is given to the need for protection against contaminants during fabrication, shipment, storage, construction, testing, and operation. There are four spacers (also called garter springs) located around each of the 480 pressure tubes of a reactor. They are intended to maintain an even gap between the hot pressure tubes and the much cooler calandria tubes. Fuel channel to calandria tube contact is prevented by garter spring location and repositioning (SLAR) operation to prevent formation of brittle hydride blisters in the fuel channel and is discussed in Section 5.3.4 of Part 2 of the Safety Report.</p> <p>In addition, operating states where conditions could lead to brittle failure are avoided, as witnessed by the limits on HT system temperature and pressure to protect pressure tube integrity. The Operational Safety Requirements for Bruce B</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The following provides a few examples of design expectations of the RCS and reactor auxiliary systems:</p> <p>Pressurizer</p> <p>For designs that include a pressurizer, the design authority should demonstrate the adequacy of the following:</p> <ul style="list-style-type: none"> <li>• volume and capability to accommodate load changes, and to accommodate secondary side transients without the need for pressure relief to the containment to the extent practicable</li> <li>• capability to withstand thermal shock, particularly in spray nozzles and connections to the main RCS circuit</li> <li>• control of pressure, such as via heaters, sprays, coolers or steam bleeding</li> </ul> <p>Primary pressure relief</p> <p>The design authority should demonstrate the adequacy of the following:</p>	<p>Heat Transport System [NK29-OSR-33000-00001, R000] present the safety limits for pressure, temperature and flow as well as surveillance requirements.</p> <p>As presented in Part 3 of the Safety Report, the reference submission F. Saunders to K. Lafrenière, "Bruce Power HTS Aging Management Program and Bruce B Aging Analysis", NK21-CORR-00531-06661/ NK29-CORR-00531-07867, December 15, 2008] contains the technical basis of the Bruce Power HTS Aging Management Program and the Bruce B safety analyses, with aged HTS conditions, for small break LOCA events. The safety analysis results extend support for Bruce B operation at reactor power of up to 93% FP to 8700 Effective Full Power Days (EFPD), which is projected to be reached by approximately March 31, 2014 for the lead unit. The analysis demonstrates dual parameter trip coverage and no onset of fuel sheath dryout for small break LOCA events at 93% FP and aged conditions of up to 8700 EFPD (i.e., approximately March 2014 for the lead unit, i.e., Unit 5). HTS aging does not have a significant impact on accident consequences or trip effectiveness following small break LOCAs. Enclosure 1 of NK21-CORR-00531-06661 / NK29-CORR-00531-07867, Letter F. Saunders to K. Lafrenière, "Bruce Power HTS Aging Management Program and Bruce B Aging Analysis, December 15, 2008] is the HTS Aging Technical Basis Document (TBD) which outlines the basis of the HTS Aging Management Program initiated to investigate the potential erosion of safety analysis margins to 8700 EFPD. The TBD systematically evaluated and identifies the impacted accidents and the path forward to manage the effects on safety analysis results. A summary of the technical basis of the HTS Aging Safety Margin Management Program</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>flow rate in single and two phase flow</li> <li>consideration of corrosion of valve surfaces</li> <li>provisions for ensuring that relief discharge does not lead to an unacceptable harsh environment inside containment</li> <li>relief valve stability</li> </ul> <p>Primary reactor coolant pumps</p> <p>For designs that use forced primary flow, the design authority should demonstrate the adequacy of the following:</p> <ul style="list-style-type: none"> <li>primary pump performance characteristics, including head and flow characteristics, flow coastdown rate, single and two-phase pump performance</li> <li>pump operating parameters (e.g., speed, flow, head)</li> <li>pump net positive suction head needed to avoid cavitation</li> <li>pump seal design and performance (including seal temperature limitations, if</li> </ul>	<p>is presented in section 3.6.1.2 to 3.6.1.5 of Part 3 of the Safety Report. As noted in Section 3.6.2.2 of Part 3 of the Safety Report, sensitivity analyses to assess the impact of HTS ageing effects on Electrical System Failures were performed for a single HT pump trip event at 8700 EFPD. The analysis demonstrated that fuel sheath dryout is precluded prior to onset of flow oscillations and that trip coverage at the aged conditions is the same as in the reference unaged analysis (Section 2.9.7 of Appendix 2). Therefore, HTS aging effects corresponding to 8700 EFPD (corresponding to approximately March 2014 for the lead unit) have no impact on trip coverage for this event. In addition, analysis of the main events impacted by ageing, are revised to reflect plant conditions applicable to the licence duration. The most recent ageing analyses to 2019 are documented in Letter F. Saunders to R. Lojk, Safety Analysis Submission in Support of Operation of Bruce A and Bruce B to 2019, NK21-CORR-00531-10943 / NK29-CORR-00531-11325, December 12, 2013.</p> <p>The operating conditions considered in the design of the HT main circuit header piping were identified and a summary listing can be found in Section 5.2.1.2 of Part 2 of the Safety Report. Temperatures, pressures and other parameters change from one location to another in the HT main circuit for each operating condition. Description of the operating conditions, including the design loading combinations and associated stress or deformation limits for a particular location in the HT main circuit, are given in the technical specification for the component closest to the location. The stress analysis of all systems and major components in the HT system meets the requirements of Section III of the ASME Code. The types of stress analysis employed are</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>applicable)</p> <ul style="list-style-type: none"> <li>vibration monitoring provisions</li> </ul> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>IAEA, NS-G-1.9, Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants Safety Guide, Vienna, 2004.</li> </ul>	<p>tailored to the particular requirements for each system and component, and are identified in the stress reports produced for Class 1 systems and components. Life Cycle Management Programs are in place to examine the HT system components for deterioration throughout the life of the plant. Periodic inspections of the HT system are done in accordance with the requirements of CSA N285.4, as set out in Clause 3.5.2 of that standard.</p> <p>The reactor coolant system and most auxiliaries are located within the pre-stressed concrete containment structure and the majority of the systems are within the normally dry reactor vault. Any leakage within this vault increases the dew point of the recirculating air and is detected. Special facilities are provided to collect leakage from flanged mechanical joints, valve stems and pump shaft glands. All valves below 5 cm (2 inches) are bellows-sealed. Grayloc couplings are used as mechanical joints on the feeder/endfitting connections and other piping below 5 cm (2 inches). The insulation cabinets are monitored to detect leakage, with leak location being by visual inspection. Additional details about heavy water leakage detection are presented in section 11.4.8 of Part 2 of the Safety Report. Special facilities are provided to detect moisture in the annulus gas system (online dew point monitors and moisture beetles) that may be attributed to a leak in a pressure tube. At higher leak rates, the beetles provide an alarm to the control room. The Annulus Gas System (AGS) is designed to provide a dry gas atmosphere in the annuli between the pressure tubes and calandria tubes. It was originally designed to operate as a stagnant pressurized system, with provision for periodic sampling (and future use as a recirculating system, if required). Manual sampling capability was provided in the original design to</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>allow the operator to monitor the integrity of the calandria tubes and pressure tubes, and to detect significant leakage from those components. The AGS was modified to operate in a continuous recirculation mode, and with online monitoring to improve its ability to quickly detect very small pressure tube leaks caused by delayed hydride cracks in rolled joints. It has been confirmed that recirculation in the Bruce B AGS improves the ability to detect very small leakage quickly with online dew point monitors (section 11.2.5.1 of Part 2 of the Safety Report).</p> <p>Reactor Coolant Boundary Leakage Detection system is discussed in Section 5.2.5, Annulus Gas System is described in Section 11.2.5 of Part 2 of the Safety Report.</p> <p>As discussed in previous sections, the original Bruce B design did not consider DEC's.</p> <p>In the area of strengthening defence-in-depth, Bruce Power is progressing the engineering of additional safety features to provide makeup water to the heat transport system for Bruce B. Table B2 in the Bruce Power Progress Report No. 8 on CNSC Fukushima Action Items provides the schedule for the heat transport makeup which indicates the scheduled installation for units 5 through 8 during targeted outages from Q1 2017 to Q3 2018 [NK29-CORR-00531-12979].</p>	
8.2.1	The components of the reactor coolant pressure boundary shall be designed, manufactured, and arranged in a manner that permits adequate inspections and tests of the boundary, support structures and components throughout the lifetime of the plant.	<p>The text in this clause is modified to include support structures and components in the first paragraph. This change is for clarification and does not impact the requirement.</p> <p>Bruce Power Pressure Boundary Quality Assurance Program [BP-PROG-00.04, R022, May 27, 2015] describes the</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
	The design shall also facilitate surveillance in order to determine the metallurgical conditions of materials for which metallurgical changes are anticipated.	<p>pressure boundary quality assurance program for Bruce Power Inc. for nuclear pressure boundary, and conventional pressure boundary activities. The May 2015 update of BP-PROG-00.04 provided "updates to various sections of this PB QA Program Manual to align it with requirements of CSA N285.0-12 - Update 2."</p> <p>The N285.0 standard specifies the technical requirements for the design, procurement, fabrication, installation, modification, repair, replacement, testing, examination, and inspection of, and other work related to, pressure-retaining systems, components, and supports over the service life of a CANDU nuclear power plant. Bruce Power carries out periodic inspections of pressure retaining systems, components and supports as required by N285.4 and in accordance with licence condition 6.1 of LCH. Full compliance with the June 2011 update of N285.4 is targeted by 2017.</p> <p>Bruce Periodic Inspection Plan for units 5 through 8 [i.e., NK29-PIP-03641.2-00001 to NK29-PIP-03641.2-00004] identifies the systems, components, and areas that require periodic inspections; specifies the inspection methods and the inspection frequency. The updated inspection plan for containment boundary components at Bruce B nuclear generating station (as required by PROL 18.00/2020, Licence Condition 6.1) is outlined in the Bruce B Periodic Inspection Plan for Unit 0 and Units 5 to 8 Containment Components [NK29-PIP-03642-00001, Rev.2]. Inspection frequency as described in Section 13.0, notes that "all non-VBO periodic inspections will be performed within the required 10-year inspection cycle".</p> <p>In order to provide access for maintenance and inspection,</p>	




 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>residual radiation fields are controlled to permit personnel access for maintenance and inspection of HT system components. Access space is provided between components and between the inside surface of the insulated cabinets and the surface of components. Access doors, platforms, ladders, etc., are provided where required for maintenance and inspection. Some HT system components external to the insulated cabinets are subject to periodic inspection. Access to these components is also provided. Insulation, where provided, is designed for removal.</p> <p>The HT system and fuel channel in-service inspection programs address the requirements for metallurgical changes of materials.</p>	
8.2.2	<p>Taking volumetric changes and leakage into account, the design shall provide control of coolant inventory and pressure so as to ensure that specified design limits are not exceeded in operational states. This requirement shall extend to the provision of adequate capacity (flow rate and storage volumes) in the systems performing this function.</p> <p>The inventory in the RCS and its associated systems shall be sufficient to support cool down from hot operating conditions to zero-power cold conditions without the need for transfer from any other systems.</p> <p>If necessary for operational states and DBAs, the</p>	<p>The new wording "operational states" replaces "normal operation" meaning that now the requirement is extended to AOOs as well. This change represents a new requirement.</p> <p>As described in Part 2, Section 5.1 of the Safety Report, the HT system, which carries the heat generated in the reactor core to the steam generators, is a pressurized, closed heavy water loop. The feed, bleed and relief system (section 5.1.5 of Part 2 of the Safety Report) is designed primarily to provide a means of pressure and inventory control for this closed loop as well as to provide adequate overpressure protection. The feed, bleed and relief system consists of a pressurizer, a bleed condenser, a bleed cooler and a feed and bleed circuit. The system flowsheet is illustrated in Figure 5-11 and the system design data are tabulated in Table 5-4 of the same chapter in Part 2 of the Safety Report.</p> <p>The combination of the reactor coolant system and its associated systems, i.e., pressurizer, feed and bleed system</p>	IC



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>design shall provide means of monitoring reactor core coolant inventory.</p> <p>Means of estimating the core coolant inventory in DEC's shall be provided, to the extent practicable.</p> <p>Guidance</p> <p>The design should take into account the provision of adequate capacity, volumetric changes, leakage, flow rate and storage volumes in the systems performing this function.</p>	<p>and D2O storage system, can accommodate this requirement. The reactor coolant and pressurizer systems alone cannot cope with a cold shutdown on any CANDU. Normally the pressurizer controls the pressure in the HT circuit. When the pressurizer is isolated, the system pressure is controlled by the feed and bleed circuit. The feed and bleed circuit controls HT system heavy water inventory. The feed and bleed circuit is designed to handle the shrink and swell rates which take place during system heatup and cooldown, and to provide HT pressure control for operation with the reactor at low power and the pressurizer isolated. The changing volume of the HT system coolant during heatup and cooldown is accommodated by the feed and bleed system, which provides pressure control for operation with the pressurizer isolated. The HT bleed-flow flows through the bleed valves, to the bleed condenser, bleed cooler and the purification circuit, and on to the feed pumps for injection back into the HT system or into the storage tank. The storage system was designed to handle and store the entire D2O swell from the HT system from cold to zero power hot. The D2O storage system is described in section 5.1.5 of Part 2 of the Safety Report.</p> <p>A list of essential reactor control/monitoring, lighting and motorized valve loads which required electrical power in the absence of all installed station AC power supplies is documented in [0B/5/6/7/8 Instrument Monitoring and Control Equipment Power Requirements During Extended Loss of AC Power, NK29-EPR-54900-0001, R000, January 11, 2013]. The critical reactor control instrumentation and monitoring loads, and priority to supply power during station blackout is outlined for Units 0/5/6/7/8 including Unit 0 SCA, EFADS and Vacuum Building. The rating of loads is listed in</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		kw (kilowatts). The last column of each table lists selected loads and the percentage of each portable generator loading. During DEC's emergency power will be provided to critical monitoring instrumentation, including HTS header level, thereby allowing HTS inventory to be monitored. The Design Guide Extended Loss of AC Power for all units [B-DG-03654-00001, Rev. 000] provides beyond design basis requirements for portable SSCs and their connection points to permanent plant SSCs intended to prevent further progression of BDBAs into severe accidents.	
8.2.3	The design shall provide for adequate monitoring and removal of impurities and radioactive substances from the reactor coolant, including activated corrosion products and fission products leaking from the fuel. The safety limit for activity in the reactor coolant shall be defined.	<p>A new requirement for defining a safety limit on activity in reactor coolant is included in this clause.</p> <p>As discussed in Part 2, Section 5.1.6 of the Safety Report, the function of the Bruce B purification system is to remove suspended and dissolved corrosion products from the HT fluid to keep the activity from this source to a minimum. A further function is maintenance of the pH as part of the overall system chemistry control. The purification system continuously removes both particulate and dissolved ionized materials from the coolant by a combination of low temperature filtration and ion exchange. The size of this system is determined by the need to maintain the total quantity of radioiodine-131 in the HT system below allowable limits and the need for removal in the purification system to compete effectively with the re-deposition of radioactive species. This system is designed in accordance with the ASME Code, Section III, Class 3. There are two banks of filters and ion exchange units (two filters and four ion exchange units per bank) for purification of the HT fluid. The system is designed for a maximum flow of 37.9 L/s (500 lgpm) from the bleed circuit at a temperature of 46°C (115°F).</p>	C



Rev Date: September 20, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>This circuit operates at low pressure, maximum of 1.31 MPa(g) (190 psig), and is located behind shielding in the reactor auxiliary bay. A spring loaded relief valve upstream of the system, relieving directly to the D2O storage tank, provides the necessary operating overpressure protection. Purification outlet flow is to the feed pump suction and heavy water storage tank. Lithium is added to the HT coolant for pH control and therefore lithium ion exchange resins are used. There is a deuterium/hydrogen addition station to limit the amount of oxygen in the HT system fluid resulting from radiolysis of heavy water. The filter vessels, including the cartridges, are disposable. The ion exchange columns are the same as those in the moderator system.</p> <p>HTS coolant activity limits are defined on radioactive Iodine-131 concentration on the HTS coolant and radioactive tritium concentration in the HTS coolant. The safety limits for HTS coolant activity are provided in Section 5.0 HTS Coolant Activity of Bruce NGS B Heat Transport System OSRs [NK29-OSR-33000-00001, R000].</p> <p>The Safety Analysis Limit for steady state iodine content is defined to ensure that radiological dose from postulated accidents (resulting in release of coolant from the HTS) will not exceed applicable regulatory limits. The applicable analysis that establishes the limit for I-131 concentration is the assessment of consequential boiler and preheater tube leaks arising from transient loads following design basis accidents or upset conditions (Section 6.9, Appendix 6 (Heat Transport Auxiliary System Pipe Breaks Outside Containment)).</p> <p>The steady-state I-131 content reflects the estimated number of typical small fuel cladding defects that exist in the reactor</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>core. These defected fuel elements release additional radioactivity into the coolant following a significant power change (e.g., during a shutdown) and/or coolant pressure change (e.g., during a break-induced depressurization of the HTS) (section 5.1.1 of HTS OSRs). Steady-state shutdown limits for I-131 inventory in the heat transport coolant are defined in Appendix 6.9.9.1 of Part 3 of the Safety Report.</p> <p>As described in section 5.1.1 of HTS OSRs, the additional transient release, which is proportional to the number of defected fuel elements, is commonly referred to as an iodine spike. Safety analyses evaluate the radiological consequences assuming that the iodine spike has occurred as a consequence of the accident and that the Purification System (i.e., an ion-exchange process system) is not operable to suppress the I-131 content after the accident (i.e., purification system flow is assumed to be zero when the reactor is tripped, consistent with post-LOCA isolation requirements). Section 6.9.9.1 of Appendix 6 (HT Auxiliary System Pipe Breaks Outside Containment) of Part 3 of the Safety Report sets the maximum limit on the total I-131 content in the HTS at 8 Ci for a purification flow rate of 10 kg/s. The consequential leak assessment identifies the limiting accident scenario as a boiler tube leak caused by a 100% rupture downstream of the last check valve in the Emergency Water Supply System (Section 6.9.12.3.2, Appendix 6 of Part 3 of the Safety Report). The predicted dose for this accident is limited by the individual thyroid dose. The corresponding Safety Analysis Limits on I-131 concentration (the measurable parameter) are given in Figure 5.1-1 and Table 5.1-2 of Heat Transport System OSRs as a function of purification flow rate during steady state operation of the HTS. Iodine I-131 limits decrease with increasing</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>purification flow. This is because an increasing purification flow rate reduces the steady state iodine levels for a given amount of defected fuel in the core, the amount of iodine inventory in the gap (which is available for post-shutdown release) is unchanged by purification flow. Thus, in order to limit the transient iodine release after shut down, it is necessary to recognize the relationship between steady state iodine levels and pre-accident purification flow rate. The relationship that defines the Safety Analysis Limit in effect maintains the same extent of fuel defects in the reactor core and thus yields the same transient iodine release into the coolant after a design basis accident. For the purposes of applying these limits, steady state operation is represented as a period of 24 hours without a power change in excess of 20 percent FP. A power change can induce the spike in the iodine concentration that takes approximately one day to dissipate by a normal flow through the Purification System. Applying the steady state limits during transient conditions would therefore be overly conservative.</p> <p>Tritium concentration in the HTS coolant builds up gradually over time by irradiation of D2O. Tritium is not removed in the Purification System. It is periodically removed by substituting irradiated (and tritiated) D2O with clean (or less tritiated) D2O. Its concentration following an accident is the same as that during steady-state operation. The maximum Safety Analysis Limit on tritium concentration in the HTS coolant of 2 Ci/kg (74 GBq/kg) is set in Section 6.9.9.1 of Appendix 6 of Part 3 of the Safety Report to minimize concerns regarding public doses from design basis accidents with consequential boiler and preheater tube leaks. This limit applies at all times (i.e., during steady state operation or during transients) whenever the potential for a break in the HTS exists. The</p>	


 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		limit on Tritium concentration is not affected by reactor power or HTS pressure. Table 5.1-1 of Heat Transport System OSRs presents the safety analysis limits for HTS coolant activity (section 5.1.2 of HTS OSRs).	
8.2.4	<p>The design shall provide a means (i.e., backup) of removing residual heat from the reactor for all conditions of the RCS. The backup shall be independent of the configuration in use.</p> <p>The means of removing residual heat shall meet reliability requirements on the assumptions of a single failure and the loss of offsite power, by incorporating suitable redundancy, diversity, and independence. Interconnections and isolation capabilities shall have a degree of reliability that is commensurate with system design requirements.</p> <p>Heat removal shall be at a rate that prevents the specified design limits of the fuel and the reactor coolant pressure boundary from being exceeded.</p> <p>If a residual heat removal system is required when the RCS is hot and pressurized, the design shall ensure that it can be initiated at the normal operating conditions of the RCS.</p>	<p>There are no changes in this requirement.</p> <p>The various methods of cooling the reactors are described in detail in Section 5 of Part 2 of the Safety Report. The preferred mode of cooling is with the reactor at full power, producing the base load electricity for which it is designed. In this mode, heat is removed by the power producing systems, specifically the steam generators and turbines, and the associated feedwater and steam handling systems. When the reactor is shut down for maintenance or to repair equipment, shutdown cooling systems remove residual heat (or decay heat), as described in Section 5. Circulation of the reactor HT fluid is maintained at all times during reactor operation, shutdown and maintenance. In addition to the normal heat removal system, two further systems are provided for removing reactor shutdown heat, the shutdown cooling system and the maintenance cooling system (section 5.1.4). The maintenance cooling system is also designed to permit the draining of steam generators and pumps. The shutdown cooling system is capable of cooling the HT system from the zero power hot temperature (260 °C) under emergency conditions (section 5.1.4.1 of Part 2 of the Safety Report). The maintenance cooling system is designed to withstand full HT system temperature and pressure of 318°C (605°F) and 11.3 MPa(g) (1635 psig), and is classified as a Class 1 system in accordance with Section III of the ASME Code. The system is provided with Class III power (section 5.1.4.2 of Part 2 of the Safety Report). The design data for shutdown</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>cooling system and maintenance cooling system are presented in Part 2 of the Safety Report, Table 5-1 and Table 5-2 respectively.</p> <p>During normal cooldown from the zero power hot state with Class IV power available, the main HT pumps circulate the coolant and heat is rejected through the Condenser Steam Discharge Valves (CSDVs) or the Atmospheric Steam Discharge Valves (ASDVs) to cool the HT system to 177°C (350°F). Further cooldown with the HT system partially depressurized is then achieved using the shutdown cooling system (section 5.1.4 of Part 2 of the Safety Report).</p> <p>The Condenser Steam Discharge Valves (CSDVs) provide a means for fast and continuous rejection of up to 68 percent of the turbine steam flow, thus allowing the reactor to continue producing power at a level that will not cause a shutdown. This mode of operation prevents xenon poison out of the reactor (poison prevent operation). During normal operation, the CSDVs are closed. During poison prevent operation they are partially open, with the degree of opening based on the power mismatch between poison prevent level and actual turbine steam consumption. The valves can only be opened when the external condenser protective system is activated. If the valves are tripped by the protective system, a manual reset is required before they can be reopened. On a turbine trip and when reactor power is above a certain level, a signal is applied to open the CSDVs at maximum speed. They revert to their normal pressure control mode after they have opened fully. Provision is also made to allow the operator to open and close these valves manually from the control computer keyboard (section 9.6.2 of Part 2 of the Safety Report).</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
		<p>The Condenser Steam Discharge Valves (CSDVs) are part of the steam reject/bypass system. They permit the continued operation of the nuclear steam supply system for an indefinite period in the event of a grid system or turbine generator fault. By fully or partially bypassing the turbines, both, reactor poison out and loss of demineralized water is avoided. The system is designed to accept 75% of rated full power steam flow. The condenser steam discharge valves are under the control of the steam generator pressure control program in both control modes. They are normally biased closed (section 7.2.1.3.2 of Part 2 of the Safety Report).</p> <p>The Atmospheric Steam Discharge Valves (ASDVs) are also part of the steam relief system. They have a capacity equivalent to approximately 11% of rated full power steam flow. This capacity, together with that of the CSDVs, is sufficient to make it unnecessary to open the steam generator safety valves following most turbine trips. They also provide a means of controlling steam pressure when the condenser steam discharge valves are unavailable due to poor condenser vacuum. The atmospheric steam discharge valves are controlled by the steam generator pressure control program in both control modes. They are normally closed (section 7.2.1.3.3 of Part 2 of the Safety Report).</p> <p>A review of the same clause in RD-337 indicated that the Bruce B design meets this requirement [NK21-CORR-00531-11005 / NK29-CORR-00531-11397]. Bruce B design provides the seismically qualified Emergency Water System (EWS) to establish an adequate heat sink for decay heat removal when the normal sources of water for this purpose are not available. The EWS is designed to provide an alternative source of water for the unlikely event that all</p>	


	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>sources of feedwater to the steam generators fail, or that service water to the ECI heat exchangers, vault coolers or primary and secondary irradiated fuel bay cooling heat exchangers fail. Section 6.7.1 of Part 2 of the Bruce B Safety Report [NK29-SR-01320-0001, Rev.5].</p> <p>.</p> <p>Bruce Power will develop technical basis for the interpretation and use of single failure criterion in the Safety Analysis. This will be considered part of the overall strategy for phased implementation of RD-310 requirements. Bruce Power is implementing a Safety Report Improvement Program starting in 2014 including annual status and progress updates to the CNSC staff. This is documented in NK21-CORR-00531-10774 and NK21-CORR-00531-11155, letter from F. Saunders to R. Lojk, Action Item 090739: Safety Report Improvement Plan for Bruce A and Bruce B.</p>	
8.3.1	<p>The steam piping up to and including the turbine generator governor valves and, where applicable, the steam generators shall allow sufficient margin to ensure that the appropriate design limits of the pressure boundary are not exceeded in operational states and DBAs. This provision shall take into account the operation of control and safety systems.</p> <p>The main steam isolation valves (MSIVs) shall be installed in each of the steam lines leading to the turbine, and located as close as practicable to the containment structure.</p>	<p>The changes introduced in this clause are editorial in nature and do not impact the intent of the requirement.</p> <p>As described in section 5.1.2.3 of Part 2 of the Safety Report, there are eight motorized Main Steam Isolating Valves (MSIVs), one in each steam discharge pipe, downstream of the steam generator nozzles. The MSIVs are designed and installed in accordance with ASME B31.1. As indicated in Part 3 of the Safety Report, the MSIVs are not required to mitigate the consequences of a steam line break. A comprehensive system of monitoring, inspection, and testing has been established to ensure ongoing integrity of mechanical components and reliability of equipment.</p> <p>In addition, each steam generator has two instrumented</p>	IC


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Where MSIVs are credited with preventing steam flow into containment, they shall be capable of closing under the conditions for which they are credited.</p> <p>Where MSIVs provide a containment barrier, they shall meet the containment requirements that apply to those conditions for which they are credited.</p> <p>The MSIVs shall be inspectable and testable.</p> <p>Steam lines up to and including the first isolation valve and, where applicable, steam generators shall be qualified to withstand a DBE.</p>	<p>Safety Relief Valves (SRVs) for overpressure protection or remote operation for rapid boiler cooldown. These instrumented safety relief valves are spring loaded with a power assisted mode. The power assisted mode does not interfere with the spring operated function for overpressure protection. There are also four globe type, power operated Atmospheric Steam Discharge Valves (ASDVs) near the steam drums to provide fine control of steam generator pressure during manoeuvring and to avoid frequent operation of the SRVs. Failures associated with the steam supply system have been analyzed and documented in Appendix 7 (Feedwater and Steam Supply System Failures) of Part 3 of the Safety Report. The analysis considers the full range of break sizes and locations in the Feedwater (FW) and steam supply systems.</p> <p>Break locations covered in the accident analysis documented in Appendix 7, Part 3 of the Safety Analysis, include those that affect all SGs equally (loss of all FW and steam balance header (SBH) breaks) and one SG quadrant preferentially (loss of FW to one SG quadrant and main steam line (MSL) or nozzle breaks). Each failure is considered over the full range of initial reactor power up to 103 percent full power (FP). In performing the analysis, consideration has been given to the potential of a major steam release within the powerhouse and its environmental effect on equipment survivability and operation. A number of essential systems with equipment located in the powerhouse have been environmentally qualified or protected from an adverse (high pressure, temperature and humidity) environment to ensure their continued operating capability under the condition of a steam-filled powerhouse. Of specific relevance to the present analysis, the following systems are environmentally qualified</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>or protected:</p> <ol style="list-style-type: none"> <li>shutdown system two (SDS2) is qualified to provide shutdown capability, including long-term monitoring,</li> <li>the emergency coolant injection (ECI) system is qualified to provide a manually initiated coolant supply to the HT system,</li> <li>steam generator cooldown via remote manual initiation of the SG SRVs, and 4. emergency water supply (EWS) system (see Section 7.1.2.4) is qualified to provide a means of decay heat removal.</li> </ol> <p>The effects of unsafe failures of systems which are neither environmentally qualified nor protected from the powerhouse steam environment are considered individually as part of the scope of the analysis. The system failures considered include the loss of Class IV power, failure of boiler level and pressure control, or setback and stepback actions, etc. (section 7.1.1 of Appendix 7 of Part 3 of the Safety Report).</p> <p>Section 7.4.2.2 and section 7.4.3.2 of Appendix 7 present the accident analysis of Main Steam Line Breaks. A detailed description of the analysis methodology, the Safety Systems initiation and the effect of control system actions are documented in section 7.6. It is noted that the reactor regulating system protective actions have not been credited in the accident analysis, although in reality a full reactor stepback is expected on low SG level in the affected bank (section 7.6.1. 2.3)</p> <p>The approach to dealing with a steam environment in the powerhouse was to install a powerhouse emergency ventilation system (PEVS) and to ensure that critical</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>equipment is environmentally qualified.</p> <p>As described in Part 2, Section 6.7.4 of the Safety Report, the Bruce B Powerhouse Emergency Venting System (PEVS) is a standby safety system designed to mitigate the consequence following a secondary side steam piping or feedwater piping failure. The fundamental function of the overall system is to restrict powerhouse over-pressure and mitigating the consequence of high energy secondary pipe breaks to support general Group 2 and specific Group 1 capability. The system utilizes the natural buoyancy of the steam/hot air inside the powerhouse to induce a chimney effect and draw cold air at lower elevations and exhaust the hot mixture at higher elevations. Two out of three pressure sensors in any unit will open all the panels to protect against excessive pressure in the powerhouse. The panels will also open upon loss of Class I power. The panels are closed manually. The system also provides protection against excessive powerhouse room temperature. Pressure and temperature actuation set points support the room values as set out in the Bruce B Room Conditions Manual B-STQ-03651-10001.</p> <p>Similarly, 6 (six) vertical centrally pivoted instrumented panels have been installed in the Main Control Room to prevent steam ingress.</p> <p>Appendix E, of the Bruce Power Seismic Qualification Standard [DPT-PDE-00017, Rev.005] identifies the seismically qualified systems at Bruce B. Steam and feedwater lines are seismically qualified to DBE, with a qualification category (A) meaning heat rejection capability of the steam generators must be maintained. For steam lines, qualification applies from the steam generator nozzles to the</p>	

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		first restraint. For feedwater lines, qualification applies to the first check valve upstream of the steam generators and preheaters, respectively (Appendix E of [DPT-PDE-00017, Rev.005]).	
8.3.2	<p>All piping and vessels shall be typically separated from electrical and control systems, to the extent practicable.</p> <p>The auxiliary feedwater, steam generator pressure control, and other auxiliary systems, shall prevent the escalation of AOOs to DBAs or DEC's.</p>	<p>The changes to the text in this clause are minor and do not impact the requirements.</p> <p>The Design Guide, Location and Separation Requirements for Safety Related Systems [NK29-DG-29-03650-5, R003, November 20, 1985] establishes minimum design requirements for safety related systems to meet the separation philosophy. The list of safety related systems for Bruce B is presented in Appendix 1 of Design Guide, Purpose and Application of Safety Systems Design Guides for Bruce G.S. 'B' [NK29-DG-29-03650-1, R003, November 20, 1985].</p> <p>The design guide [NK29-DG-03650-003] was used for the environmental qualification of the original Bruce B design. As noted in Section 9.1, the effects of humidity are considered. "Since the effects of humidity are considerably more severe at elevated temperatures, the qualification shall consider both the temperatures and humidity requirements of the environment where the component is located". Additionally, it notes that components shall be selected and located to account for "Immersion or Water Spray/Flooding - components required to function following events involving flooding shall be located above the estimated flooding levels as it is often difficult or impossible to demonstrate submerged components will function, if the component is unprotected and located in a position where it could be subjected to flooding, sprinkler system sprays, water, or jet streams</p>	Gap

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>resulting from postulated pipe ruptures and the component is required to be functional under these circumstances then EQ for the applicable situation shall be considered. Less significant effects such as those associated with the water leaks or condensation shall also be considered".</p> <p>Safety Factor 3: Equipment Qualification examines the effectiveness of the Equipment Qualification Program.</p> <p>A systematic review of the design of auxiliary feedwater, steam generator pressure control, and other auxiliary systems has not been performed to demonstrate that they would prevent the escalation of AOOs to accident conditions. Therefore, this is assessed as a gap (Gap). The topic of AOOs is addressed in detail under Safety Factor 5.</p>	
8.3.3	<p>The design shall provide over-speed protection systems for the turbine generators to minimize the probability of turbine disk failure leading to generation of missiles.</p> <p>The design shall be such as to minimize the potential for any missiles from a turbine break-up striking the containment, or striking other SSCs important to safety.</p> <p>Guidance</p> <p>The design of turbine generators should meet the following expectations:</p>	<p>The second paragraph is modified to clarify the intention of the requirement.</p> <p>The overspeed protection is a defence against a turbine disc break-up. Break-ups have occurred on several nuclear and conventional power plants in the past with very serious results, including loss of life, missiles damage and fires. A reliability target of a probability of failure from all causes is lower than 1E-4/demand is that generally met within the industry. The Safety Reports do not contain the detailed analyses but Design Manuals from the supplier quotes this kind of reliability. CNSC staff has reviewed these reports.</p> <p>The clause essentially requires that the axes of the turbine generators be at right angles to the reactor buildings. The axes of the Bruce A and B turbines are oriented in parallel with the reactor buildings.</p> <p>For Bruce B, section 2.5.3 of Part 2 of the Safety Report</p>	IC




Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>a turbine control and over-speed protection system should control turbine action under all normal or abnormal operating conditions, and should ensure that a full load turbine trip will not cause the turbine to over-speed beyond acceptable limits</li> <li>the over-speed protection system should meet the single-failure criterion, and should be testable when the turbine is in operation</li> <li>the turbine main steam stop and control valves, and the reheat steam stop and intercept valves should protect the turbine from exceeding set speeds, and should protect the reactor system from abnormal surges</li> <li>the turbine generator set should have the capability to permit periodic testing of components important to safety while the unit is operating at rated load</li> <li>an in-service inspection and testing program for main steam and reheat valves should be established</li> <li>the arrangement of connection joints between the low-pressure turbine exhaust and the main condenser should prevent adverse effects on any safety-related equipment in the turbine room in the event of a rupture (it is preferable not to locate safety-related equipment in the turbine room)</li> </ul>	<p>indicates that features incorporated into the design provide an adequate level of protection against any credible turbine generator missile. These features include:</p> <ol style="list-style-type: none"> <li>Separation of the 600 V Class II switchgear, such that a single missile cannot disable both halves of the system.</li> <li>Reinforced concrete barriers, such that a turbine generator missile cannot strike the HT pump motors.</li> <li>Adoption of separation measures [NK29-DG-03650-005] such that a single missile cannot disable sufficient equipment to prevent safe shutdown, monitoring, or decay heat removal.</li> </ol> <p>The impact of turbine generated missiles on non-accidental plant was assessed and documented in the External Hazards Assessment B-03611.7 P NSAS (E7) R003 [K-449958-REPT-0007, R03, July 24, 2014]. The Bruce B powerhouse is aligned along a SW-NE axis. Any turbine missile would therefore take an approximate NW-SE trajectory, neither being toward Bruce A. Bruce A powerhouse alignment would be consistent with turbine missiles moving in the direction of Bruce B. The conclusion is that turbine generated missiles originating at either Bruce station are not a credible threat to the other station.</p> <p>Table 110 of B-03611.7 P NSAS (E7) R003 shows that highest probability of significant damage is the probability of a strike on electrical equipment (<math>3.0 \times 10^{-5}</math>) followed by a strike on the PHT pump/motors and/or the reactivity mechanism deck area (RMDA) in the reactor building with a probability of <math>2.6 \times 10^{-6}</math> per turbine year. The Bruce B Safety Report [NK29-SR-01320-00001, Rev. 005] confirms that there is an</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>the design should consider the potential impacts of any missiles which may result from a turbine break-up striking the SSCs important to safety; the selection of the axes orientation of the turbine generator should minimize such potential</li> </ul> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>U.S. NRC, NUREG-0800, Chapter 10, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition – Steam and Power Conversion System, Washington, D.C., 2007.</li> </ul>	<p>adequate level of protection against any credible turbine generator missile that could strike on the PHT pump/motors and/or the reactivity mechanism deck area in the reactor building. Therefore, this particular scenario is screened out during Phase 1 assessment for Bruce B. For the electrical equipment impact, a bounding calculation of CDF associated with turbine missiles striking Group 1 electrical equipment was carried out for Bruce NGS A and B with the following results for Bruce NGS A and B:</p> <p>The larger value for Bruce NGS B (1.61 x1E-6 occ./yr.) compared to Bruce NGS A (5.43E-8 occ./yr) is mainly due to following factors:</p> <ol style="list-style-type: none"> <li>Higher Conditional Core Damage Probability (CCDP) in the case of complete failure of Group 1 systems at Bruce NGS B (1.01E-1) compared to complete failure of pseudo-Group 1 systems at Bruce NGS A (8.79E-3), and</li> <li>Plant specific experience of more load rejection events (generator trips) at Bruce NGS B.</li> </ol> <p>Even though the estimated CDF 1.61E-6 occ./yr) is higher than the screening criteria (Screening Frequency Level (SFL = 1E-6/yr) this specific event is a low risk contributor at Bruce NGS B compared with the internal events PRA (1.6E-5). In addition, the estimated CDF incorporates a significant level of conservatisms in the missile probability evaluation as described below.</p> <p>Areas of potential conservatism that could be considered in a more detailed analysis:</p> <ol style="list-style-type: none"> <li>The total number of load rejection events at Bruce NGS B includes three events when two 500 kV transmission</li> </ol>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>lines to Milton failed, even when explicitly no generation rejection occurred in units 5, 6 and 7 as a result of tornado damage in April 04, 1996.</p> <p>2. The probability of losing Group 1 systems (separate odd and even divisions) is conservatively assumed to be 1.0. A more detailed analysis of missiles, trajectories and equipment locations would result in a lower probability of losing all Group 1 systems.</p> <p>However, considering these conservatisms, given that this event is already a low contributor to overall plant risk, a more detailed analysis is not recommended at this time [Bruce Power External Hazards Assessment Task 7 - Final Report, B-03611.7 P NSAS, July 25, 2014].</p> <p>Further details are provided in Clause 7.15.1.</p>	
8.4	<p>The design shall provide means of reactor shutdown capable of reducing reactor power to a low value, and maintaining that power for the required duration, when the reactor power control system and the inherent characteristics are insufficient or incapable of maintaining reactor power within the requirements of the OLCs.</p> <p>The design shall include two separate, independent, and diverse means of shutting down the reactor.</p> <p>At least one means of shutdown shall be independently capable of quickly rendering the</p>	<p>A new requirement is introduced to cover reactor shutdown capability for DEC's.</p> <p>The safety analysis in Part 3 of the Safety Report [NK29-SR-01320-00002, R005] has shown that for the most critical accident scenario (in-core accidents which damage SORs) the depth of SDS1 is sufficient to maintain subcriticality for at least 15 minutes, at which time the operator can add poison to ensure continued indefinite hold down. SDS2 has enough reactivity depth to maintain indefinite shut down. The following Design Basis Accidents, evaluated in the Safety Report and associated references, rely on automatic activation of the Shutdown Systems to mitigate accident consequences:</p> <p>" Large Loss Of Coolant Accidents (LLOCA);</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>nuclear reactor subcritical from normal operation in AOOs and DBAs, by an adequate margin, on the assumption of a single failure. For this means of shutdown, a transient recriticality may be permitted in exceptional circumstances if the specified fuel and component limits are not exceeded.</p> <p>At least one means of shutdown shall be independently capable of rendering the reactor subcritical from normal operation, in AOOs and DBAs, and maintaining the reactor subcritical by an adequate margin and with high reliability, for even the most reactive conditions of the core.</p> <p>Means shall be provided to ensure that there is a capability to shut down the reactor in DECAs, and to maintain the reactor subcritical even for the most limiting conditions of the reactor core, including severe degradation of the reactor core.</p> <p>Redundancy shall be provided in the fast-acting means of shutdown if, in the event that the credited means of reactivity control fails during any AOO or DBA, inherent core characteristics are unable to maintain the reactor within specified limits.</p>	<p>" Transition Loss Of Coolant Accidents;</p> <p>" Small Loss Of Coolant Accidents (SLOCA);</p> <p>" Electrical failures;</p> <p>" Control failures;</p> <p>" Feedwater and steam supply system failures; and</p> <p>" Moderator system failures.</p> <p>The remaining Design Basis Accidents either do not require reactor shutdown, or occur on a time scale long enough to credit the operator with reducing reactor power manually using the Reactor Regulating System or with manually activating one of the Shutdown Systems (section 1.3.1 of NK29-OSR-63720-63730-0001).</p> <p>Section 4.2.6 of Part 2 of Safety Report describes the two fully capable, separate, independent and diverse shutdown systems. Each system has its own initiation sensors, detectors and logic to ensure functional and physical diversity.</p> <p>Both shutdown systems are capable of shutting the reactor down fast enough for all AOOs, DBAs such that specified limits are not exceeded. There is no recriticality following accidents. For SDS1, operator action can be credited after 15 minutes to augment the depth of shutdown. For SDS2, the shutdown depth is sufficient to keep the reactor shut down indefinitely for even the most reactive conditions of the core.</p> <p>As stated in section 4.1 of Part 2 of the Safety Report, the design of the Bruce B reactors is essentially the same as that of Bruce A. The major changes that were incorporated into the Bruce B design are increased shutoff rod depth for</p>	

 <b>candesco</b> <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>While resetting the means of shutdown, the maximum amount of positive reactivity and the maximum rate of reactivity increase shall be within the capacity of the reactor control system.</p> <p>To improve reliability, stored energy shall be used in shutdown actuation.</p> <p>The effectiveness of the means of shutdown (i.e., speed of action and shutdown margin) shall be such that specified limits are not exceeded, and the possibility of recriticality or reactivity excursion following a PIE is minimized.</p> <p>Guidance</p> <p>For the two means of shutting down the reactor to be independent of each other, they do not share components. If both means act inside the core and complete separation is not possible, adequate separation of ex-core components should be demonstrated.</p> <p>The design uses diverse methods for all aspects of the shutdown means such as:</p>	<p>Shutdown System 1 (SDS1), the addition of five horizontal flux detector units, the addition of one extra injection nozzle and injection tank for Shutdown System 2 (SDS2), and the adoption of adjuster units in place of booster units.</p> <p>Following submissions to the CNSC on the restart of Bruce A Units 1 and 2, the CNSC in the May 2007 response requested that Bruce Power should re-examine the depth of shutdown for SDS1 (page 5 of letter [NK21-CORR-00531-04994 / eDoc 3048401]) and determine if it was practicable to increase the shutdown margin. The results of the SDS1 shutdown depth assessment confirm that Bruce 1&amp;2 with a 12-bundle core configuration are within the limits determined for the existing safety case of Bruce 3&amp;4 (BARSA).</p> <p>As part of the LLOCA Safety Margin Restoration Project a number of design changes that can provide improvement to LLOCA safety margins have been identified. These alternatives involve improving the effectiveness of both shutdown systems (SDSs) by adding two neutronic trips in each SDS to sufficiently reduce the trip time credited in safety analysis. The two new trips in each SDS are intended to make use of the existing neutronic signals with one trip using signals from the in-core flux detectors and the other from the ex-core ion chambers.</p> <p>As discussed in the December, 2015 correspondence [NK29-CORR-00531-12491] Bruce Power is committed to implementing the linear rate trips as physical design improvements in both Bruce A and Bruce B, and is currently pursuing installation of Design Demonstration Units of the linear rate trip on the lead unit in Bruce B to demonstrate feasibility of design.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>o the insertion of solid control rods and injection of a solution of neutron absorbing material are the diverse methods normally used in water-cooled reactors</p> <p>o diverse methods should be considered in the design of sensors, logic and actuation of the shutdown means</p> <p>As stated in this regulatory document, "redundancy shall be provided in the fast-acting means of shutdown" unless the safety analysis demonstrates that, for any AOO or DBA coincident with failure of a single fast-acting means of shutdown, the acceptance criteria can be met. In which case, only one fast-acting means of shutdown would be required.</p> <p>For shutdown means based on injection of a neutron absorbing solution, chemistry-related issues (such as avoiding precipitation) should be addressed.</p> <p>The design authority should specify the requirements for inspection, test and maintenance, including commissioning tests to verify the speed and depth of shutdown for each shutdown means.</p>	<p>It is recognized that the shutdown systems have not been designed specifically to cope with design extension conditions as introduced in CNSC REGDOC-2.5.2. Regardless, the licensing basis includes analyses that address dual failure events such as LOCA plus LOECI. These events represent some sequences that would be considered as DEC's or severe accidents. The most challenging event for determining the adequacy of SDS1 depth is LOCA plus LOECI. Safety analysis was performed for various PT/CT failure scenarios to calculate the margin to criticality provided by SDS1 following such events - Part 3, Appendix 4.5, Section 4.5.3 of the Bruce B Safety Report [NK29-SR-01320-00002, R005]. As discussed in Section 4.5.3 of Part 3 of the Safety Report, an in-core break can damage the guide tubes of reactivity devices such as SORs or MCAs. In addition, due to coolant discharging into the moderator, the most limiting case for an in-core break occurs when the maximum possible amount of soluble neutron poison is present in the moderator. The analysis was performed for the worst-case core configuration for such accidents, which is a restart after a long shutdown from operation at the plutonium peak (Pu-peak). At the Pu-peak, the soluble neutron poison concentration in the moderator is at a maximum. The analysis was based on steady-state calculations of the reactivity balance. An accident scenario consisting of a postulated PT/CT failure occurring in an equilibrium-core configuration under normal operating conditions (the net positive reactivity associated with coolant discharge into the moderator is well within the control capability of the RRS) was also documented in the Bruce B Safety Report [NK29-SR-01320-00002, R005]. As discussed in Section 4.5.4.1.3, the limiting subcriticality margin may occur with either loss of ECI conditioning signal or loss of</p>	




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>For LWR designs, fuel rod bowing can lead to loads on control rod guide tubes which may impair a rod-based shutdown means. The fuel design should ensure that this does not occur in operational states and DBAs.</p> <p>The most reactive conditions of the core required for the analysis normally include a core with maximum allowable excess reactivity (for example, following batch refuelling) and the most reactive conditions for coolant and moderator temperature and density (for example, at cold shutdown conditions for a reactor with a negative temperature coefficient of reactivity).</p> <p>For CANDU reactors, there is a possibility of an in-core loss of coolant accident (LOCA). This poses a special challenge to reactivity control systems. In particular, hydraulic loads from an in-core LOCA can damage shutoff rod guides, and possibly damage poison injection nozzles. If shutdown action is required for an in-core LOCA, the design specification should identify how many reactivity devices may be damaged by the in-core LOCA. This should be consistent with the assumptions in the safety analysis. The results of the analysis of the extent of the damage and supporting experiments should be provided.</p>	<p>ECI. Thus, a total of four potentially limiting cases are examined to determine minimum available subcriticality margin following the break (Appendix 4.5 of Part 3 of the Safety Report). As documented in Section 4.5.4.3 Reactor Core Response, Appendix 4.5 Pressure Tube/Calandria Tube Failure of Part 3 of the Safety Report, the depth of SDS1 is sufficient to maintain the reactor subcritical for at least 15 minutes (900 seconds), at which time the operator can add poison to ensure continued indefinite subcritical state. SDS2 inherently has reactivity depth to maintain indefinite shutdown. Thus, even under the extremely pessimistic assumptions made in the analysis, there is sufficient margin to keep the reactor subcritical in the event of a simultaneous PT/CT rupture. Operator intervention prior to 900 s (15 minutes), and the normal action of the RRS after trip will further increase the subcriticality margin.</p> <p>As described in Section 4.2.6 of Part 2 of the Safety Report, SDS1 has 32 neutron absorbing rods that are referred to as shutoff rods. The primary method of quickly terminating reactor operation, when certain parameters enter an unacceptable range, is the release of 32 gravity-drop, spring assisted shutoff rods. Shutdown System 1 (SDS1) used independent triplicated logic, which senses the requirement for a reactor trip and de-energizes DC-operated clutches to release the shutoff rods (section 6.2 of Part 2 of the Safety Report). Moving the shutoff rods is a control function. Dropping them by releasing the clutches is a protective function governed by SDS1. Drive and clutch circuits are independent of each other, which ensures separation of control and protective functions. The shutoff rod units are equipped with accelerating springs. When a rod is fully withdrawn, a spring is compressed to 450 N (100 lb force),</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The performance criteria for the speed and depth of a fast acting shutdown means should be provided by the design authority. A shutdown means is considered to be effective if the safety analysis acceptance criteria are met. The performance criteria for an adequate subcriticality margin of a shutdown means should be provided by the design authority.</p> <p>For LWRs, in particular pressurized water reactors (PWRs), a large LOCA can lead to significant hydraulic loads on core internals, such as control rod guides in the upper plenum. Core barrel distortion could lead to misalignments. If control rod insertion is credited in the safety analysis for a large LOCA (most PWRs do not credit rod movement), the design should demonstrate that control rod insertion will not be impeded.</p>	<p>and held in compression by the clutch, which also carries the weight of the rod. When the clutch is released, the rod is accelerated by the spring, resulting in a drop time shorter than could be achieved by unassisted free fall. Consequently, the corresponding initial negative reactivity is achieved faster. Periodically, partial drop tests are performed to demonstrate that the rods are poised to fall. For this purpose, a timer relay is provided for each shutoff rod. Full drop tests are carried out only during reactor outages (section 6.2.6 of Part 2 of the Safety Report). Shutdown System 2 (SDS2) provides a second method of quickly terminating reactor operation. SDS2 utilizes rapid injection of concentrated gadolinium nitrate solution into the bulk moderator through eight horizontally distributed nozzles. SDS2 employs an independent triplicated logic system, which senses the requirement for emergency shutdown and opens fast acting valves to inject the gadolinium poison into the moderator using high pressure helium (section 6.3.1 of Part 2 of the Safety Report). For the accident conditions identified in Part 3, SDS2 is demonstrated by analysis to have sufficient depth, and to act with sufficient speed, that the reactor siting criteria are met. Following initial injection of the gadolinium poison under high pressure, the poison will continue to disperse throughout the moderator until an eventual negative reactivity considerably in excess of 300 mk is achieved. The performance of the system has been confirmed by on-site commissioning tests. SDS2 is designed to be effective for coincident or dual failures. The dual failure analysis couples each postulated process failure with a failure of ECI or impaired containment. For these conditions, the fission product release from containment must not exceed that permitted for dual failures. The SDS2 trip setpoints and response time of the sensing instrumentation are established</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>to meet the preceding requirements. SDS2 uses a poison injection system driven by stored energy in high-pressure gas (helium) tanks. Per SDS2 Design Manual [MK29-DM-63730-001, Rev. 011], section 3.2.1.1, SDS2 is defined as armed (available for firing) when at least seven of eight poison tanks are in service and the driving helium pressure is greater than 7.5MPa(g). To account for instrument error 7.58MPa(g) is assumed in the analysis. Normally, helium injection pressure is kept around 8.3 MPa(g) with an early warning of 8.1 MPa(g), and late warning of 7.88MPa(g). (See section 3.2.3, of [NK29-DM-63730-001]). The pressure is applied to the poison tanks only after the activation signal is received the high-speed injection valves being air to close valves. This again means that stored energy is used for activation of SDS2.</p> <p>Each shutoff rod is a stainless steel-cadmium-stainless steel sandwich in the form of a tube with an active length of 5.72 m and an active outside diameter of 112.7 mm. In their fully inserted position, the rods are symmetrical about the horizontal mid-plane of the reactor core. The total static reactivity depth provided by inserting all the shutoff rods is - 68.9 mk for equilibrium fuelling conditions. With the two most effective rods missing, the static reactivity depth of the remaining shutoff rods is -49.3 mk. (The two most effective rods are defined in such a way that when they are missing the static reactivity worth of the rest is a minimum). In normal operation, the most reactive situation occurs when the fuel is fresh and the reactivity increases by about 8.7 mk on shutdown due to reduction in fuel temperature. In this case, the shutoff rods are expected to be worth about -49.3 mk with the two most effective rods missing, as in the equilibrium burn-up case. The minimum static reactivity depth is</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>therefore about -40.6 mk (section 4.2.6.1 of Part 2 of the Safety Report).</p> <p>Shutdown System 2 (SDS2) uses the injection of a solution of neutron absorbing material, or poison, into the bulk moderator to shut down the reactor. A solution of gadolinium nitrate in heavy water is injected into the moderator from injection nozzles located along eight horizontal tubes. The locations of the injection nozzles are shown in Figure 4-7 (section 4.2.6.2 of Part 2 of the Safety Report). The power rundown transients measured during the Phase B commissioning experiments clearly indicated that the SDS2 power rundown rate is faster than the SDS1 power rundown rate. The power rundown transients measured during the experiments indicated that the analytical modelling of the shutdown system characteristics used in the accident analysis is conservative.</p> <p>The Operational Safety Requirements for Bruce B Shutdown Systems [NK29-OSR-63720-63730-00001, R001, November 2013] provide the safety limits, the limiting accidents and surveillance requirements for both shutdown systems. The surveillance frequencies are not specified in the OSR. These are determined by the unavailability requirements for the system as confirmed by unavailability assessments. The surveillance requirements for automatic instrumentation functions verify loop operability and ensure ongoing compliance with the instrument uncertainty calculations. These have been used to demonstrate adequate margin to the setpoint Safety Analysis Limits. The allowable band about the ideal within which the components of the instrument loop must remain to be considered operable (allowable values) is specified in the instrument uncertainty calculations.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
8.4.1	<p>The design authority shall specify derived acceptance criteria for reactor trip parameter effectiveness for all AOOs and DBAs, and shall perform a safety analysis to demonstrate the effectiveness of the means of shutdown.</p> <p>For each credited means of shutdown, the design shall specify a direct trip parameter to initiate reactor shutdown for all AOOs and DBAs in time to meet the respective derived acceptance criteria. Where a direct trip parameter does not exist for a given credited means, there shall be two diverse trip parameters specified for that means.</p> <p>For all AOOs and DBAs, there shall be at least two diverse trip parameters unless it can be shown that failure to trip will not lead to unacceptable consequences.</p> <p>There shall be no gap in trip coverage within the OLCs for any operating condition (such as power, temperature), taking into account plant aging. This shall be ensured by the provision of additional trip parameters if necessary. A different level of effectiveness may be acceptable for the additional trip parameters.</p>	<p>The text is changed to include a new requirement to take plant aging into account in trip coverage.</p> <p>The effectiveness of trip parameters is addressed through safety analysis to be performed in accordance with CNSC REGDOC-2.4.1 Deterministic Safety Analysis (Safety Factor 5).</p> <p>The analysis in Part 3 of the Safety Report is consistent with demonstrating that both redundant shutdown systems are effective independently in shutting down the reactor. As stated in section 1.6 of Shutdown Systems OSRs [NK29-OSR-63720-63730-00001], Shutdown System effectiveness is evaluated for all Design Basis Events requiring reactor shutdown. The range of effectiveness for trip signals is evaluated to ensure that for each accident and allowed plant operating state, at least two trip parameters on each SDS meet the derived safety criteria wherever practicable. Some exceptions exist, and these are justified on a case by case basis. A spectrum of accidents (e.g., LOCA break size and location, reactivity insertion rate for Loss of Regulation) is considered together with a range of reactor initial conditions (e.g., reactor power). While trip parameters may be effective for a number of Design Basis Events, the associated limits (setpoints, conditioning and time response) are governed by the most limiting accident for which a given parameter is required to function. These are discussed in the Safety Analysis Limits section of Shutdown Systems OSRs.</p> <p>The limiting accident that sets the requirements for the timing and rate of negative reactivity insertion by the Shutdown System (including spatial effects within the core) is the large break LOCA. Shutdown system effectiveness is</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The extent of trip coverage provided by all available parameters shall be documented for the entire spectrum of failures for each set of PIEs.</p> <p>An assessment of the accuracy and the potential failure modes of the trip parameters shall be provided in the design documentation.</p> <p>Guidance</p> <p>The effectiveness of trip parameters should be assessed through safety analysis performed in accordance with REGDOC-2.4.1, Deterministic Safety Analysis.</p> <p>Trip coverage should be demonstrated across the full range of operating states, for all credited shutdown means and all credited trip parameters. Note that the number of credited shutdown means and the number of credited trip parameters can vary with the event, the reactor design, and whether there is a direct trip available.</p> <p>Defining derived acceptance criteria appropriate to a particular design is the responsibility of the design authority. CNSC REGDOC-2.4.1, Deterministic Safety Analysis, provides the</p>	<p>demonstrated for reactor power up to the applicable limit which is 93%FP (indicated) for units in which all four bundle shift channels have been re ordered to fuelling with flow and 90%FP for the remainder. The limiting accidents for core sub criticality are single channel events resulting in pressure tube/calandria tube rupture because of the potential to impair SDS1 function by damaging neighbouring shutoff rod guide tubes, and because of the potential for moderator poison dilution.</p> <p>It is noted that, as documented in NK21-CORR-00531-10943 / NK29-CORR-00531-11325, following a single pump trip the HTHP trip is the primary trip on each SDS, and it occurs before the onset of flow oscillations, with no backup trip on either shutdown system prior to the initiation of flow oscillations. Bruce Power is evaluating changes to the trip parameters to improve SDS effectiveness for LOF events in order to provide dual parameter trip coverage before the onset of flow oscillations. In addition, Bruce B is now being fuelled with 37M fuel bundles, which offsets the effects of HTS aging.</p> <p>The analysis in Part 3 of the Safety Report is consistent with demonstrating that both redundant shutdown systems are effective independently in shutting down the reactor. With the exception of a few justified cases, as documented in Section 1.6 of Part 3 of the Safety Report, trip coverage maps for the various events demonstrate that two trips are effective.</p> <p>Acceptance criteria are not explicitly specified for AOOs (Gap). Further details are presented in the assessment against CNSC REGDOC-2.4.1 requirements in Safety Factor</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>requirements.</p> <p>Derived acceptance criteria should be defined separately for AOOs and DBAs. The derived acceptance criteria should be set to give an appropriate level of confidence that a fundamental safety function is assured, or that a barrier to fission product release will not fail. The derived acceptance criteria should:</p> <ul style="list-style-type: none"> <li>• be quantifiable and well understood</li> <li>• account for the fact that the safety analysis is stylized, and the plant condition at the time of the accident may be significantly different from the analyzed state</li> <li>• cover uncertainties in analysis, input plant and analysis parameters, as well as code validation</li> </ul> <p>Direct trips are the preferred means of actuating a shutdown means, due to their robustness and low dependence on calculational models.</p> <p>Diverse trip parameters measure different physical variables on the reactor, thus providing additional protection against common mode failure. Where it is impracticable to provide full</p>	<p>5.</p> <p>As discussed in Safety Factor 5, procedure, documented in BP-PROC-00363, defines the elements, functional requirements, implementing procedures and key responsibilities associated with the Nuclear Safety Assessment (NSA) process. The objective of NSA is to ensure that all necessary nuclear safety requirements are defined for the actual or proposed design of the plant throughout the design modification process or in addressing emergent issues (e.g., plant ageing) that may affect the Design Basis or the Safety Report Basis.</p> <p>Plant operating limits and conditions are taken into account in the analysis assumptions and inputs of Part 3 of the Safety Report. Analyses of the main events impacted by ageing are revised to reflect predicted plant conditions applicable to the licence duration. The results of new analysis are consistently used to confirm the validity of the OLCs applicable to the licence duration and if necessary used to derive a more suitable value for use as an operating limit.</p> <p>The AOOs are addressed in Safety Factor 5, therefore are not included here.</p> <p>The design of all of the safety systems considers potential failure modes of the system. The special safety system components are designed such that the most likely failure modes are in the failsafe direction. Trip parameters are considered part of the safety system and as such are examined for failure modes. The accuracy of the trip set points is assessed during the safety analysis and allowance is made in that analysis for inaccuracies in the setpoints. The results of these assessments are documented in Part 3 of the</p>	



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>diversity of trip parameters, different measurement locations, different instrument types and different processing computers should be provided. Manual trip is considered an acceptable trip parameter, if the operator has adequate time to initiate the shutdown action following unambiguous indication of the need to perform the action (in accordance with section 8.10.4).</p> <p>It is the responsibility of the design authority to identify and justify those trip parameters that can be considered “direct”. The design authority should also demonstrate that any trip parameters that are a measure of the event, but not a measure of the challenge to acceptance criteria, cannot be “masked” or “blinded” by control system action or other means.</p> <p>Trips that are dependent on a number of measured variables, such as low DNBR (departure from nucleate boiling ratio) trips in PWRs can only be considered direct if all the variables are direct.</p> <p>Guidance on applying the requirements for number and diversity of trip parameters is given in REGDOC-2.4.1, Deterministic Safety Analysis.</p>	Safety Report.	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>REGDOC-2.4.1 also provides the minimum expectations for the number of trip parameters.</p> <p>A manual reactor trip can be considered to be equivalent to a trip parameter, if the requirements for crediting operator action from the main control room are met (see section 8.10.4) and the reliability of manual shutdown meets the reliability requirements for an automatic trip.</p>		
8.4.2	<p>The design shall permit ongoing demonstration that each means of shutdown is being operated and maintained in a manner that ensures continued adherence to reliability and effectiveness requirements.</p> <p>Periodic testing of the systems and their components shall be scheduled at a frequency commensurate with applicable requirements.</p> <p>Guidance</p> <p>The reliability calculation should include sensing the need for shutdown, initiation of shutdown, and insertion of negative reactivity. All elements necessary to complete the shutdown function should be included.</p>	<p>There are no changes to the requirements in this clause.</p> <p>Each shutdown system was designed to allow on-power testing to demonstrate that it will meet its unavailability targets. Furthermore Bruce Power is committed to a maintenance and testing program as specified in the OP&amp;Ps 63.1 Shutdown System Availability [BP-OPP-00001, R019]. As per OP&amp;P 03.5, the shutdown systems shall be tested according to programs which demonstrate individual shutdown system unavailabilities, each independent of the other, of less than 1E-3 yrs/yr.</p> <p>As described in Part 2, Section 6.1.1 of the Safety Report, to provide a high degree of assurance that a special safety system will perform as designed when called upon to do so, the unavailability target of each is limited to less than 1E-3 yr/yr. Also, where such choice is available, special safety system components are designed such that the most likely failure modes are in the failsafe direction.</p> <p>The surveillance requirements are specified in Operational Safety Requirements for Bruce B Shutdown Systems [NK29-OSR-63720-63730-00001, R001]. Section 2.1 SDS1</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The reliability of the shutdown function should be such that the cumulative frequency of failure to shutdown on demand is less than 1E-5 failures per demand, and the contribution of all sequences involving failure to shutdown to the large release frequency of the safety goals is less than 1E-7/yr. This considers the likelihood of the initiating event and recognizes that the two shutdown means may not be completely independent.</p> <p>Section 7.6.2 requires that the shutdown function be delivered even in the presence of any single failure and even during the worst configuration from testing and maintenance. For example, for a rod based system to meet the SFC, the safety analysis may assume that the two highest worth control rods are unavailable (one for testing, and one assumed to fail on demand, in accordance with the SFC). In this case, no further testing of rods would be allowed until the rod under testing becomes available.</p>	<p>mechanical hardware operability conditions and Section 3.1 SDS2 mechanical hardware present the results of the applicable analyses to address the single failure criterion application.</p> <p>As discussed in Safety Factor 6, the Level 1 PRA At-Power Model Integration Report including EME B1401/RP/004 R01 (Enclosure 11 of NK21-CORR-00531-111324/NK29-CORR-00531-11729, Submission of S-294 Probabilistic Risk Assessment Final Reports, Bruce Power letter, F. Saunders to K. Lafrenière, July 31, 2014) incorporates all sequences including failure to shut down into the fuel damage category FDC1, whose value is estimated as 2.87E-8 occurrences per reactor per year. Thus the guidance target of cumulative frequency of failure to shut down on demand being less than 1E-5/yr is demonstrated by the fuel damage category FDC1 in the Level 1 PSA.</p> <p>The results of the Level 2 At-Power Summary Report, B0900/RP/055 R01, December 2013 (see NK21-CORR-00531-10958/NK29-CORR-00531-11342, Enclosure 4, Submission of S-294 Probabilistic Risk Assessment Deliverables, Bruce Power letter, F. Saunders to R. Lojk, December 24, 2013) indicate that from Level 1 PRA, Fuel Damage Category 1 (FDC1) represents all sequences involving rapid accident progression resulting from failures to shut down the reactor when required. FDC1 is conservatively assumed to cause early consequential containment failure with a 0.5 probability and the failure sequence is assigned to a unique Plant Damage States (PDS), PDS1. Release Categories (RCs) are defined to bin the consequences associated with containment event tree end-states to facilitate comparison with safety goals. RC0 consists of single</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		unit events (PDS1), two-unit events (PDS3A) and three- or four-unit events (PDS3). The contributions to RC0 of PDS3 and PDS3A are 94% and 4%, respectively, meaning that the contribution of PDS1 to RC0 is approximately 2%. The frequency of RC0 is included in the LRF calculation. RC0 frequency is 4.71E-6, which means that the contribution to it from PDS1 is 9.42E-8. This is below the target for the contribution of all sequences involving failure to shut down to the large release frequency of the safety goals of 1E-7/yr. Two aspects have to be noted: 1) the 95th percentile (from uncertainty analysis) of RC0's PDS1 contribution exceeds the 1E-7/yr target, and 2) credit for Emergency Mitigating Equipment and Severe Accident Management was not incorporated into these BBRA results, i.e. in B0900/RP/055 R01, December 2013.	
8.4.3	<p>Once automatic shutdown is initiated, it shall be impossible for an operator to prevent its actuation.</p> <p>The need for manual shutdown actuation shall be minimized.</p> <p>The means for manual actuation and for monitoring shutdown status shall be provided in the main control room and secondary control room.</p>	<p>A new requirement for manual actuation and for monitoring shutdown status in the secondary control room is introduced.</p> <p>All shutdown system actions that are required in the short term are automatic for all accidents considered at Bruce B. There are no requirements for operator action for trip initiation or any means of inhibiting the trip initiation, and once initiated the operator cannot stop such actions. The complete list of operator actions credited in the Safety Report is given in Tables 1-1 through 1-10 of Section 1 of Part 3 of the Safety Report [NK29-SR-01320-00002, Rev.005]. For each accident scenario identified in the tables, the credited operation action time, the unambiguous indicators that inform the operator of the accident, and the station operating context in which the accidents occur are presented. It can be seen that for the shutdown actions required by the operator there is substantial time for such actions, usually 15 minutes or</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>more.</p> <p>As shown in Figure 6-7 of Part 2 of the Safety Report, there are two manual trip push buttons and one test trip push button. The manual trip can be actuated from the main control room or from the secondary control area, either channel by channel or all three channels simultaneously. The trip push buttons in the secondary control area are connected directly to the trip logic, while the trips from the main control room are actuated via buffer relays. There is also a local test trip push button for each channel mounted on each SDS2 channel cubicle, which can open only one channel at a time.</p> <p>The design requirements for Secondary Control Area function are presented in the Bruce B Secondary Control Area Units 5678 Design Manual [NK29-DM-63760-001, Rev. 004, August 16, 2013]. The SCA and associated field panel areas provide control and monitoring capability remote from the MCR Complex to enable operators to:</p> <ol style="list-style-type: none"> <li>1. Shut down the reactors and monitor the shutdown state.</li> <li>2. Effect removal of decay heat.</li> <li>3. Monitor necessary neutronic and process safety parameters after the common mode incident to permit assessment of the nuclear steam supply system.</li> <li>4. Maintain the containment boundary to prevent release of radioactivity to the public in excess of the allowable limit.</li> </ol> <p>The above functions shall be accomplished by monitoring and controlling Units 5-8 (and in particular the applicable</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>Critical Safety Parameters (CSP)):</p> <p>" From the SCA and associated field panels, and</p> <p>" By local field control actions.</p> <p>As specified in Secondary Control Areas Design Manual [NK29-DM-63760-001], the SCA instrument and Control loops are dual channel. Specific system details are given under the appropriate system panel descriptions in the DM sections. Safety System controls on SCA panels are repeated on the corresponding Main Control Room Panels. The SCA located control overrides MCR located control and "Handswitch Off Normal" indication is provided when the SCA "takes control" away from the MCR. There are Secondary Control Areas in each of the Reactor Buildings (unit SCAs) and one in the Emergency Water and Power Supply Building (EWPSB) (common SCA). The unit SCA panels permit the control and monitoring of unit safety and safety related systems such as Emergency Water System (EWS) and Emergency Power System (EPS); Shutdown System No. 2 (SDS2), Neutronic Safety Parameters; Process Safety Parameters; Emergency Coolant Injection System (ECIS); Low Speed Drive of the Primary Heat Transport Pumps; and Hydrogen Ignition System.</p> <p>The common SCA panels permit the control and monitoring of station wide safety and safety related systems such as Emergency Water and Power systems, Emergency Coolant injection System and Containment (section 1.3.1 of Secondary Control Area Design Manual [NK29-DM-63760-001].</p>	
8.5	All water-cooled nuclear power reactors shall be	The changes are editorial in nature and provide clarifications	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>equipped with an emergency core cooling system (ECCS). The function of this safety system is to transfer heat from the reactor core following a loss of reactor coolant that exceeds makeup capability. All equipment required for correct operation of the ECCS shall be considered part of the system or its safety support system(s).</p> <p>Systems that supply electrical power or cooling water to equipment used in the operation of the ECCS shall be classified as safety support systems, and shall be subject to all relevant requirements and expectations.</p> <p>The design shall take into account the effect on core reactivity of the mixing of ECCS water with reactor coolant water, including possible mixing due to in-leakage.</p> <p>The ECCS shall meet the following criteria for all DBAs involving loss of coolant:</p> <p>1. All fuel assemblies and components in the reactor shall be kept in a configuration such that continued removal of the residual heat produced by the fuel can be maintained.</p>	<p>rather than imposing new requirements.</p> <p>For the loss of coolant accident, the primary source of cooling has been lost. An emergency cooling supply system, the emergency coolant injection system, injects water into the system at high pressure to remove the initial heat load. After the initial high pressure injection, water spilled from the system is collected from building sumps and pumped continuously through the core. A detailed description of the system is in Section 6 (section 1.3.3.2 of Part 2 of the Safety Report). The Emergency Coolant Injection system is a high pressure, light water system designed to refill the HT system, and thereby cool the fuel in any one of the four reactor units following a HT system loss of coolant accident. Low pressure recovery pumps and heat exchangers provide long-term cooling (section 1.2.3.7 of Part 2 of the Safety Report). As described in Section 6.4.3 of Part 2 of the Safety Report the ECI system is common to all units. A 76 cm (30 in) common supply header runs the length of the station. The header is thermally insulated as required to reduce heat input to the header from secondary side failures. Injection lines to each individual unit contain a parallel pair of normally closed motorized water injection valves, outside the containment structure. Parallel pair of motorized valves, in series with a parallel pair of check valves in the four branch lines that penetrate the containment structure, isolate the ECI system from the HT system.</p> <p>Initially, the source of water for the low pressure ECI is the grade level storage tank. This tank is connected to the suction side of the four low pressure ECI pumps, and is located adjacent to the accumulator building. The low pressure emergency coolant pumps are in a room next to the</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2. A continued cooling flow (recovery flow) shall be supplied to prevent further damage to the fuel after adequate cooling of the fuel is re-established by the ECCS.</p> <p>The ECCS recovery flow path shall be such that impediment to the recovery of coolant following a loss of coolant accident by debris or other material is avoided.</p> <p>The design shall ensure that maintenance and reliability testing can be carried out without a reduction in the effectiveness of the system below the OLCs, if the testing is conducted when ECCS availability is required.</p> <p>In the event of an accident when injection of emergency coolant is required, it shall not be readily possible for an operator to prevent the injection from taking place.</p> <p>All ECCS components that may contain radioactive material shall be located inside containment or in an extension of containment.</p> <p>ECCS piping in an extension of containment that may contain radioactivity from the reactor core</p>	<p>ECl recovery sump. (The ECl recovery sump is inside containment in the east pressure relief duct). Each of the four pumps is connected to the ECl recovery sump by a suction line containing a closed, motorized valve that normally isolates each low pressure ECl pump from the recovery sump. The pumps are supplied from Class III buses and the emergency power supply system. The pumps discharge to the common supply header through three heat exchangers and a heat exchanger bypass line. A check valve station prevents reverse flow during accumulator injection. All active logic is located in a seismically qualified room (R7-320) above the heat exchanger room. All signal connections between indications and controls in the main control room and R7-320 are buffered to prevent local electrical failures in the main control room from incapacitating the ECl system (section 6.4.3 of Part 2 of the Safety Report).</p> <p>The systems that supply electrical power and cooling water to equipment used in the operation of the ECCS are classified as safety support systems and the process is documented in Safety Related System List procedure [BP-PROC-00169].</p> <p>The ECl system is designed to meet an unavailability target of 1E-3 yr/yr. The system is periodically tested in a series of overlapping tests to ensure this target is met. All essential functions can be tested while the reactor is at power. If the ECl system is known to be unavailable, the affected reactor is shut down until the system capability is restored (section 6.4.5 of Part 2 of the Safety Report).</p> <p>As previously discussed under Clause 7.10, the capacity margin of the Bruce A and B emergency support systems to allow for further increases in demand is limited, as it was sized for a considerably different safety case. However, this</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>shall be subject to the following requirements:</p> <ol style="list-style-type: none"> <li>1. As a piping extension to containment, it meets the requirements for metal penetrations of containment.</li> <li>2. All piping and components of the ECCS recovery flow path piping that are open to the containment atmosphere are designed for a pressure greater than the containment design pressure.</li> <li>3. All ECCS recovery flow paths are housed in a confinement structure which prevents leakage of radioactivity to the environment and to adjacent structures.</li> <li>4. This housing includes detection capability for leakage of radioactivity, and the capability to either return the radioactivity to the flow path, or to collect the radioactivity and store (or process it) in a system designed for this purpose.</li> </ol> <p>Intermediate or secondary cooling piping loops shall have leak detection, whether the ECCS recovery system is inside or outside of containment, with the leak detection being such</p>	<p>is rather a design objective and has no impact on safe operation. Should additional loads be required, the Engineering Change Control Program [BP-PROG-10.02] will determine how to address the emergency support system loading issue.</p> <p>The emergency coolant injection system, which is inactive but poised during normal operation of the station, is activated automatically when a loss of coolant accident is detected in any unit. An emergency coolant injection signal is initiated when the HT pressure falls below a set value in conjunction with another parameter that indicates a LOCA, such as high reactor vault pressure, high reactor vault temperature or high moderator level within the calandria or if the HT system remains below 5.5 MPa for an extended time period (section 6.4.4 of Part 2 of the Safety Report). The response of the emergency coolant injection system can be divided into short and long-term phases. The short-term phase consists of high-pressure injection from the accumulator tanks followed by lower pressure injection from the grade level storage tank by the pumps. The long term operating mode involves recovery of water from the sump and recirculation via the pumps and heat exchangers. Modifications have been made to the sump strainers to ensure that there is no potential blockage that would affect the ECI system recovery function. Periodic inspection of the recovery sump to confirm there is no debris which could restrict flow and that the strainers have not deteriorated is specified in the surveillance requirements in section 6.2.12 of ECI OSRs [NK29-OSR-34340-00001]. Analysis of the performance of the recovery sump strained is documented in "Reverse Flow Through Bruce B ECI Recovery Strainer OB-34340-STR13" [NK29-CALC-34340-</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>that upon detection of radioactivity from the ECCS recovery flow, the loops can be isolated as per the requirements for containment isolation.</p> <p>Inadvertent operation of all or part of the ECCS shall have no detrimental effect on plant safety.</p> <p>Guidance</p> <p>The design authority should describe any reactivity control function performed by the ECCS, together with necessary limits and conditions. For example, PWRs often credit soluble boron in the ECCS accumulators and storage tanks, to supplement control rod insertion for long term reactivity control.</p> <p>ECCS designs should be proven by appropriate experimental programs and computer modelling. It should be demonstrated that there is adequate experimental evidence of ECCS effectiveness.</p> <p>Examples of items that could be important in the ECCS design include:</p> <ul style="list-style-type: none"> <li>mechanisms for core bypassing (e.g.,</li> </ul>	<p>00039 Rev 001, September 16, 2002].</p> <p>The safety analysis documented in Part 3 of the Safety Report has confirmed that this system is capable of limiting the fuel temperatures and chemical reactions from the zirconium water reaction to acceptable values for all LOCAs. Under these conditions, the fuel damage will not impede the system operation.</p> <p>ECI can be manually blocked, and has to be when the HT system is at low pressure (inactive but poised during normal operation). This is done through procedural controls as outlined in Section 34.1 of the OP&amp;Ps [BP-OPP-00001, R019], which states: The Emergency Coolant Injection System shall only be temporarily blocked from the control room following procedures approved by the Senior Operations Authority and concurred with by the CNSC.</p> <p>As described in the ECI OSRs, the Leakage Mitigation Subsystem refers to those provisions which ensure that there is no significant additional public dose resulting from leaks from equipment located in the ECIS equipment room during post-LOCA operation. The subsystem also prevents flooding the ECIS pumps should a significant leak develop during the ECIS mission time. Post-accident, the Leakage Mitigation Subsystem collects any leakage into the ECIS equipment room and returns it to containment. The operability of this subsystem is defined by mechanical hardware characteristics only (e.g., valve positions). Leakage in Common High Pressure Injection Subsystem is addressed in sections 4.1.6 and 4.3.6 of ECI OSRs. Further details about leakage from portions of the system not serviced by the Leakage Mitigation Subsystem (i.e., outside the ECI system recovery equipment</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>downcomer bypass during blowdown in PWRs, or core bypass via steam generators in CANDU)</p> <ul style="list-style-type: none"> <li>effects of non-condensable gas on ECCS performance</li> <li>phenomena that can impede core refill and rewet (such as periods of stagnation, steam binding in PWR steam generators, parallel channel effects in CANDU)</li> <li>effect of multi-dimensional flow in heat transport system headers in CANDU</li> <li>effect of non-uniform channel flow resistance in the CANDU core (e.g., peripheral low-flow and low-power channels having much higher flow resistance for ECCS refill)</li> <li>effect of the pressurizer</li> </ul> <p>Section 8.5 requires that the ECCS is capable of removing residual heat over an extended period. This normally involves recovering water spilled from the break, cooling it and returning it to the reactor. It should be demonstrated that:</p> <ul style="list-style-type: none"> <li>the design is capable of recirculating coolant even in the presence of the maximum quantity of debris that may be present after a LOCA</li> <li>possible chemical effects in the reactor</li> </ul>	<p>room) are provided in the ECI OSRs.</p> <p>During recovery operation following a LOCA the ECI recovery system becomes an extension of containment (see also Section 4.1.6). The fluid being recirculated could contain radioactive fission products and for this reason leakage from the system must be controlled. Leakage may be due to a valve being left open or passing, from packing or seals of pumps and valves, or any other leak in the pressure boundary that develops post-accident. In general, small amounts of leakage do not impact on injection effectiveness. No major leak sources are expected because the portion of the recovery system that is outside containment is built to ASME Code Class 2 and is continuously pressurized and monitored for leaks. The limit on allowable leak rate is determined by the mitigating provisions available in the vicinity of the leak (per Section 7.3 of ECI OSRs [NK29-OSR-34340-00001]), as well as the nature of the leak. If a leak is found in the recovery area that would still be well within the capacity of the currently operable sump pumps during recovery, it would not be considered to render ECIS inoperable. However the system is designed to be leak tight, and whenever a leak is discovered, it must be assessed to confirm that available mitigating provisions are adequate, with sufficient margin to accommodate the expected increase in leakage during recovery operation post-accident (section 6.1.12 of ECI OSRs). Although a pipe leak will be detected, there is no means of detecting any activity from primary to secondary side leaks in the heat exchangers. However, Bruce B Abnormal Incidents Manual (AIM) [NK29-AIM-03600.1, Rev. 056] procedures direct the operating staff to sample for heat exchanger leaks following a LOCA.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>building recovery sump have been considered, and any chemical precipitates and other species (such as gels, colloids etc.) cannot significantly impair ECCS recovery flow (for example, at strainers or the heat exchangers)</p> <ul style="list-style-type: none"> <li>recovery actions (such as transfer to hot leg injection of ECCS, or transfer to the normal residual heat removal system) are described and shown to be achievable; long-term removal of heat by boiling in the core could potentially lead to deposition or fouling (for example, precipitation of boric acid crystals) impairing flow and heat transfer</li> <li>wear on bearings and seals has been considered, including abrasion by small particles and chemical corrosion</li> <li>natural circulation flows, where credited, are capable of providing sufficient flows and cannot be impaired by such effects as accumulation of non-condensable gas or adverse temperature distributions</li> </ul> <p>Sections 7.14 and 7.16 describe the inspection, test and maintenance requirements which should include:</p> <ul style="list-style-type: none"> <li>commissioning tests to verify flow, pressure drop and (if applicable) tank isolation after injection for accumulators and other makeup</li> </ul>	<p>The emergency coolant injection pressure boundary is continuously checked by maintaining a positive internal pressure and detecting any leaks. Leakage from any valves in the ECI recovery system is returned to active drainage rather than into the loop itself. The pumps and heat exchangers associated with the ECI system are located in the ECI recovery room. The ECI system is designed to minimize leaks, and leaks into the recovery room during the long-term recirculation phase are unlikely. However, as a precautionary measure the recovery room is designed as a confinement area. The ventilation exhaust line associated with this area is connected to the Unit 4 auxiliary bay filtered exhaust system. The ventilation system is designed to box up on a loss of coolant signal (section 6.5.5.4 of Part 2 of the Safety Report).</p> <p>Emergency Coolant Injection System Design Manual [NK29-DM-34330/34340-003, Rev. 001] presents the design requirements and design description for the Emergency Coolant Injection System.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>tanks</p> <ul style="list-style-type: none"> <li>commissioning tests to verify pump head, flow and system pressure drop for pumped injection</li> </ul> <p>As stated in this regulatory document, "in the event of an accident when injection of emergency coolant is required, it shall not be readily possible for an operator to prevent the injection from taking place." This can be achieved by a variety of methods to ensure that the blocking action is intentional (such as requiring multiple actions, sequential actions, actions that are spatially separated, or actions that have to be performed by different people).</p> <p>Emergency operating procedures should prohibit blocking of ECCS injection, unless there is clear and unambiguous indication that it is not needed (for example, if there is clear indication that there is adequate inventory to ensure core cooling, and that the inventory is not decreasing).</p> <p>Injection of a large volume of cold water may cause pressurized thermal shock to the reactor coolant pressure boundary, or distortion of reactor internals. The design authority should demonstrate that thermal shock has been adequately addressed in the design, in terms of</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>calculating transient fluid conditions at key locations, as well as resulting metal temperature and the corresponding stresses.</p> <p>Water hammer loads may be generated by operation of valves, or by condensation when cold water is injected into steam filled systems. The design authority should demonstrate that a water hammer assessment has been performed.</p>		
8.6.1	<p>Each nuclear power reactor shall be installed within a containment structure, so as to minimize the release of radioactive materials to the environment during operational states and DBAs. Containment shall also assist in mitigating the consequences of DEC's. In particular, the containment and its safety features shall be able to perform their credited functions during DBAs and DEC's, including melting of the reactor core. To the extent practicable, these functions shall be available for events more severe than DEC's.</p> <p>The containment shall be a safety system and may include complementary design features. Both the containment system and the complementary design features shall be subject to the respective design requirements provided in this regulatory document.</p>	<p>The new text added is mostly for clarification purpose rather than imposing new requirements.</p> <p>As described in Section 6.5 of Part 2 of the Safety Report containment is a special safety systems, which forms an envelope around the nuclear components of the reactor and the reactor coolant system. It consists of a number of systems and subsystems whose collective purpose is to prevent any significant release of radionuclides, which may be present in the containment atmosphere following postulated accident conditions, to the outside environment An important criterion for determining the effectiveness of the containment envelope is the integrated leak rate for the period of the pressure excursion. To meet the design leakage requirements, two measures are employed. The first involves stringent design requirements to minimize the leak rate. The second is to prevent the design pressure within the containment envelope from being exceeded following a LOCA. The containment system quickly reduces the containment pressure pulse to sub-atmospheric level following a large energy release within the containment envelope and hence minimizes uncontrolled releases to the</p>	IC



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design shall include a clearly defined continuous leak-tight containment envelope, the boundaries of which are defined for all conditions that could exist in the operation or maintenance of the reactor, or following an accident.</p> <p>All piping that is part of the main or backup reactor coolant systems shall be entirely within the main containment structure, or in an extension to the containment structure.</p> <p>The containment design shall incorporate systems in order to assist in controlling internal pressure and the release of radioactive material to the environment, following an accident.</p> <p>The containment shall include at least the following subsystems:</p> <ol style="list-style-type: none"> <li>1. the containment structure and related components</li> <li>2. equipment required to isolate the containment envelope and maintain its completeness and continuity following an accident</li> </ol>	<p>outside environment. A detailed performance assessment of the containment system is given in Part 3 of the Safety Report.</p> <p>A large part of the Maintenance Cooling System is located outside the containment, for both Bruce A and B. The Maintenance Cooling System is suitably isolated from the heat transport system and analyses of failures in the heat transport system provided in the Safety Report demonstrates that fuel cooling is adequate to ensure that no fuel failures occur due to increasing fuel temperature. In addition to the containment system, there are three confinement areas for each unit. In addition to the containment system, there are four confinement areas for each unit. They are: the moderator confinement area, the instrument room confinement area, the miscellaneous equipment rooms confinement area in each unit, and the common ECI recovery room. These areas are outside the containment envelope. Here, failure of a system could result in a limited release of radioactive material but there is little stored energy involved and the integrated energy release would be small. The confinement areas are enclosed and ventilated in such a way that activity release from these areas can be adequately controlled (section 6.5.1 of Part 2 of the Safety Report).</p> <p>The containment envelope includes the four reactor vaults, the fuelling duct, the central fuelling area, the east service area, the pressure relief ducts, the pressure relief valve manifold, the vacuum building, airlocks and transfer chambers, and extensions of containment arising from numerous piping penetrations. The containment envelope (excluding penetrations) is shown in Figure 6-10 of Part 2 of the Safety Report. The majority of the extensions are</p>	




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>3. equipment required to reduce the pressure and temperature of the containment and reduce the concentration of free radioactive material within the containment envelope</p> <p>4. equipment required for limiting the release of radioactive material from the containment envelope following an accident</p> <p>When the containment design includes the use of compressed air or non-condensable gas systems in response to a DBA, the autonomy of the compressed air system shall be demonstrated.</p> <p>In the event of a loss of compressed air, containment isolation valves shall fail in their safe state. The design authority shall identify where and when the containment boundary is credited for providing shielding for people and equipment.</p> <p>Guidance</p> <p>The design should establish acceptance criteria for inspection, testing and maintenance provisions including, as applicable:</p> <ul style="list-style-type: none"> <li>containment penetration isolation times</li> </ul>	<p>normally closed and a number are normally open. The normally open extensions are automatically closed following the detection of high activity or high pressure inside containment, thus ensuring that a closed envelope is provided to contain potential activity in the event of an accident.</p> <p>The general nuclear safety and design philosophy for extensions to Containment Atmosphere, PHTS and Moderator System is to provide barriers having redundancy, reliability and performance capabilities which reflect the importance of the barrier in meeting the "CONTAIN" basic nuclear safety requirement (i.e., potential radioactive dose for DBAs must be within prescribed limits). A single barrier that is closed and not significantly leaking is sufficient to ensure release limits within prescribed limits. However, to meet the general philosophy, dual isolation is usually provided in the design. The dual isolation provides redundancy for normal operation, ensures reliable single isolation for DBAs, provides single isolation for specific barrier failures, and permits maintenance on containment barriers when containment availability is required. The design guide NK29-DG-03650-006 describes acceptable methods of penetration closure. The exemptions from the design requirements are documented in the associated Design Guide Supplement (DGS). For example the D2O recovery system cannot be isolated automatically on containment isolation logic since it is designed to operate when a heat transport break occurs. A second isolation valve in series would have to be controlled by the operator in an identical manner. This exemption from the dual automatic isolation valve requirement is justified in [NK29-DGS-29-03650-003, R000]. Similar exemption is justified for the Instrumented Pressure Relief Valves which</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>containment spray performance</li> <li>filtered venting capability</li> <li>vacuum building actuation</li> <li>hydrogen mitigation system capability (e.g., recombiners)</li> <li>systems and equipment used for containment heat removal</li> <li>concrete condition and possible concrete degradation</li> </ul> <p>The effects of release of compressed air inside the containment after isolation (for example, leakage from air-operated valves) should be considered in calculating containment pressure loads.</p> <p>Additional information:</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>CSA Group, N287.3, Design Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, Toronto, Canada.</li> <li>CSA Group, N290.0/N290.3, package,</li> </ul>	<p>are required to operate after a LOCA to reduce the containment overpressure period. As these valves are on lines leading to containment they are considered to be containment isolation valves and Design Guide Supplement [NK29-DGS-29-03650-007] was issued to confirm that the design is adequate and meets the intent of the design guide.</p> <p>Twelve main pressure relief valves, four instrumented main pressure relief valves, four auxiliary pressure relief valves and two reverse flow valves are provided to keep the reactor building pressure within design limits. All of these valves are located inside the pressure relief valve manifold. When closed, they isolate the rest of containment from the vacuum building (section 6.5.2.3 of Part 2 of the Safety Report).</p> <p>The dousing system consists of an emergency water storage tank below the ceiling of the vacuum building and a system of spray headers. The tank and headers are interconnected with a vacuum chamber. The function of the dousing system is to condense any steam discharged into the vacuum building, to cool the steam and air mixture in the building and thus limit any pressure rise (section 6.5.2.4 of Part 2 of the Safety Report). The Negative Pressure Containment System Part 4, Water Spray System (Dousing) Design Manual [NK29-DM-34200-004] presents further details about the design and operation of the system. The commissioning and in-service testing of the dousing system are presented in section 7.0 of [NK29-DM-34200-004, R004].</p> <p>The equipment to pump down and maintain the vacuum building pressure, and the equipment to circulate and chemically treat the water in the elevated storage tank, is located in the vacuum building basement (which is not a part of containment). As specified in section 6.5.2.8, heat removal</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	General requirements for safety systems of nuclear power plants and Requirements for the containment system of nuclear power plants, Toronto, Canada.	<p>from containment is provided by a number of coolers. The main coolers in each reactor vault have four axial fans and 10 main air-to-water heat exchangers. In addition, each vault has six wall mounted coolers. The main and the wall mounted coolers both utilize Class III power. The main coolers are seismically qualified, and are connected to the emergency power and water supply. The central fuelling area has its own four air coolers. They remove heat discharged from the fuelling machines when they are parked in the central fuelling area. Each of the four fuelling machine rooms has one air cooler to cool room air. The vault cooling system performs a long-term containment function following a LOCA by providing sufficient heat removal capacity to assist in maintaining the integrity of the containment envelope.</p> <p>Two separate systems are provided for mitigation of hydrogen following the low probability design basis event combinations.</p> <p>(a) Hydrogen Ignition System for mitigation of short term hydrogen generation, and</p> <p>(b) Passive Autocatalytic Recombiners (PARs) for slower longer term hydrogen generation, such as from radiolysis of water. PARs will provide defence in depth for short term hydrogen mitigation as well</p> <p>The Hydrogen Igniter System is provided to remove hydrogen generated in containment. Removal of this hydrogen in a controlled manner is required to prevent structural damage to the containment envelope that could result from potentially severe pressure or temperature transients associated with hydrogen combustion. The system consists of 16 igniters per unit (64 igniters per station) located</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>in the reactor vaults and fuelling machine ducts. The igniters are automatically activated by button up signal following a LOCA and will cause any hydrogen to be burned with a minimal pressure rise in containment (section 6.5.2.9 of Part 2 of the Safety Report). At Bruce B, the igniters and instrumentation are backed up by EPS. The igniters are energized by the containment isolation signal. [NK29-CORR-00531-12195].</p> <p>The Emergency Filtered Air Discharge System (EFADS) is operated to control long-term radiological dose to the public and station staff by providing a well-defined, filtered, controlled and monitored release path of fission products from containment following a LOCA or other Design Basis Accidents. The system consists of two 100% filters and blowers plus duct work and isolation dampers. Each filter contains a demister, heater, prefilter, upstream HEPA filter, charcoal filter and downstream HEPA filter. The exhaust flow is drawn from the vacuum building or the pressure relief valve manifold and is monitored by the post-accident radiation monitoring system prior to being released to the atmosphere via the system exhaust stack. A recirculation line enables pre-discharge monitoring of the exhaust flow prior to the end of the subatmospheric hold up period. An alternate exhaust path from the pressure relief valve manifold also is available.</p> <p>In regard to severe accidents, it should be recognized that Bruce B was not designed to cope with these, other than the dual failure LOCA plus LOECI. The capability of containment to cope with design extension conditions is addressed in Section 8.6.12.</p> <p>As discussed earlier the Bruce B original design for the containment system has not provided complementary design</p>	

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>features to cope with BDBAs and severe accidents, as required under this clause. However, this gap is being mitigated by implementation of the SAMG.</p> <p>As part of the Bruce Power Station Improvement Plans - Fukushima enhancements, projects are underway to enhance the existing understanding of severe accident phenomena and SAMG capabilities. The scope of this work also involves improvement to understanding of severe accident phenomena including containment integrity.</p> <p>.</p> <p>In regard to its potential role as a complementary design feature, the Bruce B containment system was not designed to cope with severe accidents and therefore it has no special design features that would make it a complementary design feature. However, the requirements for severe accidents, as discussed in Section 8.6.12 require that the containment remain leak tight for at least 24 hours and that there be no melt-through of the containment floor. Both of these issues are addressed in the SAMG program, and discussed further in Section 8.6.12.</p> <p>The operation of the containment pressure suppression system is automatic and predominantly passive. The pressure relief valves are actuated by a rise in pressure in the pressure relief duct, and the dousing spray system in the vacuum building is actuated by a rise in the vacuum building pressure. Thus, the energy released by the accident actuates these safety devices. All systems connected to the containment atmosphere are provided with adequate barriers that automatically isolate following an accident. Either a high containment pressure signal or a high radioactivity indication</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>initiates this containment isolation. The operation of water spray system (dousing) during accident conditions is described in section 5.2 of the design manual [NK29-DM-34200-004, R004].</p> <p>The subject of instrument air usage in containment post-accident was discussed extensively with the CNSC during the mid-1980s in connection with extensions to the sub-atmospheric holdup time following a LOCA in order to delay potential off-site releases. A detailed engineering study investigated different options and concluded that it was not cost-beneficial to make the changes to the system so that it could be automatically isolated. Instead, isolation of unnecessary instrument air is dealt with procedurally. The Abnormal Incidents Manual [NK29-AIM-03600.1, Rev. 056] instructs operators to valve out all instrument air on non-incident units when they are cold and depressurized. On the accident unit, there are procedures available to valve out as much of the unnecessary instrument air as possible, for example to close the north side instrument air valve to the vault. The leakage of other compressed gases used in containment - helium, nitrogen, carbon dioxide, and nitrogen was investigated as part of this study and was found to be negligible.</p> <p>The Instrument Air System Design Manual [NK29-DM-75120-001, R04] presents the system design and performance requirements as well as periodic inspection and maintainability requirements. The system reliability requirements are presented in section 2.11 of the DM. The Instrument Air System is a safety support system, which supplies "instrument quality" air at a nominal pressure of 862 kPa(g) (125 psig) to control valve actuators, power operators,</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>pneumatic controllers, etc., and to the laboratories and Spent Fuel Bay Purification System where the quality of service air is not acceptable.</p> <p>The Instrument Air System consists of three sub systems: Unit Instrument Air System, Common Instrument Air System, and EFADS (Emergency Filtered Air Discharge System) Building Instrument Air System. The Unit Instrument Air System supplies instrument air to process systems on a unit basis. The Common Instrument Air System receives compressed air from Service Air System and supplies instrument air to process systems in common areas. The EFADS Building Instrument Air System is the only seismically qualified instrument air system. It supplies instrument air to Post Accident Radiation Monitoring System (PARMS) and backup instrument air to the auxiliary pressure relief valves when the normal instrument air supply is lost. The list of systems supported by the instrument air system is presented in Appendix B of the Design Manual [NK29-DM-75120-001, R004].</p> <p>According to Section 11.2.1.2 of Part 2 of the Safety Report, the instrument air system has been designed on a unit basis, one complete system per reactor unit. There are three compressors for each unit, rated at 303 L/s (645 scfm) at 860 kPa (g) each. Normally, two compressors are operating and one is kept on standby. The maximum unit demand is 470 L/s (1000 scfm), the steady state demand about 377 L/s (800 scfm). Each instrument air system has two 100% air dryers of 470 L/s (1000 scfm) capacity, and air receivers capable of supplying at least 470 L/s (1000 scfm) at 415 kPa (g) for 3 minutes. The receivers provide backup in case of a Class IV power failure, until Class III power becomes available. For</p>	




Article No.	Clause Requirement	Assessment	Compliance Category
		added flexibility, there are inter-unit connections between Units 5 and 6, and Units 7 and 8. Each instrument air system also has a manual tie-in to the service air system for emergency backup. Instrument air for the central service area is taken from the service air system through two 100% dryers of 377 L/s (800 scfm) capacity. Should the service air compressors become unavailable, common instrument air will be available from the service air system receivers for several minutes. A seismically qualified supply of instrument air is also provided in the EFADS and vacuum buildings for the Post Accident Radiation Monitoring System (PARMS) and as back up for the Auxiliary Pressure Relief Valves (APRVs). This air is provided by two 100% air compressors, each with rated capacity of 6.5 L/s (13.7 scfm) at 2000 kPa (g) (290 psig).	
8.6.2	<p>The strength of the containment structure shall provide sufficient margins of safety based on potential internal overpressures, underpressures, temperatures, dynamic effects such as missile generation, and reaction-forces anticipated to result in the event of DBAs. Strength margins shall be applied to access openings, penetrations, and isolation valves, and to the containment heat removal system.</p> <p>The margins shall reflect:</p> <p>1. effects of other potential energy sources, such as possible chemical reactions and radiolytic</p>	<p>The changes are editorial in nature and have no impact on the requirements. The containment envelope includes the four reactor vaults, the fuelling duct, the central fuelling area, the east service area, the pressure relief ducts, the pressure relief valve manifold, the vacuum building, airlocks and transfer chambers, and extensions of containment arising from numerous piping penetrations. The majority of the extensions are normally closed and a number are normally open. The normally open extensions are automatically closed following the detection of high activity or high pressure inside containment thus ensuring a closed envelope is provided to contain potential activity in the event of an accident. The design and positive proof test pressures for the containment envelope are summarized in Section 6.5.2.1 of Part 2 of the Safety Report.</p> <p>The values in section 6.5.2.1 of Part 2 of the Safety Report</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>reactions</p> <p>2. limited experience and experimental data available for defining accident phenomena and containment responses</p> <p>3. conservatism of the calculation model and input parameters</p> <p>The positive and negative design pressures within each part of the containment boundary shall include the highest and lowest pressures that could be generated in the respective parts as a result of any DBA.</p> <p>The containment structure shall protect systems and equipment important to safety in order to preserve the safety functions of the plant.</p> <p>The design shall support the maintenance of full functionality following a DBE for all the parts of the containment system credited in the safety analysis.</p> <p>The seismic design of the concrete containment structure shall have an elastic response when</p>	<p>encompass the highest pressures from all of the accidents considered in the licensing process as well as the lowest pressures considered by spurious opening of containment isolation valves. The pressure rise following a controlled burn of hydrogen have been calculated and shown to be within limits. As described in the Post-LOCA Hydrogen Ignition System Design Manual [NK29-DM-62111-001, Rev. 01], the effects of controlled initiated burns at low concentrations of hydrogen and oxygen in the presence of steam, on the special safety and safety related systems (such as Shutdown Systems 1 and 2, Emergency Coolant Injection, Containment, Moderator, filtered air discharge, vault coolers, etc.) have been reviewed by the respective designers. It has been concluded that the pressure and temperature transients resulting from any deliberately initiated burns will have no adverse consequences on the safe Post-LOCA operation of the reactors. Analysis is performed to demonstrate the capability of the containment structure to withstand the pressure loading from hydrogen deflagration, for hydrogen source terms derived for large break LOCA with ECI system available and with ECI system impaired cases. Details of pressure loading due to hydrogen combustion are presented in Appendix 5.6 of Part 3 of the Safety Report.</p> <p>According to Section 6.5.2.1 of Part 2 of the Safety Report, the acceptance leakage rate for the containment envelope, except for the vacuum building, is set at 2% of the contained air mass per hour at 82.7 kPa(g) (12 psig). The vacuum building acceptance leakage rate is set at 2% of contained air mass per hour at 48.3 kPa(g) (7 psig). Operational targets are set at lower values. Leakage rate tests for the vacuum building and upper chamber are conducted periodically at 7 kPa(a) (1 psia). The acceptance leakage rates at metric</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>subjected to seismic ground motions. The special detailing of reinforcement shall allow the structure to possess ductility and energy-absorbing capacity, which permits inelastic deformation without failure.</p> <p>Guidance</p> <p>Section 8.6.12 indicates that, in addition to the specific requirements for DBAs, consideration is given to severe accidents, so as to provide reasonable confidence that the containment will perform as credited in DEC analysis.</p> <p>For additional guidance on the design of containment structures refer to section 7.15.</p>	<p>standard conditions for the main volume of the vacuum building is 200 kg/hr (100 scfm) and for the upper chamber 6 kg/hr (3 scfm). Containment pressure is continuously monitored and periodically tested to demonstrate that the leakage requirements are being met.</p> <p>Seismic qualification is discussed in further detail in Safety Factor 3: Equipment Qualification.</p> <p>As described in the Design Management procedure [BP-PROC-00335] (clause 4.9.1) the seismic qualification process is implemented via the Bruce Power Seismic Qualification Standard [DPT-PDE-00017]. This standard describes the engineering and administrative processes for preserving the seismic qualification of the systems, structures and components. It outlines the basis of qualification of Bruce B, noting in section 4.1.2 [DPT-PDE-00017] that "The original seismic qualification of the Bruce B followed the criteria of Seismic Qualification of Safety-related Systems, NK29-DG-03650-002, which invokes CSA Standards CAN3-N289.3 and N289.4. The general scope of seismic qualification is described in the Bruce B Safety Report. Bruce Power is committed to preserving seismic qualification for Bruce B in accordance with NK29-DG-03650-002."</p> <p>Design analysis demonstrated that with regard to the strength of the containment above design pressure, the concrete containment at Bruce is robust. The evaluation of concrete containment overpressure capacity for Bruce B [A. Hindy, Bruce GS B: Evaluation of Concrete Containment Overpressure Capacity -Plastic Analysis, OH-DD-85380, December 1985] demonstrated that superficial cracking would begin at 140 kPa (g) with no increase in expected leak rate. The transition from elastic to plastic behaviour occurs at</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		170 kPa (g) and at 210 kPa (g), widespread cracking would occur as the rebar yields around the pilasters. Again, no significant increase in leakage is expected at these pressures, since the cracking is not through-wall. The onset of through-wall cracking begins at 330 kPa (g), and at 380 kPa (g) there is widespread yielding of rebar. There is no structural failure up to these pressures. At 410 kPa (g), rebar failure would occur and increased leakage would occur. Despite this, aggregate interlocking at the concrete cracks is expected to maintain containment structural integrity.	
8.6.3	The containment structure shall be subject to pressure testing at a specified pressure in order to demonstrate structural integrity. Testing shall be conducted before plant operation commences and at appropriate intervals throughout the plant's lifetime.	<p>A new requirement for testing at appropriate intervals is introduced in this clause.</p> <p>The integrity of the containment system is tested by negative pressure leak rate tests on a quarterly basis, and on a positive basis at the system design pressure on a frequency prescribed by the CNSC. The Operational Safety Requirements for the Bruce B Containment System [NK29-OSR-34200-00001, R001, November 2013] describes the containment envelope and presents the safety limits and surveillance requirements for the systems and its components.</p> <p>As noted in Containment System OSRs [NK29-OSR-34200-00001, R001], the airlocks and transfer chambers are physically a part of the containment boundary. They provide access to the containment envelope without breaching the boundary. This distinctive function calls for specific monitoring, testing and corrective response requirements, in addition to those defined for the containment envelope. Operability is determined by process parameters (e.g., door seal pressure) and hardware performance measured during</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>tests (e.g., leak rate). Various components of the containment system can be tested separately to demonstrate the integrity of the system, as well as the system as a whole. Airlocks can be tested individually for leak tightness (section 6.5.4 of Part 2 of the Safety Report). The inter-space between the automatic containment isolation dampers can also be tested for leak-tightness separately for each pair of dampers. Each of the special seals noted in Part 2, Section 6.5.2.7 of the Safety Report has its individual test point and is checked on a regular basis. The operation of each pressure relief valve is tested on an annual basis by connecting the valve to a vacuum source that will lift it off its seat after sealing the pressure relief duct with sufficient water. Seals at the top of the reactor between the shield tank and the reactivity mechanisms deck can be tested by pressurizing the interspace and measuring leakage rate.</p> <p>The containment envelope includes the four Reactor Vaults, the Central Fuelling Area, the Fuelling Duct, the East Service Area, the Pressure Relief Ducts, the Pressure Relief Valve Manifold and the Vacuum Building, airlocks and transfer chambers, and extensions of containment arising from numerous piping penetrations. Bruce NGS B CSA N287.7-08 Periodic Inspection Program for Bruce B Concrete Containment Structures and Appurtenances (Excluding Vacuum Building) [NK29-PIP-21100-00001, R003, September 2014] details the periodic inspection program for visual inspection of concrete and organic containment components. Also the inspection includes containment appurtenances, i.e., airlocks/transfer chambers, dampers and penetration seals. The general philosophy used to determine the inspection/testing frequency of various containment areas and components is described in Section 4.5 Inspection</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>Frequency. The current inspection dates are listed in Appendix F. The current period between leakage rate tests at positive pressures and periodic inspections is 6 years.</p> <p>The PIP for the Vacuum Building is documented in Bruce NGS B CSA N287.7-08 Periodic Inspection Program for Bruce NGS B Vacuum Building [NK29-PIP-25100-00001, R002, September 2014]. The containment side (inside) of the Vacuum Building is normally inaccessible and will only be inspected during Vacuum Building Outages that occur to meet the Station's licence requirement. As indicated in section 4.5, the current period between inspections is 12 years.</p>	
8.6.4	<p>Leakage rate limits</p> <p>The safety leakage rate limit shall assure that:</p> <ol style="list-style-type: none"> <li>1. normal operation release limits are met</li> <li>2. AOOs and DBAs will not result in exceeding dose acceptance criteria</li> </ol> <p>The design leakage rate limit shall be:</p> <ol style="list-style-type: none"> <li>1. below the safety leakage rate limit</li> </ol>	<p>The text in item 2 under Test Acceptance Leakage Rate Limits is modified and now refers to applicable codes and standards.</p> <p>Bruce B containment design does not match the state of the art design practice in leakage rates as described in the Guidance. Bruce B containment meets the current CNSC requirements for licensing basis events, and dose acceptance criteria for DBAs.</p> <p>As described in Section 6.5.2.1 of Part 2 of the Safety Report [NK29-SR-01320-00001], the acceptance leakage rate for the containment envelope, except for the vacuum building, is set at 2% of the contained air mass per hour at 82.7 kPa(g) (12 psig). The vacuum building acceptance leakage rate is set at 2% of contained air mass per hour at 48.3 kPa(g) (7 psig). Operational targets are set at lower values. Leakage rate tests for the vacuum building and upper chamber are conducted periodically at 7 kPa(a) (1 psia). The acceptance leakage rates at metric standard conditions for the main</p>	IC




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2. as low as is practicably attainable</p> <p>3. consistent with state-of-the-art design practices</p> <p>Test acceptance leakage rate limits</p> <p>A test acceptance leakage rate shall provide the maximum rate acceptable under actual measurement tests. Test acceptance leakage rate limits shall be established for the entire containment system, and for individual components that can contribute significantly to leakage.</p> <p>The containment structure and the equipment and components affecting the leak tightness of the containment system shall be designed to allow leak rate testing:</p> <p>1. for commissioning, at the containment design pressure</p> <p>2. over the service lifetime of the reactor, in accordance with applicable codes and standards</p>	<p>volume of the vacuum building is 200 kg/hr (100 scfm) and for the upper chamber 6 kg/hr (3 scfm). The Containment Leakage Rate Measurement System Design Manual [NK29-DM-34200-010, R0] presents the design requirements and system description.</p> <p>The re-pressurization time calculated for the Bruce B intact containment is 45 hours, taking no credit for reverse flow function and assuming containment leakage at 3 percent volume/hr, compressed air in-leakage at 400 kg/hr. Sensitivity studies show that the re-pressurization time is 49 hours if the reverse flow function of an APRV is credited. The re-pressurization time is 82 hours if the reverse flow function is credited and more realistic, but still conservative, values of containment leakage at 2 percent volume/hr and compressed air leakage at 200 kg/hr are used (section 5.6.4.2.2 of Part 3 of the Safety Report).</p> <p>As indicated in Section 5.6.4.2.2 of Part 3 of the Safety Report, the effect of the presence of a turbulent component on the predicted containment re-pressurization times has been assessed based on the Bruce A analysis. The re-pressurization time was reduced by 7 hours for a large break LOCA scenario with the minimum re-pressurization time remaining above 39 hours.</p> <p>Further detailed information on the appropriate limits, and the basis for these limits, can be found in the Bruce B OSRs for containment [NK29-OSR-34200-00001, R001], Operational Safety Requirements For Bruce B Containment System.</p> <p>Bruce Power does not currently use the term "test acceptance limits" in defining the limits that the containment must meet to be considered operational. The licensing limits</p>	




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design shall provide ready and reliable detection of any significant breach of the containment envelope.</p> <p>Guidance</p> <p>A modern containment should be able to achieve a leakage rate less than 0.5% containment air mass per day at the maximum containment pressure from any DBA. For example, modern designs achieve a maximum leakage rate of 0.1% to 0.5% containment air mass per day at design pressure.</p> <p>The safety leakage rate limit is the maximum leakage rate that will allow the dose acceptance criteria to be met for any AOO or DBA; the containment should be designed with a much lower leakage. Testing for compliance throughout the reactor life ensures that the design leakage rate is not exceeded.</p> <p>Additional information</p> <p>Additional information may be found in:</p>	<p>used are specified in Appendix A of the OP&amp;Ps [BP-OPP-00001, R019]. Section 21 and Appendix 21 Negative Pressure Containment System.</p> <p>During normal operation, the pressure in the containment is maintained slightly sub-atmospheric by purging to atmosphere via the unit Vault Vapour Recovery Systems. The vacuum building is isolated from the containment envelope by the closed Pressure Relief Valves (section 1.6.1 of Containment OSRs). The containment envelope (excluding the vacuum building) is maintained at all times at a slightly negative pressure -2.0 to -3.0 kPa gauge as indicated in Table 1 of Negative Pressure Containment System Design Manual [NK29-DM-34200-001, Rev. 03].</p> <p>The pressure in the main chamber in vacuum building is normally maintained between 6.9 and 10.3 kPa (Appendix 5.6 of Part 3 of the Safety Report) absolute and again monitoring of this value from the control room will readily detect any gross breach. Since the containment at Bruce A and B is always run at slightly sub-atmospheric conditions the normal operational releases from the station are via the discharge from the active ventilation system, or through controlled liquid release paths, rather than through any potential leakage of the containment structure. Operation of the Bruce Plant has been such that the releases during normal operation are at approximately 1% of the allowed release limit. The acceptable leakage rate for the containment envelope, except for the vacuum building, is set at 2% of the contained air mass per hour at 82.7 kPa(g) (12 psig) as described in section 6.5.2.1 of Part 2 of the Safety Report. The design and operational testing requirements for leakage rate are specified in Negative Pressure Containment</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>CSA Group, N287.7, In-service Examination and Testing Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, Toronto, Canada.</li> <li>CSA Group, N287.6, Pre-operational proof and leakage rate testing requirements for concrete containment structures for nuclear power plants, Toronto, Canada.</li> </ul>	<p>System Design Manual [NK29-DM-34200-001]. The leakage rate value of 2.0 percent (section 2.1.4 of Operational Safety Requirements for Bruce B Containment System, NK29-oSR-34200-00001, R001, November 2013) of the total contained mass per hour can be considered as still being below the safety limit leakage rate since the resulting doses do not actually meet the acceptance criteria limits. Currently the reference dose limits for Bruce A and B are for single and dual failure events.</p> <p>The frequency of DBA events is defined in CNSC REGDOC-2.4.1, Clause 4.2.3 as follows: design basis accidents include events with frequencies of occurrence equal to or greater than 1E-5 per reactor year but less than 1E-2 per reactor year. Thus, the limiting DBA inside containment event would be the large LOCA (4.2% of whole body dose relative to the current limit of 5 mSv). Since the proposed DBA limit in CNSC REGDOC-2.4.1 is larger than the current single failure limit, Bruce B would meet the proposed limit using the 2.0% leakage rate as the design limiting leakage rate. All current single failure events, whether inside containment or outside, would meet the proposed new limits.</p> <p>As stated in section 3.4.1.1 of Negative Pressure Containment System Design Manual [NK29-DM-34200-001, Rev. 03] containment leakage rate tests are performed to confirm that the leakage rate is less than the design value of 2.0% vol/hr of the contained mass of air per hour at 82.7 kPa(g) and Metric Standard Conditions (MSC). The analysis value used is 3.0% vol/hr at 68.9 kPa (g).</p> <p>As noted earlier, currently there is no AOO classification for Bruce B. See Section 4.4.1 for further discussion on this</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		topic.	
8.6.5	<p>The number of penetrations through the containment shall be kept to a minimum.</p> <p>All containment penetrations shall be subject to the same design requirements as the containment structure itself, and shall be protected from reaction forces stemming from pipe movement or accidental loads, such as those due to missiles generated by external or internal events, jet impact, and pipe whip.</p> <p>All penetrations shall be designed to allow for periodic inspection and testing.</p> <p>If resilient seals such as elastomeric seals, electrical cable penetrations, or expansion bellows are used with penetrations, they shall have the capacity for leak testing at the containment design pressure. To demonstrate continued integrity over the lifetime of the plant, this capacity shall support testing that is independent of determining the leak rate of the containment as a whole.</p> <p>Guidance</p>	<p>The changes introduced in the text of this clause are mostly clarifications. Also there was a sentence deleted from 8.6.4 under Leak Rate Testing "to the extent practicable, penetrations are to be designed to allow individual testing of each penetration".</p> <p>As described in Part 2, Section 3.2.1 of the Safety Report, the reactor containment envelope encloses only those components and systems that are closely associated with the reactor and the coolant. This results in a reduced volume of containment. The balance of the equipment is located outside the containment envelope, where maintenance is more convenient, and in some cases can be undertaken with the reactor on power. However, this compact arrangement means that a larger number of penetrations through the containment envelope are required. Design details about the types of containment penetrations are provided in Section 6.5.2.7 of Part 2 of the Safety Report.</p> <p>The Design Guide, Containment Provisions for Extensions of the Containment Envelope [NK29-DG-03650-006, Rev. 004, December 2005] documents the design requirements for extensions of the containment boundary for normal operation, maintenance and post-accident operation. Power and Control Cable Penetrations Design Guide (NK29-DG-29-57600-2 R00) sets the design requirements for control and power cable penetrations in reactor building wall. As stated in section 2 of the design guide, electrical cables enter the containment areas through steel penetrations embedded in the concrete containment walls. To prevent leakage from the containment in the event of a LOCA, each cable is sealed by</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	Keeping the number of penetrations through the containment to a minimum should consider the need for separation and redundancy, and be consistent with modern designs.	<p>a cable gland. These glands, known as primary seals, are mounted on plates welded to the external face of the penetrations. In addition, each cable is provided with a secondary seal mounted on plates, bolted to the internal face of the penetrations. The primary seal provides a complete blocking of the cable whereas the secondary seal provides a seal around the cable jacket. The provision of two seals allows the internal space of the penetration to be pressurized to allow for a leak detection survey to be conducted on the primary seals. This design allows overall containment pressure tests to be conducted on a less frequent basis than would be necessary with a single seal. Containment testing of a four unit station connected by the fuelling machine tunnel is a complicated procedure and costs are saved by the double seal technique. A single primary seal is also utilized for cables which enter confinement areas.</p> <p>Regarding inspection of penetrations, as discussed in Clause 8.6.3, Bruce B periodic inspection program for the containment structure and related components was developed and being implemented to comply with CSA N285.5-2008 Periodic Inspection of CANDU Nuclear Power Plant Containment Components. The Bruce B Periodic Inspection Plan (PIP) for Unit 0 and Units 5 to 8 Containment Components [NK29-PIP-03542-00001, R002, October 2015] establishes the manner by which Bruce B implements and complies with the intent of the CSA Standard N285.5-2008. It includes Periodic Inspection requirements for common systems (Unit 0) and reactor specific systems (Units 5 to 8 inclusive).</p> <p>Bruce B does not meet the requirement for leak testing at the containment design pressure of resilient seals. Bruce B was</p>	

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>not designed with testing capability for the type of penetrations referred to above. The continuous operation with containment at a slightly sub-atmospheric pressure, along with the periodic testing at lower pressure is used to determine the overall leakage of the system. Should the test requirements not be met, penetrations are among the first item to be checked as per existing operating procedures. As described in the Containment OSRs (NK29-OSR-34200-00001, R001), the overall leakage during pressure testing includes contributions from structural boundaries (e.g., cracks, caulked joints, etc.) and system penetrations (e.g., airlocks, valves dampers, etc.). The leakage through fixed seals, such as the heat transport pump seals, is included in the leakage measured during containment leak rate tests. The pump seals in particular are protected from vibration-induced damage following a loss of coolant accident by tripping the pumps on conditions that could cause excessive vibration. Leak rate testing at positive pressure requires a station shutdown, so it is performed infrequently. In the interim, periodic negative pressure tests are performed to give early indication of any deterioration. The details of the testing requirements (frequency, test conditions) are established by the relevant engineering standards (e.g., CSA N287.1). Details about inspection requirements are presented in CSA N287.7-08 Periodic Inspection Program for Bruce B Concrete Containment Structures and Appurtenances (Excluding Vacuum Building (Nk29-PIP-21100-00001, R003) and CSA N287.7-08 Periodic Inspection Program for Bruce NGS B Vacuum Building (NK29-PIP-25100-00001, R002).</p> <p>As documented in [NK21-CORR-00531-11005 / NK29-CORR-00531-11397] the Bruce B vacuum type containment</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		was not designed with testing capability for penetrations. Various components of the containment system can be tested separately to demonstrate the integrity of the system, as well as the system as a whole. Cable penetrations can be tested by pressurizing the space between the primary and secondary seals. Detailed containment test procedures are in effect. Overall containment integrity is confirmed by a positive pressure test of the entire system, during station outages, as described in Section 6.5.4 of the Safety Report [NK29-SR-01320-00001]. Containment performance is also monitored and trended via the quarterly on-power leak rate test (QLRT), which measures the leak tightness of the containment structure at negative pressure. The results of these on-power tests show that containment leakage remains well within the OP&P limit of 2%/hr at the design pressure and Metric Standard Conditions.	
8.6.6	<p>Each line of the reactor coolant pressure boundary that penetrates the containment, or that is connected directly to the containment atmosphere, shall be automatically and reliably sealed. This requirement is essential to maintaining the leak tightness of the containment in the event of an accident, and preventing radioactive releases to the environment that exceed prescribed limits.</p> <p>Automatic isolation valves shall be positioned to provide the greatest safety upon loss of actuating power.</p>	<p>The changes are editorial, i.e., to provide clarification and streamline the section; hence no change in the requirements.</p> <p>As described in Part 2, Section 6.5.2 of the Safety Report, the Bruce B containment has a number of extensions arising from numerous piping penetrations. The majority of the extensions are normally closed but some are normally open. The normally open extensions are automatically closed following the detection of high activity or high pressure inside containment thus ensuring a closed envelope is provided to contain potential activity in the event of an accident.</p> <p>In general, all manual valves that are required to be open are identified, locked open and that designation appears on the appropriate flow sheet.</p> <p>Bruce NGS B Penetrations and Extensions of the</p>	IC



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Piping systems that penetrate the containment system shall have isolation devices with redundancy, reliability, and performance capabilities that reflect the importance of isolating the various types of piping systems. Alternative types of isolation may be used where justification is provided.</p> <p>Where manual isolation valves are used, they shall be readily accessible and have locking or continuous monitoring capability.</p> <p>Reactor coolant system auxiliaries that penetrate containment</p> <p>Each auxiliary line that is connected to the reactor coolant pressure boundary, and that penetrates the containment structure, shall include two isolation valves in series. The valves shall be normally arranged with one inside and one outside the containment structure.</p> <p>Where the valves provide isolation of the heat transport system during normal operation, both valves shall be normally in the closed position.</p>	<p>Containment Envelope Report No. 83185 documents two lists (i.e., Containment Penetration List and Extensions of the Containment Envelope Information List) that include penetration identification, location, type of penetration, identification of systems and lines passing through the penetration and details concerning the extensions of the containment envelope. Section 2 of the report presents the embedded part number, which identifies the penetration, the location and location drawing number; whereas section 3 provides the details related to extensions of the containment envelope.</p> <p>Bruce B has piping systems penetrating containment that do not have redundant isolation valves. In the 1980's, a report was prepared on containment extensions at Bruce B [Ontario Hydro D&amp;D Report 83185]. The report defined the normal containment boundary and back-up isolation points for each penetration, including PHT penetrations, if the normal containment boundary is unavailable. Thus, the second isolation points for each containment extension are clearly identified.</p> <p>Regarding the requirement for the valves providing isolation of the heat transport system during normal operation, where there are two such valves both would be closed and may be locked as standard operating practice.</p> <p>All systems, which penetrate the containment structure or are part of or are connected to the Primary Heat Transport Systems (PHTS) or Moderator systems fall within the scope of the design guide for Containment Provisions for Extensions of the Containment Envelope [NK29-DG-03650-006, Rev.04]. In section 6.2.2.3.1 it states that "to provide containment isolation, each line greater or equal to the 1 inch</p>	




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Systems directly connected to the reactor coolant system that may be open during normal operation shall be subject to the same isolation requirements as the normally closed system, with the exception that manual isolating valves inside the containment structure will not be used. At least one of the two isolation valves shall be either automatic or powered, and operable from the main and secondary control rooms.</p> <p>For any piping outside of containment that could contain radioactivity from the reactor core, the following requirements shall apply:</p> <ol style="list-style-type: none"> <li>1. The design parameters shall be the same as those for a piping extension to containment, and are subject to the requirements for metal penetrations of containment.</li> <li>2. All piping and components that are open to the containment atmosphere shall be designed for a pressure greater than the containment design pressure.</li> <li>3. The piping and components shall be housed in a confinement structure that prevents leakage of radioactivity to the environment and to adjacent structures.</li> </ol>	<p>nominal diameter that is part or connected to the PHTS pressure boundary and penetrates the containment structure "shall be provided with two isolation valves in series". For systems normally connected to containment atmosphere (Section 6.2.2.2) it states that:</p> <p>(1) normally open lines shall have "two automatic isolation valves in series shall be provided for those lines which may be open to the containment atmosphere for &gt; 1h year for normal operational purposes"</p> <p>(2) large normally closed lines (greater or equal to 1 inch) shall have "two closed isolation valves in series". Note that small (less than 1 inch) normally closed lines which are connected to unqualified closed system or normally closed system are provided with one isolation valve. The unqualified or closed system provides a barrier to release during normal operation to the system.</p> <p>(3) it is noted in Section 6.2.2.2.1 [NK29-DG-03650-006, Rev.04] that the design guide that, "where two valves are provided, preferably, one should be located inside and as close as practicable to the containment structure and one outside and as close as practicable to the containment structure to allow for maintenance on either barrier".</p> <p>The exceptions from these requirements are documented in the following design guide supplements. The Design requirements document [NK29-DM-34200-001, Rev.03] in section 2.9.4 identifies a list of applicable design guides and design guide supplements related to negative pressure containment system. This includes the rationale for why such exceptions are considered acceptable, those which relate to dual isolation are, for example:</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>4. This housing shall include detection capability for leakage of radioactivity and shall include the capability to deal safely with the leakage.</p> <p>Systems connected to containment atmosphere</p> <p>Each line that connects directly to the containment atmosphere, that penetrates the containment structure and is not part of a closed system, shall be provided with two isolation barriers that meet the following requirements:</p> <ol style="list-style-type: none"> <li>1. two automatic isolation valves in series for lines that may be open to the containment atmosphere</li> <li>2. two closed isolation valves in series for lines that are normally closed to the containment atmosphere</li> <li>3. the line up to and including the second valve is part of the containment envelope</li> </ol> <p>Closed systems</p>	<p>" DGS-29-03650-003 Containment Boundary Exemption from the dual automatic isolation valve requirement in line 33330-L11D6 as per DG-03650-6 Section 10.2.1.1.</p> <p>" DGS-29-03650-007, NPC, Vacuum System. Exemption for the dual automatic closing isolation valves requirements for IPRVs 0-3421-PRV3, 4, 15, 16.</p> <p>" DGS-29-03650-014, Containment Isolation ECI Recovery Pump. Lines (3434L42-47) connected to containment atmosphere (via L12-15) are isolated by relief valves thereby not meeting containment isolation requirements.</p> <p>" DGS-29-03650-015, NPC-Vacuum System. Lines 3422L137 and L140 do not meet dual automatic closing isolation requirements. Pneumatic valves (3422-MV181, 184, 185, 188) open when IPRVs reduce containment overpressure post LOCA, thereby not performing containment isolation function. Lines 3422-L137 and L140 do not meet Class 4 boundary considerations.</p> <p>Various pipes and ducts penetrate the containment envelope or vacuum building boundary and communicate with the protected volumes. The portions of these flow paths up to and including the redundant isolation device are called the containment extensions. Most of the extensions are closed and are simply a part of the overall containment envelope or vacuum building boundary. Some extensions are (or may be) open during normal operation and these are isolated after the accident. Potentially open flow paths communicating with the containment atmosphere are provided with automatic isolation on high pressure or high activity. As noted in</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>All closed piping service systems shall have at least one single isolation valve on each line penetrating the containment, with the valve being located outside of, but as close as practicable to, the containment structure.</p> <p>Where failure of a closed loop is assumed to be a PIE or the result of a PIE, the isolations appropriate to the system shall apply.</p> <p>Closed piping service systems whether inside or outside the containment structure which form part of the containment envelope, require no further isolation if:</p> <ol style="list-style-type: none"> <li>they meet the applicable service piping standards and codes</li> <li>they can be continuously monitored for leaks</li> </ol>	<p>Section 6.5.2.6 of Part 2 of the Safety Report [NK29-SR-01320-00001, Rev.05] there are a number of service systems which, although not necessary for the post-accident operation of the containment system, are connected to the containment envelope. These include the vault air dryers and the containment drains. The reactor vaults, the central fueling area, and the east service areas are connected to air dryer systems to recover heavy water vapour. There are six systems: one for each vault, one for the central fueling area and one for the east service area. Each system consists of a loop of ducting from the containment proper to the dryer equipment and back to the containment. The vault, central fuelling area vapour recovery system, and East Services Area Vapour recovery systems will be isolated from containment, on a high vault pressure or airborne radioactivity signal, by dual isolation dampers in the suction and discharge lines.</p> <p>The central fuelling area system has no filter bank. The exhaust is to the irradiated fuel storage bay exhaust system, is normally closed. Provisions exist for manual purging of the central fueling area via the vapour recovery system. Isolation valves are provided to allow the removal of any piece of equipment for repair and maintenance without destroying the integrity of the containment envelope. In the case of the normally open vent lines, two valves in series are provided.</p>	
8.6.7	<p>Personnel access to the containment shall take place through airlocks that are equipped with doors that are interlocked to ensure that at least one of the doors is closed during operational states, DBAs and DEC's.</p>	<p>A new requirement to account for DEC's is included in the first paragraph.</p> <p>Airlocks and transfer chambers form part of the containment boundary and provide a means for personnel and equipment access. There are 28 airlocks and 10 transfer chambers at</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Where provision is made for entry of personnel for surveillance or maintenance purposes during normal operation, the design shall specify provisions for personnel safety, including emergency egress. This requirement shall also apply to equipment air locks.</p> <p>Guidance</p> <p>Containment openings for the movement of equipment or material through the containment should be designed to be closed quickly and reliably, in the event that isolation of the containment is required.</p> <p>The need for access by personnel to the containment should be minimized. Following an accident, access to the containment for the purpose of ensuring the safety of the facility (for either short or long term) should not be necessary.</p>	<p>Bruce B. Table 3-1 lists the location and function of each airlock and transfer chamber (section 3.2.4.2 of Part 2 of the Safety Report).</p> <p>As described in section 3.2.4.2 of Part 2 of the Safety Report, the airlocks are cylindrical steel pressure vessels with one or more doors on each steel face. Transfer chambers are similar to airlocks but are constructed of reinforced concrete with steel bulkheads and doors. Except for Airlocks 3 and 21 and transfer Chamber 6, each airlock or transfer chamber has a sliding plate equalizer valve operated by a hand wheel to equalize the pressure across the door, before it is opened. There are interlocks in the airlock and transfer chamber design to prevent use of one door while the opposite door is open or if the equalizer valve is positioned so that it is venting the airlock to the side opposite that to be entered.</p> <p>All airlocks and transfer chambers, except Airlocks 3 and 21 and transfer chamber 6, have inflatable seals. The seals will not inflate unless the associated door is latched. Conversely, the seals will not deflate until the associated door is unlatched. Interlocks prevent the unlatching of a door, and thus seal deflation, unless the equalizer valve has been positioned to vent across the door being unlatched. Airlocks 3 and 21 and transfer Chamber 6 have O-ring or gasket-type seals, use manual valves for pressure equalization, and do not have interlocks. All airlocks and transfer chambers with inflatable seals are equipped with dual air receivers. Dual air receivers provide redundancy to each set of seals, with one local receiver supplying air to the outer seals, and the other to the inner seals. The air supply is from the instrument air systems, which are supplied with Class III power. There are emergency connections to permit hookup of emergency</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>bottled gas. All airlocks and transfer chambers have two personnel doors with the following exceptions:</p> <ol style="list-style-type: none"> <li>1. Airlock 2 has two equipment doors with a personnel door inset into each. The equipment doors are interlocked with the personnel doors so that doors cannot be opened at both ends simultaneously unless there is authorization to bypass the interlock.</li> <li>2. Airlock 3 has two removable bolted covers for handling tubular equipment only.</li> <li>3. Transfer Chambers 1, 2, 3, and 4 have the door arrangement described in Subsection 3.2.4.4.</li> <li>4. Transfer Chamber 6 has bulkheads only. The bulkheads are removed only for the transfer of equipment.</li> </ol> <p>All airlocks and transfer chamber doors are opened and closed manually (section 3.2.4.2 of Part 2 of the Safety Report).</p> <p>Each airlock and transfer chamber has a pressure equalization valve that allows the connection of the inner space to either the containment or service side to equalize pressure prior to opening the appropriate door. Given this connection of the inter-space to one of the sides, a single door (or single composite door) is fully capable of maintaining the containment boundary. Local leakage rate testing capability is provided to ensure seal integrity on each door. On automatically opened airlocks, an interlock mechanism is provided to ensure that the position of both doors and the pressure equalization valve does not result in a breach of containment. Each automatic operating door also has a set of limit switches to provide control room indication of door</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>position.</p> <p>Airlocks and transfer chambers are tested by being used for access on a routine basis. Because of high radiation fields, some of the airlocks are only opened when the reactor is shut down. The leak tightness of the airlocks is checked annually with the exception of airlocks AL2, AL4, AL5, AL11 and AL16, which are tested every two years. Airlocks are tested by pressurizing each airlock and transfer chamber with both doors closed and measuring the pressure rundown. Breach of containment through depletion of the seals alone or in combination with the equalizer valve position and door opening etc., is annunciated in the MCR (section 3.4.4 of Negative Pressure Containment System, NK29-DM-34200-001, Rev. 03). As described in section 6.5.4 of Part 2 of the Safety Report, each airlock can be tested individually for leak tightness.</p> <p>The pneumatic supply system of these devices includes a local accumulator tank. This tank maintains the seals inflated until an alternate gas supply (e.g., gas bottles) is manually provided following an accident that disrupts the normal gas supply.</p>	
8.6.8	The design shall provide for ample flow routes between separate compartments inside the containment. The openings between compartments shall be large enough to prevent significant pressure differentials which may cause damage to load-bearing and safety systems during AOOs, DBAs and DEC.	<p>There is a new requirement to account for DEC.</p> <p>The Bruce B Safety Report states that "containment structural integrity is assessed (Section 5.6.4.1) for peak overpressure due to ... pressure loading due to hydrogen deflagration. ... The assessment demonstrates that containment structural integrity is maintained..." (Section 5.10 of Part 3 of the Safety Report). Further details about the containment response and dose assessments are presented</p>	IC



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design of internal structures shall consider the hydrogen control strategy, and assist in the effectiveness of that strategy.</p> <p>Guidance</p> <p>Acceptable methods should be used to calculate pressure differentials and demonstrate that there will be no loss of safety function to load-bearing structures and safety systems during AOOs, DBAs and DECAs (including consideration of hydrogen). In particular, the analyses of a large LOCA, main steamline break and DBE are expected to lead to challenging conditions. Analysis assumptions should ensure that they are conservative with respect to containment pressure, compartment differential pressure and hydrogen distribution, as well as the safety functions of SSCs.</p> <p>Sufficient openings should be provided between compartments, so as to preclude potential hydrogen accumulation at dead ends. If appropriate, phenomena such as flame acceleration and standing flames should be taken into account.</p> <p>The internal structures should provide adequate</p>	<p>in Appendix 5.6 of Part 3 of the Safety Report.</p> <p>Analysis of the structural response of the concrete containment, including the contribution of deadweight, equipment, post-tensioning and operating temperature, shows that the maximum overpressure loading does not impair the global structural integrity. With the exception of some localized reinforcement yielding, the structural stresses are well within the elastic range. Due to the high redundancy of the structure, the transient nature of the overpressure load and the presence of the carbon steel liner, these local overstresses, though beyond the elastic design limits, present no concern with respect to the containment leak-tightness. Temperature transients accompanying hydrogen burns do not affect containment integrity. Similar to Bruce A the Bruce B containment has been designed with as few internal rooms as possible. There are large openings between the reactor vaults and the fuelling machine duct that allow an unimpeded path to the vacuum building. However, since this duct may contain parked fuelling machines, restrictions are in effect regarding parking arrangements in order to ensure that the containment design pressure is not exceeded for a large LOCA. For Bruce A a study was undertaken to demonstrate that the pre-heater enclosure, the only "small room" associated with the Bruce A containment structure, could survive the conditions of a break within that enclosure. The design differences between Bruce A and Bruce B for containment system are described in section 3.6 of Negative Pressure Containment System Design Manual [NK29-DM-34200-001, Units 5-8, Rev. 03].</p> <p>The containment pressure loading due to hydrogen combustion is assessed and documented in Section 5.6.2.1.3</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>return flow paths for coolant (e.g., from a postulated pipe break to the containment sump) if credited in the safety analysis. The possibility of obstruction of the flow paths by debris should be considered.</p> <p>For additional guidance on the design of internal structures refer to section 7.15.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>CSA Group, N291, Requirements for Safety-Related Structures for CANDU Nuclear Power Plants, Toronto, Canada.</li> </ul>	<p>of Part 3 of the Safety Report. Analysis is performed to demonstrate the capability of the containment structure to withstand the pressure loading from hydrogen deflagration, for hydrogen source terms derived for large break LOCA with ECIS available and with ECIS impaired cases.</p> <p>In addition, as described in Section 6.5.2.9 of Part 2 of Safety Report two separate systems are provided for mitigation of hydrogen following the low probability design basis event combinations.</p> <p>(a) Hydrogen Igniter System for mitigation of short term hydrogen generation.</p> <p>The hydrogen igniter system is provided to remove hydrogen generated in containment. Removal of this hydrogen in a controlled manner is required to prevent structural damage to the containment envelope that could result from potentially severe pressure or temperature transients associated with hydrogen combustion. The system consists of 16 igniters per unit (64 igniters per station) located in the reactor vaults and fuelling machine ducts. The igniters are automatically activated by button up signal following a LOCA and will cause any hydrogen to be burned with a minimal pressure rise in containment (section 6.5.2.9 of Part 2 of the Safety Report).</p> <p>Post-LOCA Hydrogen Ignition System Design Manual (NK29-DM-62111-0001, Rev. 01) provides further details about functional and performance requirements for this system.</p> <p>(b) Passive Autocatalytic Recombiners (PARs) for slower longer term hydrogen generation such as from radiolysis of water. PARs will provide defence in depth for</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>short term hydrogen mitigation as well</p> <p>Radiolysis of water from the fission product decay energy constitutes the main source of hydrogen in the long term. In addition hydrogen can also be produced due to breakdown of paints or other chemicals present in the containment or due to corrosion of metals. Passive Autocatalytic Recombiner system is provided for long term hydrogen mitigation by recombining the hydrogen released with oxygen present in the containment atmosphere to reduce the risk of any deflagration or detonation from accumulated hydrogen. Passive Autocatalytic Recombiner (PAR) is a completely passive device and does not require any services or supplies. A PAR unit will automatically activate on the presence of hydrogen above the lower threshold concentration and initiate recombination to produce steam. The buoyancy driven flow will continue to draw air and hydrogen in to the unit with steam discharged from the top.</p> <p>Bruce Power has completed the installation of Passive Autocatalytic Recombiners in both Bruce A and Bruce B [NK21-CORR-00531-12654 / NK29-CORR-00531-13087].</p>	
8.6.9	<p>The design shall enable heat removal and pressure reduction in the reactor containment in operational states, DBAs and DEC's. Systems designed for this purpose shall be treated as part of the containment system, and are capable of:</p> <p>1. minimizing the pressure-assisted release of fission products to the environment</p>	<p>The change is editorial, i.e., "all plant states" are replaced with "operational states, DBAs and DEC's"; hence no change in the requirement.</p> <p>The containment system quickly reduces the containment pressure pulse to subatmospheric level following a large energy release within the containment envelope and hence minimizes uncontrolled releases to the outside environment.</p> <p>As described in Part 2, Section 6.5.2.4 of the Safety Report, the dousing system consists of an emergency water storage</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2. preserving containment integrity</p> <p>3. preserving required leak tightness</p> <p>Guidance</p> <p>The means of providing systems to remove heat and reduce pressure in the containment can vary widely between designs and may employ systems such as:</p> <ul style="list-style-type: none"> <li>• pressure suppression pools, ice condensers, vacuum chambers</li> <li>• containment coolers and fans</li> <li>• sump or in-containment water cooling systems used as part of a LOCA recirculation</li> <li>• passive containment cooling</li> <li>• containment spray or dousing systems</li> <li>• free volume inside the reactor building</li> <li>• containment venting through filters or scrubbers</li> </ul> <p>Pressure and energy management equipment</p>	<p>tank below the ceiling of the vacuum building and a system of spray headers. The tank and headers are interconnected with a vacuum chamber, and if the main vacuum building pressure rises 26.9 kPa (3.9 psi) above the upper vacuum chamber pressure, water is discharged from the emergency water storage tank. The cylindrical concrete water storage tank is open to the building atmosphere. It has a gross capacity of 10 902 m<sup>3</sup> (385 000 ft<sup>3</sup>). It is filled by the fire protection system pumps at 151.5 L/s (2000 lpm). After an accident or, if for any other reason the water is discharged to the floor of the building, it can be returned by means of the emergency storage system pumps. The function of the dousing system is to condense any steam discharged into the vacuum building, to cool the steam and air mixture in the building and thus limit any pressure rise. The dousing system is part of the Containment system that has an overall reliability of 1E-3 a/a (section 3,8 of NK29-DM-34200-004). As specified in section 3.5 of the Design Manual for Water Spray System [NK29-DM-34200-004], The structure and piping are designed to DBE Cat. A so that the water spray system remains functional following a design basis earthquake. Since there are no working components for dousing, the dousing function in effect is Category B.</p> <p>As described in the Emergency Water Storage System Design Manual [NK29-DM-34200-003, Rev. 007], the emergency water storage system is a part of the negative pressure containment system and provides the emergency water required for the vacuum building spray dousing system. The functions of this system are to:</p> <p>" Return recovery floor water to the storage tank.</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>credited in DBAs is treated as part of the containment system. For example, if credited, fan motors should be designed for operation in post-accident combustible gas conditions.</p> <p>For DEC's, all heat sources should be considered, including combustion of gases, metal-water reactions and the formation of solid solutions (including eutectics). The design should ensure that the heat removal capacity is consistent with analysis of containment conditions.</p> <p>Air systems (such as instrument air and breathing air) should be reliably isolated after a postulated initiating event that requires containment isolation, in order to prevent containment over-pressurization and to reduce combustion and explosion effects.</p>	<p>" Recirculate the water in the storage tank.</p> <p>" Drain the vacuum duct seal water back to the storage tank.</p> <p>" Provide make up water to the system.</p> <p>" Monitor and control the temperature of the water.</p> <p>" Direct recovery floor water to the station waste management system.</p> <p>" Monitor water level on the recovery floor.</p> <p>" Supply backup water to the PHT system via the emergency coolant injection system.</p> <p>The critical measurements for the emergency water storage system are duplicated. These measurements are assigned to either channel N or channel P. Indications and controls are located in the vacuum building basement on panel 60710 PL826. Indications of emergency water storage tank level and vacuum building water recovery floor level are provided on the main control room panel 66100 PL18C. In addition, indication is provided in the emergency water and power supply building on panel 63420 PL1750 (section 8.1 of NK29-DM-34200-003, Rev. 007). This design manual [NK29-DM-34200-003, Rev. 007] describes the facilities and applications of the emergency water within the vacuum building and basement areas.</p> <p>As described in section 6.5.2.8 of Part 2 of the Safety Report) heat removal from containment is provided by a number of coolers. The main coolers in each reactor vault have four axial fans and 10 main air-to-water heat exchangers. In addition, each vault has six wall mounted coolers. The main</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		and the wall mounted coolers both utilize Class III power. The main coolers are seismically qualified, and are connected to the emergency power and water supply. The central fuelling area has its own four air coolers. They remove heat discharged from the fuelling machines when they are parked in the central fuelling area. Each of the four fuelling machine rooms has one air cooler to cool room air. The coolers normally maintain the containment atmosphere below 40°C. The vault cooling system performs a long-term containment function following a LOCA by providing sufficient heat removal capacity to assist in maintaining the integrity of the containment envelope.	
8.6.10	<p>The design shall provide systems to control the release of fission products, hydrogen, oxygen, and other substances into the reactor containment, as necessary, to:</p> <ol style="list-style-type: none"> <li>1. reduce the amount of fission products that might be released to the environment during an accident</li> <li>2. prevent deflagration or detonation that could jeopardize the integrity or leak tightness of the containment</li> </ol> <p>The design shall also:</p>	<p>There are no changes to the requirement.</p> <p>According to [NK21-CORR-00531-11005 / NK29-CORR-00531-11397] for both Bruce A and B, controls do not exist to prevent ingress of compressed air and other non-condensable gases into containment following an accident. This gap is addressed procedurally by the Abnormal Incidents Manual (AIM) [NK29-AIM-03600.1, Rev. 056] procedures to direct the operating staff to valve out all instrument air on non-incident units when they are cold and depressurized. On the accident unit there are procedures available to valve out as much of the unnecessary instrument air as possible, for example to close the north side instrument air valve to the vault. Thus the intent of this requirement is met through alternate methods.</p> <p>As described in Part 2, Section 6.5.2.10 of the Safety Report, the emergency filtered air discharge system is operated in the long-term mode following a LOCA or other Design Basis Accidents, to keep the containment pressure below</p>	IC


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>1. provide isolation of all sources of compressed air and other non-condensable gases into the containment atmosphere following an accident</p> <p>2. ensure that, in the case of ingress of non-condensable gas resulting from a PIE, containment pressure will not exceed the design limit</p> <p>3. provide isolation of compressed air sources to prevent any bypass of containment</p>	<p>atmospheric and to allow for a controlled and monitored release of fission products from containment. The system consists of two 100% filters and blowers plus ductwork and isolation dampers. Each filter contains a de-mister, heater, prefilter, upstream HEPA filter, charcoal filter and downstream HEPA filter. Air is drawn from the vacuum building, and the exhaust monitored by the post accident radiation monitoring system, prior to being released to the atmosphere via the system stack. A recirculation line enables predischage monitoring of the exhaust. An alternate exhaust path from the pressure relief valve manifold is also available.</p> <p>The emergency filtered air discharge system is housed in a building beside the south side of the vacuum building (section 3.1 of Part 2 of the Safety Report). The EFADS building is a rectangular concrete structure located on the south side of the pressure relief valve manifold. The building is not part of the containment envelope and EFADS connections to containment have normally closed isolating dampers. The two filter units are surrounded by a series of shield walls about 1 m (3.25 ft) thick. The exhaust stack reaches slightly above the roof of the vacuum building and is anchored to the structure of the stairwell, which provides access to the roof of the vacuum building. The EFADS building includes a room that houses the PARMS equipment (section 3.7.3.2 of Part 2 of the Safety Report). As described in section 11.2.1.2 of Part 2 of the Safety Report) seismically qualified supply of instrument air is also provided in the EFADS and vacuum buildings for the Post Accident Radiation Monitoring System (PARMS) and as back up for the Auxiliary Pressure Relief Valves (APRVs). This air is provided by two 100% air compressors, each with rated capacity of 6.5 L/s (13.7 scfm)</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>at 2000 kPa (g) (290 psig).</p> <p>The post- accident radiation monitoring system provides for radioisotopic analysis for noble gases, particulates and iodine emitted from the emergency filtered air discharge system. The emissions are also analyzed for tritium and gross gamma contents (section 6.5.2.11 of Part 2 of the Safety Report).</p> <p>As discussed in Clause 8.6.8, the hydrogen ignition system is provided to burn, in a controlled manner, any hydrogen generated in containment as a result of low probability design basis event combinations. The design basis event predominantly associated with significant generation of hydrogen is the dual failure case of LOCA plus loss of ECI. Burning of hydrogen in a controlled manner is required to prevent structural damage to the containment envelope that could result from potentially more severe pressure/temperature transients associated with hydrogen combustion. The system consists of 64 environmentally qualified igniters, distributed in pairs within the Reactor Vaults and the Fuelling Machines (FM) duct. The system is unitized, i.e., there are 16 igniters per reactor unit, powered directly from the unit Class II, 120 V Class II distribution system. The 120 V Class II distribution system provides uninterruptible ac power supplies to the triplicated safety systems, the dual digital computers controlling the plant and essential control power for process systems, instruments, and electric power distribution systems. This system derives its power from the 250 Vdc system through solid state dc-ac inverters. Three independent buses are provided to satisfy the requirements of the triplicated systems. Each bus is supplied by two 100 percent inverters running on "Hot Standby" arrangement with</p>	



	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>additional backup available from the Class III bus. Detailed description of the system is provided in the 120 VAC Class II System Design Manual [NK29-DM-53520-001]. The igniters are also supplied by the Emergency Power System (EPS) 120 Vac supply as described in section 2.3.2.2.12 of the Emergency Power Supply System Design Manual [NK29 DM 54300]. The system is divided into two channels for redundancy.</p> <p>The igniters are automatically activated by button-up signal following a LOCA and will cause any hydrogen produced to be burned with a minimal pressure rise in containment. The Hydrogen Igniter System may be operated manually as described in section 4.4 of the system design Manual. The Post-LOCA Hydrogen Ignition System Design Manual [NK29-DM-62111-001, Rev. 01] specifies the design requirements for this system and presents details about system operation, trips, alarms and interlocks, reliability and maintainability and the effects of malfunction of other systems.</p> <p>In addition, Bruce Power has completed the installation of Passive Autocatalytic Recombiners in both Bruce A and Bruce B [NK21-00531-12654 / NK29-CORR-00531-13087]</p> <p>As discussed in the July, 2014 progress report for FAIs 1.3.1 and 1.3.2, Bruce Power is planning on installation of containment bypass tees and containment boundary valves into the existing Emergency Filtered Air Discharge System (EFADS) piping where it exits the Vacuum Building and Pressure Relief Valve (PRV) manifold at Bruce A and B. Bruce Power successfully installed a connection point on the EFADs lines where they exit the Vacuum building and PRV Manifold at Bruce B [ NK21-CORR-00531-12209 / NK29-</p>	

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		CORR-00531-12635].	
8.6.11	<p>The coverings and coatings for components and structures within the containment shall be carefully selected, and their methods of application shall be specified to ensure fulfillment of their safety functions. The primary objective of this requirement is to minimize interference with other safety functions or accident mitigation systems in the event of deterioration of coverings and coatings. In addition, the choice of materials inside containment shall take into account the impact on post-accident containment conditions, including fission product behaviour, acidity, equipment fouling, radiolysis, fires, and other factors that may affect containment performance and integrity, and fission product release.</p> <p>Coverings and coatings shall also be selected considering the need for their removal and replacement to permit access to components for maintenance and inspection.</p> <p>Guidance</p> <p>The design authority should demonstrate that there is confidence that interference with safety functions and other safety systems by coverings, coatings, and materials is minimized. Examples</p>	<p>A new requirement for selection of coverings and coatings is added as a second paragraph.</p> <p>As part of EQ program, Bruce Power has upgraded the cables to feed selected in-containment equipment - ECI valves, and SDS2 ion chamber cabling, SDS2 flux detectors, and wall mounted vault coolers (i.e., all equipment credited for harsh environment that resides in the vault). The wiring program documents identify that the cables used will ensure specifications such that power cables have a minimum insulation resistance of 1 M Ohm at the end of the mission life, and instrumentation cables have an insulation resistance of 10 M Ohms at the end of their mission life. The rest of the cables in the vault (pressurizer heaters, bleed valves, bleed condenser and bleed cooler valves, maintenance cooling valves, fuelling machine power track, etc.) have flammable jackets.</p> <p>One material that has caused concern over the years is calcium silicate insulation covering on many systems (pressurizer, bleed condenser, etc.). The concern is that post LOCA the fibres from the calcium silicate insulation plug the ECI recovery strainer. This is being addressed by analysis at Bruce B that shows the ECI recovery flow would not be lost due to suspended fibres. The analysis of the performance of the ECI recovery sump strainer is documented in "Report for LOCA-Generated Debris Impact on Bruce B Nuclear 5-8 ECIS Recovery Operation - Stage 1 Site Assessment" [NK29-REP-34340-00006, Rev. 2, September 2002], As discussed in the report, the calcium silicate insulation on the heat transport piping located within the zones of influence of</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>include:</p> <ul style="list-style-type: none"> <li>insulation materials, corrosion products, delaminated paints and coatings that may foul ECC</li> </ul> <p>recovery flow paths or prevent operation of equipment</p> <ul style="list-style-type: none"> <li>use of rubberized sealing materials that could melt or otherwise fail, and lead either to additional containment leakage or failure of a safety-related component or system</li> <li>materials that may react under post-accident conditions to generate combustible, corrosive or poisonous gases</li> </ul> <p>Where large structures in containment are credited as heat sinks in computing post-accident pressure and temperature in containment, calculations should use consistent information about coating materials and their thermal properties.</p>	<p>a HTS piping failure considered for the Stage 1 assessment, will be replaced with fiberglass insulation to reduce the fine debris bed head-loss on the ECIS recovery strainer. In addition, the minimum assured water level in the grade level storage tank has been raised to 10 m from 9 m to reduce the recovery water temperature and thus increase its subcooling. Calculations have been completed which demonstrate the adequacy of the modified components. Using conservative assumptions of debris generation and transport to the recovery strainer, calculations based on COG test program data demonstrate that the recovery water will not flash as it passes through the debris bed and recovery strainer. These calculations have also demonstrated that even when head loss through the strainer debris bed is accounted for, there is adequate Net Positive Suction Head (NPSH) to the recovery pumps for the entire 90 day ECI mission period. Additionally, it has been confirmed that any fine fibrous debris that passes through the strainer prior to the debris bed being fully formed, will not adversely affect HX performance. An assessment of the impact the modified ECIS recovery sump grating modifications might have on containment response confirmed that there would not be any unacceptable affects.</p> <p>Iodine chemistry is complex and is strongly influenced by water chemistry, radiation and the presence of surfaces and organic materials. Since organic materials are present inside containment, organic iodides would be produced, and because some organic iodides are highly volatile, these volatile organic iodides would be the dominant airborne species inside containment.</p> <p>The carbon steel liner of the Bruce B containment is coated with inorganic zinc primer. This type of paint can remove</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>iodine from water solutions in contact with it. In integral experiments using the zinc primer, up to 70 percent of the waterborne iodine was adsorbed by the submerged painted surface. All of the steel liner is primed with the inorganic zinc primer; however, the portion located in the reactor vault is top-coated with an organic based paint, vinyl. Organic based paints were shown in integral tests to adsorb a large fraction (70 percent or more) of the total iodine.</p> <p>See Section 5.6.3.2.1.2 of Part 3 of the Safety Report [NK29-SR-01320-00002 Rev.05].</p> <p>The containment steel liner surface and welded joints are visually inspected for cracks, holes, buckling, etc. and non-destructive test are also conducted is any deterioration is detected. The acceptance criteria for steel liners and welds are provided in section 8.3 of [NK29-PIP-21100-00001].</p>	
8.6.12	<p>Following onset of core damage, the containment boundary shall be capable of contributing to the reduction of radioactivity releases to allow sufficient time for the implementation of offsite emergency procedures.</p> <p>Damage to the containment structure shall be limited to prevent uncontrolled releases of radioactivity, and to maintain the integrity of structures that support internal components.</p> <p>The ability of the containment system to withstand loads associated with design extension conditions</p>	<p>A new requirement for the complementary design features is introduced in item 4. "DECs" replaces "severe accidents" in the third paragraph.</p> <p>Bruce B containment has been shown capable of withstanding the conditions of severe accidents such that the leakage requirements are met. The consequences of the aspects of severe accidents listed in this clause are mitigated by SAMG, as discussed earlier. The current design documentation does not explicitly consider the load conditions during DEC's. Therefore, it is assessed as a gap. (Gap 1)</p> <p>Hydrogen ignition systems are provided to remove hydrogen generated in containment, in order to prevent containment structural damage as a result of potentially severe pressure</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>(DECs) shall be demonstrated in design documentation, and shall include the following considerations:</p> <ol style="list-style-type: none"> <li>1. various heat sources, including residual heat, metal-water reactions, combustion of gases, and standing flames</li> <li>2. pressure control</li> <li>3. control of combustible gases</li> <li>4. sources of non-condensable gases</li> <li>5. control of radioactive material leakage</li> <li>6. effectiveness of isolation devices</li> <li>7. functionality and leak tightness of airlocks and containment penetrations</li> <li>8. effects of the accident on the integrity and functionality of internal structures</li> </ol>	<p>or temperature transients associated with hydrogen combustion, as described in Section 6.5.2.9 of Part 2 of the Safety Report [NK29-SR-01320-00001].</p> <p>As part of the Fukushima Action items (FAI 1.3.2) Bruce Power conducted an assessment that examined the effectiveness of various Containment Filtered Venting Systems (CFVs) designs as well as the effectiveness of other options for protecting containment integrity and limiting fission product release during a multi-unit severe accident. It was concluded that the existing design capability and emergency mitigation measures are adequate to protect containment integrity and uncontrolled release, per Section 2.2 of [NK21-CORR-00531-12554 / NK29-CORR-00531-12979].</p> <p>Bruce Power has completed the installation of Passive Autocatalytic Recombiners in both Bruce A and Bruce B [NK21-CORR-00531-12654 / NK29-CORR-00531-13087].</p> <p>The addition of water to cool the fuel debris can create consequential challenges to containment, specifically: overpressurization due to the production of steam, increased hydrogen generation, and the build up of water level on the containment floor. The In Vessel Retention strategy aims to prevent corium concrete interactions (as a result of subsequent calandria vault / shield tank failure) which reduces much of the uncertainty with respect to maintaining containment integrity and represents a success of mitigating actions to recover control in the event of a severe accident. The research documents from the COG Joint Project JP 4426, CANDU Severe Accident Support to Industry - Post Fukushima, provided to the CNSC in correspondence [NK21-CORR-00531-12555 / NK29-CORR-00531-12981]</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design authority shall demonstrate that complementary design features have been incorporated that will:</p> <ol style="list-style-type: none"> <li>1. prevent a containment melt-through or failure due to the thermal impact of the core debris</li> <li>2. facilitate cooling of the core debris</li> <li>3. minimize generation of non-condensable gases and radioactive products</li> <li>4. preclude unfiltered and uncontrolled release from containment</li> </ol> <p>Guidance</p> <p>Provisions for DEC's vary greatly between designs. The claimed functionality and analysis should be supported by adequate evidence.</p> <p>The containment leakage rate in DEC's with core damage should not exceed the design leakage rate for a sufficient period to allow for the</p>	<p>concluded that "the combination of existing plant features in supporting analyses (e.g., Level 2 PSA) and various plant enhancements, either planned or under active evaluation by the utilities a part of their post- Fukushima response, provide confidence that maintaining containment integrity is an achievable goal following a severe accident. Although the original design did not include complementary design features, the subsequent analysis and consideration of the production of non-condensable gases from the concrete floor, demonstrates Bruce Power indirectly complies with this requirement.</p> <p>SAMGs are being implemented to address any non-condensable gases and radioactive products. The implementation of SAMG is addressed in Safety Factor 13.</p> <p>As described in Part 2, Section 6.5.2.10 of the Safety Report, the emergency filtered air discharge system (EFADS) is operated in the long term following a LOCA in order to maintain containment pressure sub-atmospheric and to allow a controlled and monitored release of fission products from containment. The system consists of two 100 percent filters and blowers plus ductwork and isolation valves. Each filter contains a demister, heater, pre-filter, upstream HEPA filter; charcoal filter and downstream HEPA filter. The exhaust flow is drawn from the vacuum building and is monitored by the post-accident radiation monitoring system prior to being released to the atmosphere via the system exhaust stack. A recirculation line enables pre-discharge monitoring of the exhaust flow prior to the end of the sub-atmospheric hold up period. An alternate exhaust path from the pressure relief valve manifold also is available.</p> <p>As part of Fukushima related action items implementation,</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>implementation of offsite emergency measures. This period should be demonstrated, with reasonable confidence, to be at least 24 hours.</p> <p>The design should minimize generation of combustible, non-condensable gases from corium- concrete interaction.</p> <p>Containment venting design should take into account such factors as:</p> <ul style="list-style-type: none"> <li>• ignition of flammable gases</li> <li>• generation of non-condensable gases</li> <li>• impact on filters by containment environmental conditions, such as radioactive materials, high temperature and high humidity</li> </ul> <p>Experimental or analytical evidence should be provided to demonstrate that venting will not lead to unfiltered and uncontrolled releases of radioactive materials into the environment.</p>	<p>the initiative to enhance the existing understanding of severe accident phenomena and SAMG capabilities is underway. This project has a generic component, undertaken under COG JP-4426 followed by station-specific implementation at each station. The scope of the work involves the following:</p> <ul style="list-style-type: none"> <li>o Enhancement of SAMG to include multi-unit events and IFB events.</li> <li>o Assessment of instrument and equipment survivability under severe accident and identification of equipment upgrades required.</li> <li>o Assessment of plant habitability under severe accident conditions and identification of modifications required.</li> <li>o Improvement to understanding of severe accident phenomena including containment integrity, hydrogen production, aerosol behaviour, and in-vessel retention.</li> </ul> <p>These actions are tracked through Station Specific Actions. As noted in the February 2016 update, Bruce Power provided the research documents from Candu Owners Group Joint Project 4426, CANDU Severe Accident Support to Industry - Post Fukushima, that are pertinent to containment integrity [NK21-CORR-00531-12554 / NK29-CORR-00531-12979].</p>	
8.7	<p>The design shall include systems for transferring residual heat from SSCs important to safety to an ultimate heat sink. This overall function shall be subject to very high levels of reliability during operational states, DBAs and DEC's. All systems</p>	<p>A new requirement is added to cover DEC's.</p> <p>The various heat sinks available for normal operation were discussed in Section 8.2.4 and the emergency cooling system in Section 8.5. The normal Boiler Feedwater System is backed up by the Auxiliary Boiler Feedwater system and</p>	IC



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>that contribute to the transport of heat by conveying heat, providing power, or supplying fluids to the heat transport systems, shall be therefore designed in accordance with the importance of their contribution to the function of heat transfer as a whole.</p> <p>Natural phenomena and human induced events shall be taken into account in the design of heat transfer systems, and in the choice of diversity and redundancy, both in the ultimate heat sinks and in the storage systems from which fluids for heat transfer are supplied.</p> <p>The design shall extend the capability to transfer residual heat from the core to an ultimate heat sink so that, in the event of a severe accident considered as a DEC:</p> <ol style="list-style-type: none"> <li>1. acceptable conditions can be maintained in SSCs needed for mitigation of severe accidents</li> <li>2. radioactive materials can be confined</li> <li>3. releases to the environment can be limited</li> </ol>	<p>the Emergency Water System to provide heat removal from the boilers. The Inter-Unit Feedwater tie from other operating units can also supply emergency feedwater to any unit. Power for these systems comes from the normal Class IV power backed up by Class III standby generators or, to a more limited extent, the Emergency Power Supply. Service water to heat exchanges and other components is supplied via the Unit Low Pressure Water Service System, the High Pressure Recirculating System or the Common Service Water System. Service Water Systems are described in Section 11 of Part 2 of the Safety Report.</p> <p>The Seismic and Environmental Programs that have been undertaken at Bruce B have demonstrated that the essential parts of the existing systems are capable of meeting their environmental and seismic requirements.</p> <p>In regard to potential flooding, the building site is protected from the lake by a dike, which varies up to 1.39 m (4.5 ft) above grade level, and about 2.74 m (9 ft) above the highest water level recorded at the site. This dike provides an adequate safety barrier against the most severe anticipated combination of spring run-off, wind velocity and wave action. Buoyancy due to the presence of ground water will not be a problem (section 2.2.2 of Part 2 of the Safety Report). Each of these systems has been designed with redundancy, diversity and reliability in accordance with their importance to the function of heat removal.</p> <p>As part of Fukushima enhancements and station improvements plans a project is initiated to provide complementary design features which allow emergency</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Guidance</p> <p>The safety significance and reliability requirements of the heat transfer to an ultimate heat sink should be addressed with respect to any claims made in the safety case for their availability to provide cooling for operational states, DBAs and DEC's.</p>	<p>makeup water to be added to the Bruce B heat transport system.</p> <p>Bruce Power is making short-term provisions and longer-term provisions to provide make-up water to critical systems. The short-term provisions are either complete or are underway as follows:</p> <p>" Modifications to allow emergency water to be added to boilers which for Bruce B have been completed in all units [NK21-CORR-00531-12554 / NK29-CORR-00531-12979]. The water is provided by portable Emergency Mitigating Equipment (EME). (EME) pumps which are stored in a building adjacent to the site and at a higher elevation. Bruce Power has completed all short term modifications to allow emergency water to be added to the steam generators and IFBs using EME pumps.</p> <p>" The design of an alternate method of providing makeup water to the SGs using the Inter Unit Feedwater Ties (IUFT) is complete</p> <p>" The installation of piping to allow makeup water to be added to the primary and secondary IFBs is complete at Bruce A and Bruce B.</p>	
8.8	<p>The design shall include an emergency heat removal system (EHRS) which provides for removal of residual heat in order to meet fuel design limits and reactor coolant boundary condition limits.</p> <p>If the design of the plant is such that the EHRS is</p>	<p>A new requirement is introduced for the EHRS to function during DEC's, if required.</p> <p>Bruce A and B design does not provide this fifth (special) safety system, as these requirements were intended for new build NPPs. For Bruce B the emergency heat removal function is provided by the Emergency Water System, the Shutdown Cooling System and the Maintenance Cooling System (Gap 1). A redundancy and diversity assessment of</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>required to mitigate the consequences of a DBA, then the EHRS shall be designed as a safety system. There shall be reasonable confidence that the EHRS will function during DEC's, if required.</p> <p>Correct operation of the EHRS equipment following an accident shall not be dependent on power supplies from the electrical grid or from the turbine generators associated with any reactor unit that is located on the same site as the reactor involved in the accident.</p> <p>Where water is required for the EHRS, it shall come from a source that is independent of normal supplies.</p> <p>The design shall support maintenance and reliability testing without a reduction in system effectiveness below what is required by the OLCs.</p> <p>As far as practicable, inadvertent operation of the EHRS, or of part of the EHRS, shall not have a detrimental effect on plant safety.</p> <p>If the fire water supply or system components are interconnected to the EHRS, operation of one</p>	<p>these systems was performed for Bruce 1&amp;2, and it was concluded that changes to plant design and procedures are not warranted. As indicated in section 1.3.2, of Part 1 of the Safety Report [NK29-SR-01320-00001, R005] considering, Bruce B continued the basic design of the Bruce A station, the assessment is applicable to Bruce B as well.</p> <p>The Emergency Water System (EWS) is an independent, seismically qualified, manually operated Group 2 safety support system, which provides an alternate source of feedwater to the boilers to remove residual and decay heat in the event that all other supplies become unavailable. The EWS also provides emergency make-up to the Heat Transport System (HTS) and cooling water supply to the Emergency Cooling Injection (ECI) heat exchangers, reactor vault coolers, Secondary Control Area (SCA) air conditioning unit (ACU) and the primary and secondary irradiated fuel bay (PIFB and SIFB) heat exchangers. The EWS supply to the HTS pump cooling and the emergency make-up to the Air Foam Fire Protection system (AFFP) are not credited in any safety analysis and therefore not addressed in the Bruce B Emergency Water System OSR [NK29-OSR-71380-00001, R000, August 2009]. The entire EWS is located outside containment. The valves, instrumentation and controls are either located in an area protected from the harsh environment following a steam balance header failure or qualified in excess of the postulated conditions. Further details of seismic and environmental qualification are presented in the Emergency Water System (Process Design) [NK29-DM-29-71380-002, Rev. 3, December 12, 1983] sections 3.4 and 3.5 respectively. The design requirements, system operation and equipment description are provided in the Emergency Water System Design Manual – Process</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>shall not impair operation of the other.</p> <p>Guidance</p> <p>The emergency heat removal system is to provide a path to ultimate heat sink, in the case that normal heat removal capabilities are not available. The purpose of this system is to prevent events from escalating and to mitigate their consequences.</p> <p>Emergency heat removal relates to post-accident heat removal and may be provided by a number of systems, depending on circumstances:</p> <ul style="list-style-type: none"> <li>• post-LOCA heat removal may be provided by ECCS (refer to section 8.5)</li> <li>• for non-LOCA events, emergency heat removal may be through primary or secondary cooling systems</li> </ul> <p>For all means of emergency heat removal, the design should be such that all equipment is appropriately designed to function in the class of accidents for which it is credited.</p>	<p>Design [NK29-DM-29-71380-002, Rev. 3, December 19, 1983]. As described in section 6.7.1.2 of Part 2 of the Safety Report, emergency water is supplied by three vertical turbine pumps located in the Emergency Water and Power Supply Building. Two pumps are capable of supplying the maximum system demand. Each pump has a rated capacity of 504.7 L/s (6667 lgpm) at a rated head of 80.8 m (265 ft). The pump motors are supplied by the Emergency Power System. There is a tank, located at a high elevation in each unit, which is connected to the steam generators. The water from this tank flows by gravity to the steam generators once they are sufficiently depressurized. An orifice in the lines to each steam generator ensures equal flow to each generator. A simplified flow diagram of the emergency water system is shown in Figure 6-12 (Part 2 of the Safety Report). All components (pumps, piping etc.) are independent of the normal service water system. The Emergency Water and Power Supply Building is located on the west side of the powerhouse and houses part of the equipment for the emergency water system and the emergency power supply system. The emergency water system draws lake water from the adjacent Circulating Water discharge channel and supplies water to the reactor building for emergency cooling purposes (section 3.7.1 of Part 2 of the Safety Report). The EWS pumps serve all units and for each reactor unit there is emergency water tank providing water for steam generator cooling purposes until the EWS pumps have been started. The reliability and maintainability design considerations are described in section 3.6 of the Emergency Water System Design Manual (Process Design) [NK29-DM-29-71380-002, Rev. 3].</p> <p>The EWS is powered by the Emergency Power System</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>If the system credited has another role in normal operation, then the design should be such that the system will meet the requirements of a safety system when used in DBAs or DECAs. The design basis requirements for the system in this role should be provided.</p> <p>Many of the actions associated with operation of the systems credited for emergency heat removal may not be initiated automatically. When there is reliance on manual operation, the review of human factors considerations should have very high importance.</p> <p>Primary side emergency heat removal could be through normal shutdown cooling means. The design should be such that:</p> <ul style="list-style-type: none"> <li>• a means of depressurizing the primary system is provided and the means of depressurization meets the requirements of a safety system, or</li> <li>• the shutdown cooling system is capable of being operated at full primary pressure and temperature</li> </ul> <p>Passive or non-passive (e.g., natural circulation or pumped) heat removal may be used. Non-</p>	<p>(EPS), and therefore, is independent of Class IV and Class III power. During normal plant operation the system is in the poised mode and has no process function. The emergency water supply from the pumps is manually initiated for all loads except the HTS pump low speed operation for which the pump flow will be automatically established. The Emergency Water System operation is described in section 6.7.1.3 of Part 2 of the Safety Report. As described in section 6.7.2.2 of Part 2 of the Safety Report, the system has provisions to start automatically following loss of Class III power supplies or LOCA to provide uninterrupted operation of ECI recovery and PHT pumps. An overview of the limiting accidents considered for EWS design is presented in the EWS OSRs. The pumped EWS common and unit water supply flow paths are the only seismically qualified source of feed and service water to the boilers and other safety loads. Even if a unit is shutdown, EWS would eventually be required to act as an emergency heat sink in the event of a complete loss of power to the unit, either to the boilers or as makeup to the HTS. As a result, pumped EWS supply is required to be operable at all times. Pumped EWS supply to a shutdown unit may be taken out of service temporarily provided it could be returned to service before the HTS overheats. During this period the system could perform its required function and is therefore considered to be operable as specified in the EWS OSRs.</p> <p>The Emergency Heat Removal function is provided by more than one system; hence there are several ways this cool down could take place.</p> <p>During normal cooldown from the zero power hot state with Class IV power available, the main HT pumps circulate the coolant and heat is rejected through the Condenser Steam</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>passive systems require emergency power. Natural circulation systems should demonstrate the capability over the full range of applicable operating conditions.</p> <p>Secondary side emergency heat removal that relies on water being provided to the secondary side of steam generators may be provided by a separate pumped supply or by a secondary depressurization and gravity feed. The water supply should meet the requirements of a safety system.</p>	<p>Discharge Valves (CSDVs) or the Atmospheric Steam Discharge Valves (ASDVs) to cool the HT system to 177°C (350°F). Further cooldown with the HT system partially depressurized is then achieved using the Shutdown Cooling System. The shutdown cooling circuit cools the HT system from 165°C (329°F) to 90°C (194°F) or less. The system is capable of cooling the HT system to 59°C (138°F) and can be used to hold it at that temperature for an indefinite period. The shutdown cooling system is capable of cooling the HT system from the zero power hot temperature (260°C) under emergency conditions. The system uses the preheaters and main HT pumps to transfer heat from the HT system coolant to a dosed demineralized water recirculation loop. The system is shown in Figure 5-10 and the system design data are tabulated in Table 5-2 of Part 2 of the Safety Report. The shutdown cooling system consists of two 50% demineralized water to service water heat exchangers and two 100% recirculation pumps. Operation of the shutdown cooling system requires that the feedwater system be pressurized. The shutdown cooling system is part of the feedwater circuit and is designed and constructed in accordance with ASME B31.1, as is the feedwater system (section 5.1.4.1 of Part 2 of the Safety Report). The Shutdown Cooling System does not require seismic qualification as per the Seismic Qualification of Safety Related Systems Design Guide [NK29-DG-03650-002, Rev. 007]. The function of removing decay heat following a DBE is performed by other seismically systems [section 3.6 of Shutdown Cooling System Design Manual NK29-DM-2934710/63471, Rev. 01, December 13, 1983]. Only Class IV power is required for the Shutdown Cooling System because the primary heat transport pumps on Class IV are necessary for operation of the shutdown cooling system. The control and instrumentation of the</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
		<p>shutdown cooling system for Bruce B is the same as for Bruce A except for the power supply to the shutdown cooling pumps and isolating valves which has been changed from Class III to Class IV (Shutdown Cooling System Design Manual, NK29-DM-29-34710/63471 R001).</p> <p>As described in section 5.1.4.2 of Part 2 of the Safety Report the Maintenance Cooling System (MCS) is normally used for cooling the HT system to 59°C or less after the shutdown cooling system has reduced the HT system temperature to less than 90°C (194°F). It can be used to cool down the HT system from 160°C (326°F) if the Shutdown Cooling System is unavailable. Maintenance of some components (steam generators, pumps, valves) requires that the HT system be depressurized and drained to the header level. Following depressurization, the HT system can be drained to any level above the reactor headers with the decay heat being removed by the maintenance cooling heat exchanger. All heavy water drained from the HT circuit is purified before being stored. The Maintenance Cooling System is designed to withstand full HT system temperature and pressure of 318°C (605°F) and 11.3 MPa(g) (1635 psig), and is classified as a Class 1 system in accordance with Section III of the ASME Code. The system is provided with Class III power. During normal operation, the MCS is poised and isolated from the heat transport system. It is normally placed in service no sooner than 24 hours after a reactor shutdown and when the primary coolant temperature has been reduced below 90 °C using the Shutdown Cooling System. Following DBAs, the MCS may be used as a heat sink similar to its normal use. As described in the Bruce B Shutdown and Maintenance Cooling Systems OSRs [NK29-OSR-34700-00001], MCS may have to be employed sooner if the</p>	





Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>accident requires that the HTS be cooled as soon as possible to mitigate accident consequences. It may also be activated for an emergency cooldown of the HTS, should the Shutdown Cooling System be unavailable. In this mode of application the MCS can be used at more elevated HTS temperatures, attainable by cooldown via boiler steam relief to the atmosphere. Cooling water for the maintenance cooling heat exchanger is taken from the Low Pressure Service Water Supply (LPSWS). In addition to the low pressure supply to the heat exchanger provision is also made for a supply of warmer high pressure service water to prevent freezing when the maintenance cooling system is on standby. Cooling water for the maintenance cooling pumps is provided by the high pressure service water system. The MCS is designed to remain isolated from the heat transport system following a DBE. The Class 1 pressure boundary of the maintenance cooling system is designed for DBE so that pressure boundary is maintained following a Design Basis Earthquake. The Maintenance Cooling System is located below reactor header level and except for piping connecting to the heat transport system and the associated isolating valves, the system is outside containment. Double isolation is provided for all MCS lines (the maintenance cooling pumps' suction and discharge lines) which penetrate the containment. The environmental requirements for the maintenance cooling system isolating valves are specified in section 2.7 of MCS Design Manual [Maintenance Cooling System Design Manual, NK29-DM-34720-63472-001, Rev. 002]. The applicable safety analysis, safety analysis limits and surveillance requirements are documented in the operational safety requirements for Bruce B Shutdown and Maintenance Cooling Systems [NK29-OSR-34700-00001].</p>	



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>The design requirements, the reliability and maintainability design considerations, and detailed description of the Shutdown Cooling and Maintenance Cooling systems operation are provided in the associated design manuals, i.e. Shutdown Cooling System [NK29-DM-34710-63471, R001] and Maintenance Cooling System DM [NK29-DM-29-34720-63472-001, Rev. 002].</p> <p>It is noted that, although the combination of these systems provides a reliable cooldown system, they are not completely independent of each other because they share the electrical supply systems needed for their operation. Each unit has a Low Pressure Service Water (LPSW) system, which is equipped with four vertical turbine pumps located in the unit pump house. Three of these pumps are operated in parallel, with the fourth kept on standby. Of the four pumps, two are supplied from a Class III bus and the other two from a Class IV bus. If Class IV power fails, the water supply to all non-essential equipment is automatically shut off. Since one pump has sufficient capacity to meet the demand for all the essential equipment, including moderator cooling, shield cooling, vault coolers, and turbine seal oil coolers, the necessary water supply is secured at all times (section 11.1.3.1 of Part 2 of the Safety Report). The auxiliary boiler feedwater pumps and LPSW are powered by Class III, as is the Maintenance Cooling system. The control and instrumentation of the Shutdown Cooling System for Bruce B is the same as for Bruce A except for the power supply to the shutdown cooling pumps and isolating valves which has been changed from Class III to Class IV (Shutdown Cooling System Design Manual, NK29-DM-29-34710-63471 R001). The EWS is supplied with EPS. Both the MCS and SDC</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>reject their heat to the LPSW system, which is independent of the normal feedwater system. The Emergency Water System water source, should it be needed is lake water from the EWS pumps located in the Emergency Water and Power Supply Building (EWPSB) located west of Unit 5 [Emergency Water System Design Manual, (Mechanical, I&amp;C and Electrical) NK29-DM-29-71380-001, Rev. 2, September 1983].</p> <p>In addition, the systems at Bruce B that currently perform the EHRS function meet the following requirements:</p> <ul style="list-style-type: none"> <li>As systems important to safety the MCS, SDC and LPSW will have reliability targets per S-98 and OSRs that will define testing frequency. Table 1 of the Bruce B Annual Reliability Report 2015 [Enclosure 1 to NK29-CORR-00531-13197] presents the list of systems important to safety and unavailability targets, including Emergency Water System and Low Pressure Service Water System.</li> <li>While the MCS is normally used at other than full system temperature and pressure, it can cope with these under emergency conditions so inadvertent operation should not have a detrimental effect on plant safety.</li> <li>The systems that perform the function do not rely on firewater system. It is noted that automatic intermittent addition of fire protection water is required to maintain the EWS header flooded when no emergency water pumps are running as specified in Emergency Water System Design (Mechanical, I&amp;C and Electrical) [NK29-DM-29-71380-001, Rev. 2,</li> </ul>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>September 1983]. The Fire Protection (Water) System is also connected to, and could be made available to a number of emergency loads including supply to Emergency Water System in EWPSB as described in section 11.5.1.4 of Part 2 of the Safety Report. The Fire Protection Water System (NK29-DM-71410-001, R003 Fire Protection (Water) System Design Manual) presents further design details.</p> <p>Since the emergency heat removal function is provided by more than one system; it cannot be confirmed that the same function will be available during DEC's, if required. Therefore, this is assessed as a gap (Gap 2).</p>	
8.9	<p>The design shall specify the required functions and performance characteristics of each electrical power system that provides normal, standby, emergency and alternate power supplies to ensure:</p> <ol style="list-style-type: none"> <li>1. sufficient capacity to support the safety functions of the connected loads in operational states, DBAs and DEC's</li> <li>2. availability and reliability is commensurate with the safety significance of the connected loads</li> </ol> <p>The requirements of both the standby and emergency power systems may be met by a single system.</p>	<p>These are entirely new requirements. RD-337 has only Emergency Power Supply requirements.</p> <p>The design of electrical power systems is described in Section 8.2 of Part 2 of the Safety Report. The station is interconnected with Hydro One's 500 kV system via the Bruce B switchyard. The output of the turbine generators is transformed to 500 kV and connected to the switchyard by 500 kV overhead lines. These circuits are conservatively designed, with respect to tension and ice loading, to increase their reliability. The switchyard is located approximately 150 m (500 ft) from the powerhouse. The switchyard consists of a number of ring bus sections interconnected by a main bus. With this arrangement, a fault in any element will not adversely affect an adjacent element. Presently, three 500 kV transmission lines connect the station with other stations of the Hydro One eastern system. A 500 kV tie line also connects the switchyard to the Bruce A switchyard. To protect the equipment from lightning and switching voltage surges, sky wires are installed in the switchyard, and the</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Electrical power systems shall be designed to include the various modes of interaction between offsite power and onsite power. In addition, design provisions shall be established for coping with grid disturbances including conditions caused by solar flare (coronal mass ejection) events.</p> <p>The design shall specify:</p> <ol style="list-style-type: none"> <li>1. environmental and electromagnetic conditions to which electrical equipment and cables may be subjected</li> <li>2. limits on electromagnetic emissions conducted or radiated from electrical equipment</li> </ol> <p>The electrical power systems shall include appropriate protection, control, monitoring and testing facilities.</p> <p>Guidance</p> <p>A systematic approach should be followed to identify the electrical power systems needed in order to ensure that SSCs necessary to fulfill the</p>	<p>transformers are equipped with lightning arresters. The design requirements and design considerations for Bruce B electrical power system are documented in Electrical Power System Design Manual [NK29-DM-50000 R000].</p> <p>According to Section 8.3.1.1, the design criteria for station service systems are as follows:</p> <ol style="list-style-type: none"> <li>1. Not more than one unit should be lost due to a station service system fault.</li> <li>2. After the isolation of the Bruce B from the bulk electrical system, any one of the surviving units must be able to supply its own unit service load and also that of the other units through the 500 kV bus.</li> <li>3. Adequate (dual bus or better) reliability must be provided for safety and production critical loads.</li> <li>4. Voltage regulation requirements must be met.</li> <li>5. The systems must be stable under postulated fault conditions.</li> <li>6. The design must meet the requirements of all classes of power and lend itself to automatic and emergency transfer schemes.</li> <li>7. All loads associated with individual units are supplied from their respective unit supply buses and loads common to the plant are supplied from separate common supply buses.</li> </ol> <p>Both unit and common systems are divided into odd and even (A or B, for units; P, Q, etc., for common) buses, so that at least dual bus security is provided. Loads are connected so that half of any process is supplied from an odd bus and the other half from an even bus. Lower voltage level buses</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>safety functions are powered from electrical power supplies with appropriate safety classification and reliability.</p> <p>The design bases, design criteria, regulatory documents, standards, and other documents that will be used to design the electrical power systems should be specified.</p> <p>For each of the electrical power systems, the design bases include:</p> <ul style="list-style-type: none"> <li>• consideration of all modes of operation, plant states up to DEC's and all credible events that could impact the electrical power systems</li> <li>• reliability and availability targets for systems and key equipment</li> <li>• capacity and performance requirements</li> <li>• identification of all loads (i.e., the systems and equipment that require electric power to perform their safety functions) including electrical characteristics, maximum demand conditions, and safety classification</li> <li>• protective schemes and coordination of protection</li> <li>• specification of acceptable ranges of voltage and frequency for continuous operation of</li> </ul>	<p>have an odd or even designation to match their source of supply. The station service system buses are classified by their level of reliability. The odd and even concept is also applied to the cable tray systems, junction boxes, etc. The odd and even systems are physically separated as much as possible to achieve high system reliability under both normal and abnormal conditions (section 8.3.1 of Part 2 of the Safety Report).</p> <p>An adequate supply of electrical power is required for the essential safety related system (Group 1) loads that are credited to function following a station-wide loss of Class IV power, or other initiating events. Only those loads that are required for nuclear safety are addressed in Operational Safety Requirements for Bruce B Electrical Systems [NK29-OSR-53000/55000-0001 R000]. These safety related systems must be capable of providing the basic nuclear safety functions, i.e., control, cool, contain and monitor. Bruce B Electrical Systems include Class IV, Class III, Class II, and Class I electrical power supplies. There are four Standby Generators (SG) each with a rated capacity of 12.1 MW at a compressor inlet air temperature of 35°C. Following a loss of Class IV power, the SGs are started automatically to supply power to the Class III loads via the Emergency Transfer Scheme (ETS). The OSR covers the operability requirements of the mechanical/electrical hardware that needs to function following an initiating event, such as a loss of Class IV power, to satisfy the electrical power requirements ensuring that the essential safety related systems can fulfill their safety functions. This includes all buses, circuit breakers, rectifiers, inverters, converters, transformers and batteries as well as standby generators and their supply systems. For circuit breakers that supply required</p>	




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>the connected loads for each electrical power system</p> <ul style="list-style-type: none"> <li>identification of acceptable ranges for onsite and offsite transient disturbance events that could impact electrical power systems</li> </ul> <p>The design should specify the requirements for the preferred power supply (PPS) (i.e., the normal alternating current (AC) power supplies for plant electrical systems important to safety) and the plant interface with the transmission grid to reduce the potential for loss of normal AC power supplies.</p> <p>Transmission system studies should be undertaken for reasonably expected grid system conditions and disturbances to demonstrate that normal AC power supplies will not be degraded to a level that causes unnecessary challenges to safety systems, standby and emergency power supply systems. Performance criteria should be established for:</p> <ul style="list-style-type: none"> <li>unit generator performance during defined frequency and voltage excursions to ensure that generators remain connected to the electrical grid</li> <li>lightning and surge protection design provisions to protect the plant electrical distribution systems against transient over-voltage</li> </ul>	<p>loads in other OSRs (i.e., Emergency Coolant Injection (ECI) pump circuit breakers or ECI valve MCC breakers), the operability conditions and surveillance requirements for such components are covered in the applicable system OSRs.</p> <p>It is noted that there is an independent power supply system that protects against the unlikely failure of all Class III power supplies. The Emergency Power System (EPS) is intended to provide an independent and continuously available source of electric power to selected safety-related systems and components required to assist mitigation of the consequences of specific design basis events. The EPS is covered in Operational Safety Requirements for Bruce B Emergency Power Supply System [NK29-OSR-54300-00001, R000]. The EPS is environmentally and seismically qualified. The EPS system is the only power system with all its equipment seismically qualified to a Design Basis Earthquake (DBE) level [NK29-DM-54300-001, R004].</p> <p>The EPS main load list and the major equipment lists are presented in Appendix C and Appendix D respectively of the Bruce B Emergency Power Supply Design Manual [NK29-DM-54300-001, Rev. 04].</p> <p>The EPS system provides an alternate power supply to specific process and special safety system loads such as the emergency water pumps, which are required to remove the decay heat from the reactor; the ECI Recovery Pumps; Variable Frequency Power Supply (V.F.P.S.) converters; the services in the control areas, the monitoring instruments etc. (section 3.1 of NK29-DM-54300-001, Rev. 04):</p> <p>The EPS starts up automatically on receipt of a LOCA signal or sustained Under Voltage signal. Emergency mode can be</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>conditions such as switching and lightning surges</p> <p>The normal AC electrical power systems should have the capacity and capability to supply all plant electrical loads during operational states, DBAs and DEC's.</p> <p>Normal AC power supplies should be designed to:</p> <ul style="list-style-type: none"> <li>prevent deviations from normal operation</li> <li>prevent single failures from impacting more than one redundant division of electrical power supply</li> <li>avoid preventable challenges to standby and emergency systems as a result of an electrical system disturbance, transient, or upset condition (e.g., turbine-generator trip)</li> </ul> <p>Electrical power supply from the offsite power system to the onsite power system should be supplied by a minimum of two physically independent transmission lines designed and located in order to minimize the likelihood of their simultaneous failure. The safety analysis should provide information concerning offsite power circuits coming from the transmission system to the plant switchyard. A switchyard common to</p>	<p>entered manually by an operator action after an event that results in the loss of Group 1 functions and if the automatic run-up of emergency power generators (EPGs) has failed (section 2.1.1.2.2 of EPS Design Manual). Each Emergency Power Generator shall have a guaranteed continuous power rating of 4000 kW at 0.8 pf with ambient condition of 35°C (95°F) and 98.48 kPa (14.17 psia) at terminal voltage between 100 percent and 105 percent of the rated voltage of 4.16 kV (section 2.5.1.1 of EPS Design Manual). As a design requirement each emergency power generator is capable of carrying all emergency power system loads.</p> <p>The EPS system is continuously energized and is monitored in the main control room. The system is entered manually by an operator action after an event that results in the loss of Group 1 functions if the automatic run-up of EPGs has failed (section 2.1.1.2.2. of the EPS DM). The EPS distribution panels for the EPS loads for each unit are located in the SCA. A scheme of annunciation window indicates in which area a malfunction has occurred to give the operator warning of equipment failure. Independent control panels are provided to avoid controls failures affecting both EPGs (section 2.1.2 of EPS DM). The status of the handswitch (Normal/EPS) is monitored both in the local control rooms (SCA/EWPSB) and in the main control room. As described in section 8.3.11 of Part 2 of the Safety Report, Each of the Secondary Control Areas (SCA) has two Motor Control Centres (MCCs), which are each supplied from the unit 600 V Class III or 600 V EPS. They may be tied together through two normally open disconnect switches. The MCCs are normally energized from the unit 600 V Class III and on loss of this supply can be manually transferred to the 600 V EPS or to the other 600 V supply via the tie disconnect switches. All other MCCs are</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>both circuits is acceptable, but separate transmission line towers should be used. For some reactor designs, it might be sufficient to have only one offsite power connection, although this should be justified.</p> <p>Each of the plant's offsite transmission lines should have the capacity and capability to supply power to all plant electrical loads under all plant states.</p> <p>A minimum of one offsite transmission line and associated PPS should be designed to be automatically available to provide power to its associated safety divisions within a few seconds following an AOO or a DBA.</p> <p>A second PPS circuit should be designed to be available within a period of time commensurate with the requirement to support plant safety functions during AOOs and DBAs.</p> <p>For plants designed for house load operation, the normal AC power system should be designed to accommodate generator voltage and frequency transients associated with transferring from normal operation to the house load operating mode.</p>	<p>normally powered from the EPS buses. On loss of common Class III power, the MCCs are automatically re-energized when the power is restored to the EPS buses, either from the standby generator or from the emergency power generators.</p> <p>Following an event which results in the loss of the normal power supply the specified loads will be transferred automatically or manually to the EPS supply. Bruce NGS B Emergency Power Supply Design Manual [NK29-DM-54300-001, Rev. 04] details the functional and performance requirements for the system. The design limits, seismic, environmental, reliability, maintainability, periodic inspection, loading and loading combination requirements and safety requirements are described in this DM.</p> <p>The EPS reliability requirements are specified in section 2.12 of Emergency Power Supply Design Manual [NK29-DM-54300-001, Rev. 004].</p> <p>Bruce Generating Station Units 5-8 Electrical Power Systems Design Manual [NK29-DM-29-50000, Rev. 000] describes in detail the design basis for electrical power systems.</p> <p>As indicated in Section 8.6.11 As part of EQ program, Bruce Power has upgraded the cables to feed selected in-containment equipment - ECI valves, and SDS2 ion chamber cabling, SDS2 flux detectors, and wall mounted vault coolers (i.e., all equipment credited for harsh environment that resides in the vault). The wiring program documents identify that the cables used will ensure specifications such that power cables have a minimum insulation resistance of 1 M Ohm at the end of the mission life, and instrumentation cables have an insulation resistance of 10 M Ohms at the end of their mission life. The rest of the cables in the vault</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>CSA Group, N290.5, Requirements for electrical power and instrument air systems of CANDU nuclear power plants, Toronto, Canada (note: CSA N290.5 is a CANDU specific document which particularly addresses the two group design philosophy).</li> <li>IAEA, NS-G-1.8, Design of Emergency Power Systems of Nuclear Power Plants, Vienna, 2004.</li> <li>IEEE, 1050, Guide for Instrumentation and Control Equipment Grounding in Generating Stations, Piscataway, New Jersey 1996.</li> <li>IEEE, C62.23, IEEE Application Guide for Surge Protection of Electric Generating Plants, Piscataway, New Jersey, 1995.</li> <li>IEEE, 141, IEEE Recommended Practice for Electric Power Distribution for Industrial Plants, Piscataway, New Jersey, 1993.</li> <li>IEEE, 242, IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems, Piscataway, New</li> </ul>	<p>(pressurizer heaters, bleed valves, bleed condenser and bleed cooler valves, maintenance cooling valves, fuelling machine power track, etc.) will have flammable jackets.</p> <p>There is no design limit specified on electromagnetic emissions conducted or radiated from electrical equipment. Therefore, this is assessed as a gap (Gap).</p> <p>As part of the post-Fukushima actions, Bruce Power initiated an evaluation of the requirements and capabilities for electrical power for key instrumentation and control. Bruce Power has presented a phased approach to extend electrical power supply for key I&amp;C needed for accident management actions following a loss of all AC power supplied and has completed, for Bruce A and B, enhancement of plant electrical systems to provide electrical power (using AC portable generators) for key I&amp;C equipment for an indefinite period of time. Action Item 1307-3692 has been raised for Bruce Power to confirm that the deployment, connection, and operability of portable generators can be completed in less time than specified in the load shedding strategy. The information in response to AI 1307-3692 concerning the extended battery life with the load shedding strategy is provided in [NK21-CORR-00531-10560/NK29-CORR-00531-10963]. The results show that there is sufficient time to invoke the load shedding strategy and extend the battery life prior to deploying, connecting and operating the portable generators. The results also show that the load shedding will extend the battery life by 8 hours or more. Bruce Power provided additional information including plans and schedules for deployment of identified updates and demonstration that portable generators are capable of operating an extended period subject to online fuelling every 24 hours.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Jersey, 2001.</p> <ul style="list-style-type: none"> <li>IEEE, 308, IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations, Piscataway, New Jersey, 2001.</li> <li>IEEE, 387, IEEE Standard Criteria for Diesel-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations, Piscataway, New Jersey, 1995.</li> <li>IEEE, 279, IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations, Piscataway, New Jersey, 1971.</li> <li>IEEE, 665, IEEE Standard for Generating Station Grounding, Piscataway, New Jersey, reaffirmed 2001.</li> </ul>	<p>As noted in Clause 7.2, Seven 100 kW, 600 VAC generators (including one spare) have been purchased to provide power to Bruce B in the event of a blackout. The Emergency Electrical Power Upgrades for Bruce B are described in Attachment 2 of Bruce Power Progress Report No. 1 on CNSC Action Plan - Fukushima Action Items [NK29-CORR-00531-10193].</p>	
8.9.1	<p>The standby and emergency power systems shall have sufficient capacity and reliability, for a specified mission time, and in the presence of a single failure to provide the necessary power to:</p> <ol style="list-style-type: none"> <li>maintain the plant in a safe shutdown state and ensure nuclear safety in DBAs and DEC's</li> <li>support severe accident management actions</li> </ol> <p>Dedicated onsite fuel storage facilities shall have</p>	<p>New requirements are introduced after item 2 of the first paragraph.</p> <p>As described in Section 8.4 of Part 2 of the Safety Report, the station has three sources of standby and emergency power on site - the station batteries, the standby generators and the emergency power generators.</p> <p>The batteries are the lead acid type and are connected to give a nominal output voltage of 250 V DC and the capability of supplying the bus load for 40 min when there is no AC supply to the rectifiers or 20 minutes if transfers have operated to ensure safe reactor shutdown. There is one set of batteries per 250 V DC bus in the plant. Each set of batteries is housed in its own ventilated room (section 8.4.2</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>a sufficient quantity of fuel to operate standby and emergency power sources while supplying connected loads.</p> <p>The PPS to the electrical power systems shall be from offsite power or the main generator.</p> <p>The design shall:</p> <ol style="list-style-type: none"> <li>1. identify all events for which actuation of standby and emergency power sources are required</li> <li>2. specify the required start-up time and safety load energization times for standby and emergency power sources such that they are available in a time commensurate with the safety function of the connected loads</li> <li>3. specify conditions for electrical protection to trip standby and emergency power sources to protect equipment from significant failure</li> <li>4. minimize challenges to standby and emergency power supplies as a result of an electrical system disturbance or transient</li> </ol>	<p>of Part 2 of the Safety Report).</p> <p>As described in Bruce B 250 VDC Class 1 System (Units 05678) Design Manual [NK29-DM-55100, R005] to maximize security, main loads are duplicated between the two main buses in each unit and common area. In addition a third 250 VDC Class I bus is provided. The third battery system provides a power supply for the independent feeds to "C" channel loads. This includes the 120 V Class II "C" bus and the 48 VDC Class I "C" bus. Each battery (2 x 116 cells) is capable of carrying the full unit Class I and Class II loads for 20 minutes. When the two batteries are in operation, each carrying the load on its own bus, which is the usual case, the Class I and Class II loads can be maintained more than double this duration. Each battery is located in its own fireproof battery room as depicted in Figure 3-14 of Part 2 of the Safety Report. Bruce B Impairments of Special Safety Systems and Other Safety Related Systems Operating Manual [NK29-OM-03500.1, Rev, 013] provides information to the operator to determine the availability of the special safety systems and their important safety related system. The general approach in this manual is to highlight the conditions where the system is impaired to the extent that the design intent is not met and in such case the system is considered unavailable. The OM specifies the required actions including notifications are defined for such impairments. Section 5.11 of the Operating Manual presents further details. The positive and negative conductors from the batteries are Corflex armoured cables for maximum security of supply. Methods of tests and servicing of the batteries are described in the technical specifications, while the maintenance should follow manufacturer's recommendations.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>condition</p> <p>5. specify requirements for standby and emergency power supplies including all support auxiliaries and fuel supplies</p> <p>The design of the emergency power system shall take into account common-cause failures involving loss of normal power supply, and standby power supply (if applicable). The emergency power system shall be electrically independent, physically separate and diverse from normal power supply, and standby power system (if applicable).</p> <p>The standby and emergency power sources shall:</p> <p>1. preferably be initiated automatically</p> <p>2. be capable of being periodically tested under load conditions representing full load demand and full mission time</p> <p>Guidance</p>	<p>Each unit and the common area have three 250 V DC Class I buses, each fed by two 100% rated rectifiers operating in parallel from the 600 V Class III system. The rectifiers are sized such that failure of one rectifier will result in that rectifier being isolated and the load on the affected bus being carried by the second rectifier. In addition, a battery floating on each bus is capable of carrying the DC load on that bus for 40 minutes. Two of the three 250 V DC Class I buses feed the 250 V DC Class I loads, and provide feeds to the 48 V DC Class I system, the 600 V Class II system and the 120 V Class II system. There is an automatic transfer between non-duplicated 250 V DC Class I loads. The third 250 V DC Class I bus provides feeders to the 48 V DC Class I system and the 120 V Class II system (section 8.3.9 of Part 2 of the Safety Report).</p> <p>As described in section 8.4.3 of Part 2 of the Safety Report, there are four standby combustion turbine generator sets, each rated at 15 MVA and each capable of providing the Class III power requirements for safe plant shutdown of two units, plus the common loads. The standby generator sets are started automatically, following loss of Class IV power, which is the normal power supply to the critical Class III loads, or following a Loss of Coolant Accident (LOCA) with ECI initiation. Each generator set is driven by a fuel oil fed gas turbine. The fuel oil is stored in four above-ground tanks, one tank per turbine. The tanks are arranged in pairs where either member of each pair can supply fuel to either one of the two turbines associated with it. Fuel oil is fed from the tank by gravity to two pumps located in the standby generator enclosure. One of the pumps is driven by an AC motor while the other is driven by a DC motor. The DC pump is normally used when there is no AC power available, usually when</p>	




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Standby and emergency power sources should consist of complete electrical generating units including all support auxiliaries, a stored energy supply for starting and a dedicated and independent fuel supply system with onsite storage.</p> <p>The stored energy supply for starting standby or emergency power sources should have sufficient stored energy for five consecutive start attempts.</p>	<p>starting the standby generator, or as a backup pump.</p> <p>In addition as part of the reliability requirements as described in Bruce B Standby Generator Fuel Oil System Design Manual [NK29-DM-54660-R000] refilling of the tanks shall not be necessary during four days of separation of the station from the system grid with continuous base load running of the standby generators. To ensure that the station power supply is maintained, as a performance requirement, each fuel oil storage system shall have sufficient storage capacity to operate two of the four combustion turbines continuously, at 12.1 MW each at 35 °C ambient, for up to four days separation of the station from the system grid [NK29-DM-54660 R000]. Appendix E of Emergency Power Supply Design Manual [NK29-DM-54300-001] presents the considerations related to temporary portable power supply enhancements.</p> <p>The Emergency Power Supply OSRs [NK29-OSR-54300-00001, R000] describes the safety analysis limits and surveillance requirements for the system, The Emergency Power System (EPS) is a separate electrical distribution network that can provide sufficient power to Group 2 safety related systems for reactor shutdown, forced primary coolant circulation, and monitoring after a common mode incident (e.g., seismic event, fire, etc.) that has left all or portions of the normal Group 1 Class I, Class II, Class III and IV power systems non-functional. The EPS is both environmentally and seismically qualified, distinguishing it from all other electrical distribution systems in the plant. After a common mode event, a LOCA signal or a sustained under voltage signal from EPS 4.16 kV bus automatically starts the EPGs. The bus under voltage signal is time delayed in order to give the</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
		<p>Standby Generators (SGs) first opportunity to restore power to the EPS buses. If the SGs do restore power to the EPS buses, the EPGs run on no load with their output breakers open. If there is a sustained under frequency or if the voltage has not been restored within five (5) minutes, the 4.16 kV EPS buses are automatically isolated from the normal Class III power supply and EPG output breakers close when conditions permit. The limiting accidents considered for the design of the system are summarized in section 1.6.1 of the EPS OSRs. The surveillance requirements for the EPS are listed in section 2.2 of EPS OSRs and determined by the unavailability requirements for the system based on unavailability assessments. Further details are presented in Bruce B Annual Performance Report.</p> <p>Class III standby power is automatically initiated, and EPS diesels start automatically on sustained under-voltage. Following a common mode event, the EPS and hence the EPGs may be required to operate for many days or even weeks. There is a need to verify that the EPGs are capable of running for a significant length of time in order to verify their running reliability. This surveillance verifies this capability. Presently specified reliability running period is set at 4 hours (EPG1- Reliability Start Test", SST 5.2, Safety System Test, NK29-SST-09034.5, May 01, 2006). The running period is a compromise between a longer running period, which would better simulate a typical post-accident mission time, but which would use an excessive amount of fuel and result in unnecessary wear on the EPGs; and a shorter test which may not identify long term running deficiencies (section 2.2.5 of EPS OSRs [NK29-OSR-54300-00001]. The standby Class III power system is required to be tested per OP&amp;P 03.5, which requires that testing is required on any system which is</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
		<p>not normally operating but is required to function in the event of a system failure. The maintenance or testing is carried out in accordance with procedures approved by the senior operations authority, OP&amp;P 54.1 of [BP-OPP-00001, Rev.019].</p> <p>Two 100% Emergency Power Generators (EPGs) are located in the seismically qualified Emergency Water and Power Supply building (EWPSB) and have the capability to black start (from their own energy source). Each EPG is capable of supplying the required safety related station loads [EPS OSRs, NK29-ORS-54300-00001, R000]</p> <p>Table 2-1 Postulated Initiating Events of Part 3 of the Safety Report presents the list of electrical failures considered in the analysis. The heat transport system pumps are one of the major unit Class IV system loads. Failures in the Class IV power system can result in a loss of power to one or more of these pumps, with a consequent reduction of forced circulation in the heat transport system. The safety concerns associated with such events are possible impairment of fuel cooling capability and pressurization of the heat transport system which may pose a threat to the integrity of the heat transport system. Analysis of a number of postulated failures in the Class IV power system, leading to either total loss of this power supply to a unit, or partial loss of Class IV power to some HT pumps is performed to demonstrate the capability of the design to accommodate such failures. Appendix 2 Electrical System Failures summarizes the results of analysis.</p> <p>The Operational Safety Requirements for Bruce B Emergency Power Supply System are documented in [NK29-</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>OSR-54300-00001, R000].</p> <p>Currently the standby generators at Bruce B are meeting their reliability targets as documented in Table 3.3.2 of the Bruce B Annual Reliability Report 2015 [Enclosure 1 to NK29-CORR-00531-13197]. The Class III restoration times were aligned with those proposed in the revision of BP-PROC-00328, New Work Prioritization and Approval, and the Impairments Manual (NK29-OM-03500.1 Section 5.1). The Class III unavailability model was updated accordingly and a decrease in the Predicted Future Unavailability (PFU) from 7.254E-02 y/y to 3.835E-02 y/y was observed. The updated PFU is below the limit of 4.0E-02 y/y as noted in section 3.3.5.2 of [NK29-CORR- 00531-13197]. The Emergency Power System (EPS) Predicted Future Unavailability (PFU) met the target in 2015 and an increase in PFU was observed due to the update of the model with plant specific data for the reporting period as per the Annual Reliability Report 2015 [NK29-COOR-00531-13197]. The increase was observed as a result of a large increase in the failure rate of component reliability database NuREP group 274. The increase in failure rate for group 274 was due to Emergency Power Generators (EPG1 and EPG2) start failures. The list of Systems Important to Safety and Unavailability Targets is presented in Table 1 of Bruce B Annual Reliability Report 2015 [Enclosure 1 to NK29-CORR-00531-13197].</p>	
8.9.2	The design of the direct current (DC) power systems and uninterruptible AC power systems (if applicable) shall specify operating mission times when performing the intended safety functions of the connected loads and meet the capacity requirements of section 7.10.	<p>This is a new section.</p> <p>As described in Section 8.3.1.4 of Part 2 of the Safety Report, the Class II buses are AC buses fed through inverters from the Class I system and are considered uninterruptible. Class II loads are those loads which require AC supplies, but cannot tolerate the short interruptions which</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design shall include provisions for periodic testing for DC power and uninterruptible AC power supplies to confirm their capability.</p> <p>Guidance</p> <p>DC power systems</p> <p>DC power systems important to safety should be designed to be independent of the effects of DBAs to which they must respond, and be fully functional during and following such accidents.</p> <p>Redundant load groups should each have a DC power supply division consisting of one or more batteries, one or more battery chargers, distribution system, protection and isolation features.</p> <p>Each DC power supply division should be independent and physically separate from other DC divisions.</p> <p>Battery chargers should be designed to prevent transients on the AC supply from affecting the</p>	<p>can occur on the Class III system.</p> <p>The Class I buses are DC buses which are normally fed from the Class III system through rectifiers. Batteries capable of carrying the Class I loads for the short periods of time that the Class III system could be unavailable or to permit a safe plant shutdown are floating on the Class I buses. The Class I buses are thus uninterruptable. The 48 V DC buses, each fed by two converters from two 250 V batteries, are considered to be Class I. Class I loads are those loads which require DC supplies, but cannot tolerate the short interruptions which can occur on the Class III systems.</p> <p>Operational Safety Requirements for Bruce B Electrical Systems [NK29-OSR-53000-55000-00001, R000] present the safety limits, applicable analysis and surveillance requirements for Bruce B Electrical Power Systems. Since the capacity requirements and the design provisions for periodic testing as required in Clause 7.10 are not sufficiently documented, this is assessed as a gap. (Gap)</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>functioning of the DC system, and from DC transients affecting the AC supply.</p> <p>Uninterruptible AC power systems</p> <p>Uninterruptible AC power systems important to safety should be designed to be independent of the effects of design-basis accidents to which they must respond, and be fully functional during and following such accidents.</p> <p>Each division of uninterruptible AC power system should consist of:</p> <ul style="list-style-type: none"> <li>• an AC power supply and a DC power supply to an inverter</li> <li>• a separate AC power supply from the same division</li> <li>• a feature to automatically switch between the inverter output and the separate AC supply</li> </ul> <p>The electrical characteristics and requirements of the connected loads should be considered in the design so that interactions with the uninterruptible AC power system do not degrade the safety support functions of the loads supplied.</p>		

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	Uninterruptible AC power systems should be designed to prevent transients on the AC supply to the battery charger or on the DC supply to the inverter from affecting the functioning of the inverter.		
8.9.3	<p>The electrical power system design shall include provisions for mitigating the complete loss of onsite and offsite AC power. This is accomplished by the use of onsite portable, transportable or fixed power sources or offsite portable or transportable power sources, or a combination of these.</p> <p>The alternate AC power source shall be available and located at or nearby the NPP, and shall:</p> <ol style="list-style-type: none"> <li>1. be connectable to but not normally connected to the offsite or onsite standby and emergency AC power systems</li> <li>2. have minimum potential for common mode failure with offsite power or the onsite standby and emergency AC power sources</li> <li>3. be available in a timely manner after the onset</li> </ol>	<p>This is a new section. New requirements are introduced.</p> <p>Provisions for mitigating complete loss of onsite and offsite AC power have not been considered in the original design of Bruce A and B electrical power systems. Since the heat transport system pumps are one of the major unit Class IV system loads, failures in the Class IV power system can result in a loss of power to one or more of these pumps, with a consequent reduction of forced circulation in the heat transport system (Appendix 2 of Part 3 of the Safety Report). The safety concerns associated with such events are possible impairment of fuel cooling capability and pressurization of the heat transport system which may pose a threat to the integrity of the heat transport system. Analysis of a number of postulated failures in the Class IV power system, leading to either total a loss of this power supply to a unit, or partial loss of Class IV power to some HT pumps is performed to demonstrate the capability of the design to accommodate such failures. The current safety analysis as documented in Part 3 of the Safety Report does not consider events with station blackout. Therefore, this is assessed as a gap (Gap).</p> <p>Electrical modifications to allow the quick connection of portable generators to backfeed into the Qualified Power Supply (QPS) at Bruce A and into the Emergency Power</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>of a station blackout</p> <p>4. have sufficient capacity and reliability for operation of all systems required for coping with station blackout and for the time required to bring and maintain the plant in a safe shutdown state</p> <p>The design shall include provision for periodic capacity testing of the alternate power supply to confirm its capability to cope with a station blackout event.</p> <p>Guidance</p> <p>The plant's capability to maintain critical parameters (reactor coolant inventory, containment temperature and pressure, room temperatures where critical equipment is located) and to remove decay heat from irradiated fuel should be analyzed for the period that the plant is in a station blackout (SBO) condition.</p> <p>The capability of the DC systems required to monitor critical parameters and power the lighting and communication systems during an SBO should be evaluated for adequacy.</p>	<p>Supply (EPS) at Bruce B were previously completed in 2012. This modification allows key instrumentation and control equipment to remain operable for an indefinite period of time. Procurement of EME (fire trucks, portable generators, refuelling truck, portable pumps, etc.) has been completed. As indicated in the February 2016 update, a plan and schedule for procurement of emergency equipment, and the additional associated Action Item 1207-3694 have been closed [NK21-CORR-00531-10614 / NK29-CORR-00531-11007 / eDoc 4156148].</p> <p>As described in the compliance note for Clause 7.3.4 above, Bruce Power recognized the need for SAMGs to address multi-unit events including a station blackout. The site-specific SAMGs have been completed and the overall SAMG implementation is being tracked and reported to the CNSC. The SAMG updates to address multi-unit events and irradiated fuel bay events have also been completed as reported in Attachment B to [NK21-CORR-00531-12209 / NK29-CORR-00531-12635].</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
8.10.1	<p>The design shall provide for a main control room (MCR) from which the plant can be safely operated, and from which measures can be taken to maintain the plant in a safe state or to bring it back into such a state after the onset of AOOs, DBAs or DEC's.</p> <p>The design shall identify events both internal and external to the MCR that may pose a direct threat to its continued operation, and shall provide practicable measures to minimize the effects of these events.</p> <p>The safety functions that can be initiated by automatic control logic in response to an accident shall be capable of being initiated manually from the MCR.</p> <p>The layout of the controls and instrumentation, and the mode and format used to present information, shall provide operating personnel with an adequate overall picture of the status and performance of the plant and provide the necessary information to support operator actions.</p> <p>The design of the MCR shall be such that appropriate lighting levels and thermal environment are maintained, and noise levels</p>	<p>The change is for clarification only.</p> <p>As described in Section 7.1.5 of Part 2 of the Safety Report, the main control room for the four units is located in the service building. The control centre is located centrally, with respect to the four generating units, in the central service area. It is divided into the following basic areas: the main control room, four control equipment rooms, four computer rooms, two common equipment rooms, and two common fuelling machine equipment rooms. A shift supervisor's office, a work-control office, a computer auxiliaries room, emergency operating centre, a lunchroom and a washroom are also located in the control centre. The main control room contains the main control panels for the station and a fuel handling control centre. As noted in Clause 8.3.1 above, 6 (six) vertical centrally pivoted instrumented panels have been installed in the Main Control Room to prevent steam ingress. The Bruce Power Environmental Qualification Room Conditions Manual provides the single Environmental Qualification (EQ) equipment [B-STQ-03651-10001, Rev.1]. In section 4.3 this provides the Bruce Nuclear 5-8 specific normal and accident environmental conditions, including temperature, pressure, radiation, humidity, flooding and chemical conditions. Fire protection of the main control room is also enhanced. The original seismic qualification of the Bruce B followed the criteria of Seismic Qualification of Safety-related Systems, [NK29-DG-03650-002].</p> <p>All safety functions that are initiated automatically in the MCR can also be manually initiated within the SCA.</p> <p>Bruce power has completed an analysis with the objective of identifying improvement opportunities to Human Factor</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>shall be minimized in accordance with applicable standards and codes.</p> <p>The design of the MCR shall take ergonomic factors into account to provide both physical and visual accessibility to controls and displays, without adverse impact on health and comfort. This includes hardwired display panels as well as computerized displays, with the aim of making these displays as user-friendly as possible.</p> <p>Cabling for the I&amp;C equipment in the MCR shall be arranged such that a fire in the secondary control room (SCR) cannot disable the equipment in the MCR.</p> <p>The design shall provide visual and, if appropriate, audible indications of plant conditions and processes that have deviated from normal operation and that could affect safety.</p> <p>The design shall also allow for the display of information needed to monitor the effects of the automatic actions of all control, safety, and safety support system.</p> <p>The MCR shall be provided with secure</p>	<p>design guidance and where practicable, provides recommendations for the improvement of MCR and SCA design. The results of the review identified that the MCR and the SCA interfaces reviewed are approximately over 73 percent compliant with the clauses in the guidelines reviewed. Any deviations were resolved with the understanding that many represent known stereotypes that are relevant to Bruce Power or the industry in general, and changes would increase the likelihood of error. Safety Factor 12 Human Factors, review task 5.11 addresses the human machine interface for the design of the control room. Bruce Power has completed an The results of the assessment are summarized in B-REP-06700-00001, Human Factors Review against Modern Safety Standards Human Factors Engineering Summary Report.</p> <p>Per Section 11.5.2.7, of Part 2 of the Safety Report [NK29-SR-01320-00001, Rev.05] a satellite telephone system is installed to provide the unit operator with a communications link independent of the public switched telephone system, the system voice circuits, and Class IV power. The installed equipment uses the MSAT telephone system adopted by the Independent Market Operator (IMO) and interconnected utilities. IAEA GSR part 7 requires that suitable, reliable and diverse means of communication are provided (Clause 5.43). Secure communication channels is interpreted to mean suitable, reliable and diverse. This is considered a secure communication channel.</p> <p>As described in Section 7.1.1.1 of Part 2 of the Safety Report, Unit signals are continually monitored and alarm messages are provided with an audible warning when limits are exceeded. The alarm messages are presented on two</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>communication channels to the emergency support facilities and to offsite emergency response organizations, and to allow for extended operating periods.</p> <p>Guidance</p> <p>There should be sufficient displays in the MCR to monitor all safety functions.</p> <p>The design should prevent unsafe manual operations (e.g., by using a logic interlocking, depending on the plant status).</p> <p>Where safety and non-safety system are brought into close proximity, the design should keep adequate functional isolation and physical separation.</p> <p>Appropriate measures are taken, including the provision of barriers between the control rooms and the external environment, and adequate information is provided for the protection of occupants of the control room against hazards such as high radiation levels resulting from DBAs or DEC's, release of radioactive material, fire, or explosive or toxic gases.</p>	<p>alphanumeric colour video display units which may be read from most points in the control room and are logged by online printers [NK29-SR-01320-00001, Rev.5].</p> <p>There is an audible alarm that operates whenever a new alarm condition is displayed on the displays or the annunciator windows, section 7.1.5 of Part 2 of the Safety Report [NK29-SR-01320-00001, Rev.5].</p> <p>Bruce Power Severe Accident Management Guidance Plant Habitability - Summary Report, was included as Enclosure 3 of [NK21-CORR-00531-11801 / NK29-CORR-00531-12195]. This assessment followed the methodology developed by COG. The results concluded, in Section 9.1.1, that overall for single unit accidents were found to be well mitigated for both Bruce A and Bruce B with respect to dose conditions in key areas surrounding the plant. For multiunit accidents demonstrate that the UO SCA for Bruce B remains habitable until approximately 48 hours and the Main Control Rooms remain habitable for approximately 14 hours following a four-unit severe accident were Emergency Moderator Makeup (EMM) is not credited until after core collapse occurs (section 9.1.2). It is therefore concluded that, practicable measures to minimize the effects of these events has been provided in the design.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The manual initiation of safety functions provides a form of defence in depth for abnormal conditions (including the common-cause failure of the automatic control and protection systems) and supports long-term post-accident operation. Manual actuation should be provided to both system and component levels, where appropriate.</p> <p>The display and manual controls for critical safety functions initiated by operator action should be diverse from computerized automatic safety systems.</p> <p>Habitability assessments should be conducted for all control facilities. The minimum duration of habitability should be sufficient to fulfill the required safety function in each facility. Criteria for control room habitability should be established.</p>		
8.10.1.1	<p>The MCR shall contain a safety parameter display system (SPDS) that presents sufficient information on safety-critical parameters for the diagnosis and mitigation of DBAs and DEC's.</p> <p>The SPDS shall have the following capabilities:</p> <p>1. display safety-critical parameters within the full</p>	<p>The changes are editorial - "DECs" replaced "BDBAs, including severe accidents" and "emergency response facility" replaced "emergency support centre".</p> <p>As documented in [NK21-CORR-00531-11005 / NK29-CORR-00531-11397], a review of the same clause in RD-337 indicated that Bruce A/B design does not have a Safety Parameter Display System (SPDS), as required in this clause. Safety parameter information is available between Bruce Power emergency support centres on the plant LAN.</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>range expected in operational states, DBAs and DEC's</p> <p>2. track data trends</p> <p>3. indicate when process or safety limits are being approached or exceeded</p> <p>4. display the status of safety systems</p> <p>The SPDS shall be designed and installed such that the same information is made available in a secure manner to the emergency response facility.</p> <p>The SPDS shall be integrated and harmonized with the overall control room human-system interface design.</p> <p>Guidance</p> <p>The primary function of the SPDS is to serve as an operator aid in the rapid detection of abnormal conditions, by providing a display of plant parameters from which the safety status of</p>	<p>The LAN is not qualified, so it is not used as the basis for emergency decision making. Decisions are based on direct communications by satellite phone with three way communication to verify the communication. Availability of emergency communications is verified according to "Emergency Facility and Equipment Maintenance (EPP)" procedure [SEC-EPP- 00004, R008, April 19, 2012] and by operational checks at the start of an emergency.</p> <p>Section 6.6 of Part 2 of the Safety Report describes the Special Safety System Monitoring Computer (SSMC) as a computer system used to monitor the state of the shutdown and ECI systems. For each unit the system consists of a monitoring computer optically linked to nine intelligent multiplexers, one for each channel of the two shutdown systems, and one for each channel of the unit-specific parts of the emergency coolant injection system. In addition, a station safety system monitoring computer, optically linked to three intelligent multiplexers, is used to monitor the common portions of the emergency coolant injection system. The computer peripherals (display, printer, keyboard) are located in the control room adjacent to the operator's desk. The computer itself is located in the computer room, and the multiplexers are located in the shutdown system instrument rooms.</p> <p>Bruce B meets the intent of the requirement in the sense that the SSMC, the Bruce B equivalent of a Safety Parameter Display System and described above, is an add-on system that was installed to make best use of information available in the control room. It has been in operation for many years and the operators are familiar with its use and its capabilities.</p> <p>The Operational Safety Requirements for Critical Safety</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>operation may be assessed in the control room. The display system may include other functions that aid operating personnel in evaluating plant status. The design of the display system should be flexible to allow for future incorporation of advanced diagnostic concepts and evaluation techniques.</p> <p>The SPDS should display a minimum set of plant parameters or derived variables from which the safety status of the plant can be assessed. These parameters and variables relate to functions such as:</p> <ul style="list-style-type: none"> <li>• reactivity control</li> <li>• reactor core and irradiated fuel cooling</li> <li>• heat removal from primary system</li> <li>• reactor coolant system integrity</li> <li>• radioactivity control</li> <li>• containment integrity</li> </ul> <p>The SPDS should:</p> <ul style="list-style-type: none"> <li>• have sufficient availability and reliability</li> <li>• not display unreliable or invalid data and</li> </ul>	<p>Parameter Monitoring (CSPM) [NK29-OSR-60060-00001, R000, May 2010] documents the Critical Safety Parameters (CSPs) that must be maintained within limits in order to ensure that the control, cool and contain safety functions are being satisfied continually post-accident. CSPM is no longer required when it has been determined that the reactor is adequately cooled, controlled and contained. CSPM instrumentation is required to provide necessary indications following all design basis accidents. The indications are provided in the Main Control Room (MCR); and should the MCR become uninhabitable, necessary CSPM indications are provided in the Secondary Control Areas (SCAs) and the Emergency Water and Power Supply Building (EWPSB). Two independent instrument loops for each CSP or Support Parameter (SP) in both the MCR and the SCA/EWPSB are considered to provide adequate redundancy. Critical Safety Parameters are the small set of parameters whose status indicates adequacy of reactor power control, fuel cooling and containment of radioactivity. SPs provide an early warning that CSP action limits are being approached or assist in determining the appropriate restoration procedure to be followed given one or more CSPs are in an unacceptable range. The Critical Safety Parameter Monitoring (CSPM) OSRs [NK29-OSR-60060-00001, R000, May 2010] identify the operability conditions associated with CSPM instrumentation, the safety analysis limits for the CSPs and the associated surveillance requirements.</p>	




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>alarms</p> <ul style="list-style-type: none"> <li>be designed to meet the specified human factor usability requirements</li> </ul> <p>The display of abnormal operating conditions significant to safety should be distinctly different in appearance from the display depicting normal operating conditions.</p> <p>The information displayed by the SPDS display should be presented in ways that are easy for the operators to read and understand.</p> <p>The display should be designed to improve the operator's recognition, comprehension, and detection of abnormal operating states.</p>		
8.10.2	<p>The design shall provide an SCR that is physically and electrically separate from the MCR, and from which the plant can be placed and kept in a safe shutdown state when the ability to perform essential safety functions from the MCR is lost.</p> <p>The design shall identify all events that may pose a direct threat to the continued operation of the MCR and the SCR. The design of the MCR and the SCR shall be such that no event can simultaneously affect both control rooms to the</p>	<p>Very minor editorial changes are made to this section. The repetition is eliminated, e.g., some requirements are already covered in 8.10.1. No changes in the intent of the existing requirements.</p> <p>Secondary control areas for post-accident monitoring and control of the basic safety functions following incidents which would render the main control room uninhabitable. The secondary control areas are seismically and environmentally qualified. There are seismically qualified protected egress routes from the main control room to the secondary control areas. There are Secondary Control Areas in each of the four</p>	IC



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>extent that the essential safety functions cannot be performed.</p> <p>For any PIE, at least one control room shall be habitable and accessible by means of a qualified route.</p> <p>Instrumentation, control equipment, and displays shall be available in the SCR, so that the essential safety functions can be performed, essential plant variables can be monitored, and operator actions are supported.</p> <p>Safety functions initiated by automatic control logic in response to an accident shall also be capable of being initiated manually from the SCR.</p> <p>The design of the SCR shall ensure that appropriate lighting levels and thermal environment are maintained, and noise levels align with applicable standards and codes.</p> <p>Ergonomic factors shall apply to the design of the SCR to ensure physical and visual accessibility to controls and displays, without adverse impact on health and comfort. These shall include hardwired display panels as well as computerized displays</p>	<p>reactor buildings. They are physically separated and isolated from the main control room. There is also a secondary control area in the Emergency Water and Power Supply Building (EWPSB common SCA). Control devices located in any SCA override the equivalent main control room controls (section 6.7.3 of Part 2 of the Safety Report).</p> <p>There are four unitized secondary control areas for unitized loads, and a common secondary control area in the emergency water and power supply building for common loads. The main difference between the two systems is that the common SCA system is air cooled, whereas it is water cooled for the Unit SCAs (section 3.9 of SCA Design Manual, NK29-DM-63760-001].</p> <p>As described in Bruce B Secondary Control Area Design Manual Units 5678 [NK29-DM-63760-001, Rev. 004] summarizes the features of the SCAs, the support equipment and the systems, control and monitoring required to fulfill SCA requirements as defined in section 1.2 as follows:</p> <p>The SCAs contain controls and indications that enable operators to: (1) Shut down the reactors and monitor the shutdown state; (2) Effect removal of decay heat; (3) Monitor necessary neutronic and process safety parameters after the common mode incident to permit assessment of the nuclear steam supply system; (4) Maintain the containment boundary to prevent release of radioactivity to the public in excess of the allowable limit.</p> <p>The SCAs are required to remain functional during the design basis events detailed in safety design guides B-SPEC-01370-00002 such that:</p> <p>1. All the equipment located within the SCA shall be</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>that are as user-friendly as possible.</p> <p>Cabling for the I&amp;C equipment in the SCR shall be such that a fire in the MCR cannot disable the equipment in the SCR.</p> <p>The SCR shall be equipped with an SPDS similar to that in the MCR. As a minimum, this display system shall provide the information required to facilitate placing and keeping the plant in a safe shutdown state when the MCR is uninhabitable.</p> <p>The SCR shall be provided with secure communication channels to the emergency response facility and to offsite emergency response organizations.</p> <p>The SCR shall allow for extended operating periods.</p> <p>Guidance</p> <p>Sufficient controls, indications, alarms and displays should be provided in the SCR to bring the plant to a safe state, to provide assurance that a safe state has been reached and maintained,</p>	<p>seismically qualified to appropriate level</p> <p>2. All control and indicating circuits shall have the capability of being supplied from a seismically qualified emergency power supply (EPS) system</p> <p>3. Normal atmospheric conditions inside SCAs should be maintained during DBE.</p> <p>The SCA rooms are seismically qualified and the room penetrations sealed in accordance with the conditions given in Section 2.3 of Secondary Control Area Design Manual.</p> <p>All necessary actions of the safety systems that are initiated automatically can also be manually activated from the MCR. The new SCA Control Panels are standard 19 inch seismically qualified instrumentation and control cabinets. In order to optimize operator familiarity with the new control room environment it is attempted to model the layout of the safety system panels after the corresponding MCR panels. The number of controlled and monitored parameters, is reduced to only those necessary to the SCAs mission. Safety System controls on SCA panels are repeated on the corresponding Main Control Room Panels. The SCA located control overrides MCR located control and "Handswitch Off Normal" indication is provided when the SCA "takes control" away from the MCR (Secondary Control Area Design Manual, NK29-DM-63670-001].</p> <p>The safety functions initiated by automatic control logic in response to an accident can also be initiated manually from the SCA. For example the SDS2 trip logic is based on three independent channels. There are two manual trip push buttons and one test trip push button. The manual trip can be actuated from the main control room or from the secondary</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>and to provide operators with information on the status of the plant and the trends in key plant parameters.</p> <p>Suitable provisions outside the MCR should be made for transferring control to the SCR whenever the MCR is abandoned.</p> <p>There should be adequate routes through which, under emergency conditions, the operation staff from one control room can safely leave and reach another control room.</p> <p>Refer to section 8.10.1 for other applicable design guidance and expectations.</p>	<p>control area, either channel by channel or all three channels simultaneously. The trip push buttons in the secondary control area are connected directly to the trip logic, while the trips from the main control room are actuated via buffer relays. There is also a local test trip push button for each channel mounted on each SDS2 channel cubicle, which can open only one channel at a time (section 6.3.4 of Part 2 of the Safety Report). The ECI is controlled from either the main control room or the secondary control areas.</p> <p>The Unit Secondary Control Areas and the Emergency Water Power Supply Building control room are provided with three banks of five breathing air bottles. The breathing air bottles in each area are capable of supplying 2 people wearing breathing air face masks for a minimum of 24 hours (section 11.2.1.4 of Part 2 of the Safety Report). Air conditioning is provided for the control room area, several instrument rooms, secondary control area, emergency water and power supply building, common equipment rooms, offices, and the chemical laboratory. The system maintains a suitable operating environment for equipment and staff. Details of the air conditioning systems for the control room area, instrument rooms, the secondary control area, and the emergency water and power supply building control area are provided in section 11.3.3 of Part 2 of the Safety Report).</p> <p>A seismically qualified intercom system permits annunciation between the emergency water and power supply building and the four Secondary Control Areas (SCAs) and between any of the SCAs. The system operates on a party line basis such that communication between any two or more intercom stations can be established with all parties involved simultaneously. All equipment in the system is seismically</p>	

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>qualified to withstand a DBE to category B (section 11.5.2.6 of Part 2 of the Safety Report).</p> <p>The SCA does not have a SPDS. However, per section 6.7.3.2 of Part 2 of the Safety Report [NK29-SR-01320-00001, Rev.5] the secondary control areas are seismically (DBE) and environmentally qualified to provide controls and indications that enable operators to monitor the shutdown state, and monitor necessary neutronic and process parameters to permit assessment of the nuclear steam supply system. For example: the shutdown system 2 panel in the secondary control area contains displays of all SDS2 parameters with the exception of the high-neutron-power and HT low-core-differential-pressure trips (log-of-neutron-power indication, however is provided) (see Section 6.3.6).</p> <p>The instrumentation provided in the SCA is of the same safety grade and reliability as that used in the MCR. Although control devices located in any SCA override the equivalent ones in the MCR, they do not exactly duplicate them. The Design Requirements do not indicate the need for computer displays but appropriate hardwired panels mimic those in the MCR. Because all of the interfacing systems are hard wired with relay logic, the SCA and associated field panels are also hardwired with relay logic.</p> <p>Per clause 7.10, the purpose of the Bruce Power Nuclear Emergency Response Plan (NERP) [BP-PLAN-00001, R005, December 2, 2014] is to describe the concepts, structures, roles, and processes needed to implement and maintain Bruce Power's capability to prepare for and to respond to a nuclear radiological emergency. This Plan outlines the command, control, and coordination structure and activities, activation, site integration, external agency coordination,</p>	




Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>deployment of emergency resources, and emergency facilities through the use Emergency Response Procedures developed to guide effectively trained emergency response staff in emergency response and mitigation techniques. In addition to design basis events, as specified in section 4.1.1.1, this plan takes into account requirements to support a sustained response to a beyond design basis multi-unit event resulting in an extended loss of off-site power for up to 72 hours without assistance.</p> <p>As outlined in Section 2.6 in The Unit Secondary Control Areas [NK29-DM-63760-001, Rev.004] the SCAs have:</p> <p>(1) Bell telephone and PA systems: standard telephone sets with BNPD site wise telephone and PA access and coverage are provided in each SCA. These systems are seismically qualified to DBE Category 'A'.</p> <p>(2) UHF Radio system: enables the operator, via the repeater station in the emergency water and power supply building (EWPSB) common SCA to communicate with any other operating station on the site. The system is seismically qualified to DBE Category 'C'. Per the Bruce Power Nuclear Emergency Response Plan (Section 4.1.2.2, of BP-PLAN-00001) on-site and offsite teams are equipped with portable radios.</p> <p>(3) Maintenance Telephone: Each of the four SCAs are provided with maintenance telephone jacks whose cables are terminated in the in the Central Distribution Frames behind the main control room. The system is seismically qualified to DBE Category 'A'. The maintenance communication system is an internal telephone system which provides plug-in facilities at strategic locations throughout the station (see</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>Section 11.5.2.2 of Part 2 of the Safety Report).</p> <p>(4) Intercom System: Consists of a master station in the EWPSB common SCA and satellite stations in each unit SCA. The intercom system is seismically qualified to DBE Category "C" is intended for the main inter-SCA communication medium after the common mode event.</p> <p>IAEA GSR part 7 requires that suitable, reliable and diverse means of communication are provided (Clause 5.43). Secure communication channels is interpreted to mean suitable, reliable and diverse. With two independent means of communication between the SCA and the emergency management Centre (EMC) it is determined that there are adequate provisions for secure communication in the SCA.</p> <p>Bruce Power is building a state-of-the-art Emergency Management Centre (EMC) and unifying the existing Site Management and Corporate Emergency Support Centres into a single, modern command centre. This facility will be fully equipped with emergency response equipment including electronic dosimetry, satellite communication and external broadcast capability and backup power [NK21-CORR-005631-09676 / NK29-CORR-00531-10193]. As described in section 7.2.1.2 the EMC "is the primary emergency response facility that provides the mechanisms to support the operational interface with external agencies and authorities (Provinces PEOC and CNSC Headquarters Emergency Operations Centre) as well as on-site emergency response."</p> <p>As communicated to the CNSC in letter, F. Saunders to R. Lojk, "Update of Detailed Plan and Schedule for the Emergency Management Centre", November 18, 2013, NK21-CORR-00531-10902 / NK29-CORR-00531-11278 /</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		NK37-CORR-00531-02153, Bruce Power was targeting to complete the installation by no later than March 31, 2014. Emergency Management Center is now in use and available.	
8.10.3	<p>The design shall provide for onsite emergency support facilities that are separate from the plant control rooms for use by the technical support staff and emergency support staff in the event of an emergency.</p> <p>The emergency support facilities shall consist of a technical support centre (TSC) and an onsite emergency response facility. The technical support centre and the emergency response facility can be located in one place or separated.</p> <p>The emergency support facilities shall provide equipment, facilities, and communication means for trained staff to manage, control and coordinate any emergency response as well as to provide technical support to operations, emergency response organizations, and severe accident management evaluation.</p> <p>The emergency support facilities design shall ensure that appropriate lighting levels and thermal environment are maintained, and that noise levels are minimized in accordance with applicable standards and codes.</p>	<p>New text is added to this clause mostly to clarify the requirements. Second and third paragraph are new requirements.</p> <p>The Bruce B design does not provide onsite emergency support facility (or facilities) separate from the plant control rooms which include a SPDS similar to those in the MCR and in the SCA. This is considered a Gap. Design provisions for such a facility (or facilities) shall protect occupants from DBA or DEC conditions and be equipped to allow extended operation.</p> <p>As described in section 4.3.1 of Bruce Power Nuclear Emergency Response Plan [BP-PLAN-00001, R005, December 2, 2014], there are a series of facilities from which different activities are controlled, both onsite and offsite.</p> <p>Such onsite facilities include:</p> <ul style="list-style-type: none"> <li>- Main Control Room (MCR)</li> </ul> <p>The MCR is a centralized on-site facility where the site's nuclear units are monitored and operated. The facility is staffed around the clock with licensed operators. It is the first on-site facility to become involved with the response to an emergency event.</p> <ul style="list-style-type: none"> <li>- Work Control Area (WCA)</li> </ul> <p>WCA is an on-site area adjacent to the MCR. When alerted by the station PA system on-shift Operations department staff assemble at the WCA and await further instructions and</p>	Gap



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The emergency support facilities shall include secure means of communication with the MCR, SCR, and other important points in the plant, and with onsite and offsite emergency response organizations.</p> <p>The design shall ensure that the emergency support facilities:</p> <ol style="list-style-type: none"> <li>1. includes provisions to protect occupants over protracted periods from the hazards resulting from DBAs and DEC's</li> <li>2. is equipped with adequate facilities to allow extended operating periods</li> </ol> <p>The emergency response facility shall include a SPDS similar to those in the MCR and in the SCR.</p> <p>Information about the radiological conditions in the plant and its immediate surroundings, and about meteorological conditions in the vicinity of the plant, shall be accessible from the ERF.</p>	<p>assignments by the MCR supervision. WCA is activated at the discretion of the MCR supervision, for a Station Emergency and for most events that are categorized as an Abnormal Incident or higher.</p> <ul style="list-style-type: none"> <li>- Emergency Operations Centre (EOC)</li> </ul> <p>EOC is an on-site facility where the initial, centralized coordination of all on-site and off-site response activities take place. The facility is staffed by the on-shift staff. Emergency repair, radiation survey, and other teams are staged and dispatched from the EOC. EOC is activated at the discretion of the shift supervision, for a Station Emergency and at most events categorized as Abnormal Incidents and higher. The non-incident facility EOC is a back-up location for the incident facility's EOC. The EOC for Bruce B is located at the 663 foot elevation adjacent to the MCR (Section 8.2.2.2 of [BP-PLAN-00001, R005, December 2, 2014]).</p> <ul style="list-style-type: none"> <li>- Site Management Centre (SMC)</li> </ul> <p>SMC is the on-site facility where station management augmentation and technical staff assemble. Overall, site emergency response is managed from the SMC including the support to and oversight of the MCR and EOC. SMC staff is on call and the SMC is activated when requested by the Shift ERO or the ERM, and for events categorized as Abnormal Incident and higher. A back-up location for the SMC is the Corporate Emergency Support Centre (CESC). The Site Management Centre is located at the B-06 Technical Building Second Floor and provides a secondary alternate back-up facility for the Emergency Management Centre (section 4.2.6 of [BP-PLAN-00001]).</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Guidance</p> <p>The design provides emergency support facilities which include a technical support center and an onsite emergency response facility</p> <p>The TSC will provide the following functions:</p> <ul style="list-style-type: none"> <li>provide technical support and plant management to plant operation personnel during emergency conditions</li> <li>handle peripheral duties and communication not directly related to reactor manipulations in order to relieve the burden of reactor operators during emergency conditions</li> <li>prevent congestion in the control rooms</li> <li>perform emergency support functions until the emergency response facility is functional</li> </ul> <p>To facilitate the above functions, the TSC should be located as close as possible to control rooms with sufficient size to accommodate the technical support staff.</p> <p>Equipment should be provided to gather, store, and display data needed in the TSC to analyze</p>	<p>Such offsite facilities include:</p> <ul style="list-style-type: none"> <li>Emergency Management Centre (EMC)</li> </ul> <p>The EMC coordinates and manages the overall Corporate response to a nuclear emergency and is the facility that provides primary contact for communications with the Provincial, regional and local municipal government centres. It also provides support with the appropriate technical and financial resources, including the support to and oversight of the Main Control Room and Station Emergency Operations Centres (Section 4.3.1 of [BP-PLAN-00001]).</p> <ul style="list-style-type: none"> <li>Corporate Emergency Support Centre (CESC)</li> </ul> <p>The Corporate Emergency Support Centre is the primary location of the Crisis Management Team. This facility is used as the primary location where the Crisis Management Team would assemble and receive briefings from the EMC to assist in overseeing the response and engage in recovery efforts. However, the Crisis Management Team is able to assemble remotely when required. This facility also provides primary backup to the Emergency Management Centre (section 4.2.6 of BP-PLAN-00001).</p> <p>As described in Section 11.5.2 of Part 2 of the Safety Report, each of the emergency support centres have a satellite phone as backup in case of interruption of LAN or phone service. The LAN is not qualified, so it is not used as the basis for emergency decision making. Decisions are based on direct communications by satellite phone with three way communication to verify the communication. Communications with the provincial emergency centres are provided by fax using a standard form that is updated and transmitted every hour. Should this communication fail, the satellite phone is</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>plant conditions.</p> <p>The TSC should have a complete and up-to-date repository of plant records and to aid the technical analysis and evaluation of emergency conditions.</p> <p>Equipment should be provided in the emergency response facility for the acquisition, display, and evaluation of all radiological, meteorological, and plant system data pertinent to determine offsite protective measures.</p> <p>Equipment used in performing essential emergency response facility functions should be located within the emergency response facility complex. However, supplemental calculations and analytical support of emergency response facility evaluations may be provided from facilities outside the emergency response facility.</p> <p>The emergency response facility data system should be designed to achieve an appropriate level of reliability.</p> <p>The location of the emergency response facility should ensure optimum functional and reliability characteristics for carrying out its specific</p>	<p>used for direct contact with the Bruce Power emergency support centres. Availability of emergency communications is verified according to "Emergency Facility and Equipment Maintenance" procedure [SEC-EPP-00004, R008, April 19, 2012] and by operational checks at the start of an emergency.</p> <p>The Bruce B design does not provide an onsite emergency facility (or facilities) that are separate from the plant control rooms, which include a SPDS similar to those in the MCR and in the SCA. Therefore, there are no design provisions for such a facility (or facilities) to protect occupants from DBA or DEC conditions and be equipped to allow extended operation as required in this clause. This is considered a gap (Gap).</p> <p>The information from the SSMC is available only in the MCR. The SCA has the same information but is supplied through hard-wired displays. Information on the critical safety parameters would be relayed to the appropriate centres by staff from either the MCR or the SCA as appropriate. As noted in Clause 8.10.1.1, the various emergency control centres at Bruce have access to this information on any computer logged into the Plant Information (PI) system in the LAN system. The difference between this and the above requirement is the fact that it is not a dedicated or secure system (e.g., not DBA qualified).</p> <p>The radiological conditions from the plant and the area surrounding the plant are obtained by survey crews and then forwarded to the SMC and EOC. There is not automatic transmission of data from the measurement locations to the SMC or the EOC. Weather information is available to the EOC from data collected on-site and transmitted to Unit 0.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>functions.</p> <p>If the TSC and emergency response facility are located in one place, then they should be physically separate from the control rooms with adequate distance to ensure the capability of carrying out its functions.</p> <p>In the case of plants with multiple units at a site, the emergency support facilities should be demonstrated to be adequate to respond to common-cause events in multiple units.</p>	<p>This information is forwarded to the EOC by the SMC when they get it from the shift. As a backup, weather information from Kincardine is available via the Internet.</p> <p>Detailed discussion about emergency planning and arrangements is presented in Safety Factor 13.</p>	
8.10.4	<p>If operator action is required for actuation of any safety system or safety support system equipment, all of the following requirements shall apply:</p> <ol style="list-style-type: none"> <li>1. there are clear, well-defined, validated, and readily available operating procedures that identify the necessary actions</li> <li>2. there is instrumentation in the control rooms to provide clear and unambiguous indication of the necessity for operator action</li> <li>3. following indication of the necessity for</li> </ol>	<p>A major change is introduced in item 3 regarding operator actions, i.e., it used to be 15 minutes and 30 minutes. Alternative times were allowed in RD-337; however this sentence no longer exists.</p> <p>As demonstrated in Part 3 of the Safety Report, the safety analyses have shown that for the most reactivity accidents, SDS1 can keep the reactor subcritical for at least 15 minutes, before operator action is required. This is consistent with the current CNSC guidance of 15 minutes for actions initiated in the MCR (Section 4.4.4.5 Guidance for operator action of CNSC REGDOC-2.4.1). Operator actions assumed in Part 3 of the Safety Report are 15 minutes for actions inside the control room and 30 minutes for actions outside the control room. These assumptions are clearly not aligned with the proposed values for new plants; however they are consistent with the guidance of CNSC REGDOC-2.4.1 and CSA 290.1.</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>operator action inside the control rooms, there are at least 30 minutes available before the operator action is required</p> <p>4. following indication of the necessity for operator action outside the control rooms, there is a minimum of 1 hour available before the operator action is required</p> <p>For automatically initiated safety systems and control logic actions, the design shall facilitate backup manual initiation from inside the appropriate control room.</p> <p>Guidance</p> <p>The design should ensure that no failure of monitoring or display systems will influence the functioning of other safety systems.</p> <p>The available time before operator action can be credited should be counted from the receipt of an unambiguous indication of a potential accident (typically an alarm) and includes diagnostic time.</p> <p>The time available to perform the actions should</p>	<p>The Abnormal Incidents Manual [NK29-AIM-03600.1, Rev. 056] provides well-defined and validated procedures for handling accident situations.</p> <p>The complete list of operator actions called for in the safety analyses is given in Tables 1-1 through 1-10 of Section 1.3 of Part 3 of the Safety Report. In general, the majority of the indications come from equipment in the control room. Some come from field locations depending upon the accident scenario. For each accident scenario identified in the tables, the credited operation action time, the unambiguous indicators that inform the operator of the accident, and the station operating context in which the accidents occur are presented [NK29-SR-01320-00002, R005].</p> <p>All necessary actions of the safety systems that are initiated automatically can also be manually activated from the MCR. The new SCA Control Panels are standard 19 inch seismically qualified instrumentation and control cabinets. In order to optimize operator familiarity with the new control room environment it is attempted to model the layout of the safety system panels after the corresponding MCR panels. The number of controlled and monitored parameters, are reduced to only those necessary to the SCAs mission. Safety System controls on SCA panels are repeated on the corresponding Main Control Room Panels. The SCA located control overrides MCR located control and "Handswitch Off Normal" indication is provided when the SCA "takes control" away from the MCR (Secondary Control Area Design Manual, NK29-DM-63670-001]. Additional details are provided in Section 8.10.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>be based on the analysis of the plant response to AOOs and DBAs, using realistic assumptions. The time required for operator action should be based on a human factors engineering analysis of operator response time, which (in turn) is based on a documented sequence of operator actions. Uncertainties in the analysis of time required are identified and assessed. An adequate time margin should also be added to the analyzed time.</p> <p>If operator action is required for actuation of any safety function, other than meeting the requirements of this regulatory document, the analysis should also demonstrate that:</p> <ul style="list-style-type: none"> <li>• there is sufficient time available for the operator to perform the required manual action</li> <li>• the operator can perform the actions correctly and reliably in the time available</li> </ul> <p>The sequence of actions should use only alarms, controls, and displays that would be available in locations where the tasks will be performed and should be available in all scenarios analysed.</p> <p>A preliminary validation should be conducted, to provide independent confirmation to the</p>	<p>As described in Appendix A of the Secondary Control Area Design Manual [NK29-DM-63760-001, Rev. 004] the controls for the start up and operation of the portable generators are local to the portable generators. The portable generators will not annunciate operational issues in the MCR and/or SCA rooms. The operation of portable generators shall be monitored by staff.</p> <p>Operator actions in Part 3 of the Safety Report are assumed to be 15 minutes for actions inside the control room and 30 minutes for actions outside the control room. These assumptions clearly do not meet the proposed values for new plants but they are consistent with the guidance of CNSC REGDOC 2.4.1 and CSA 290.1. Therefore, it is assessed as a gap (Gap).</p>	



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design


File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>validity of the estimated “time available” and “time required” for human actions. The preliminary validation results should support the conclusion that the time required, including margin, to</p> <p>perform individual steps and the overall documented sequence of manual operator actions are reasonable, realistic, repeatable, and bounded by the initial analysis.</p> <p>An integrated system test should also be conducted, to validate the manual actions credited in the safety analysis, using a full-scale simulator. Tasks conducted outside the control room should be included in the integrated system validations.</p> <p>Where justified, alternative action times may be used. The alternative action times should make due allowance for the complexity of the action to be taken, and the time needed for activities such as diagnosing the event and accessing the field location.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"><li>• ANSI/ANS, 58.8, Time Response Design</li></ul>		



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Criteria for Safety Related Operator Actions, La Grange Park, Illinois, 2008.</p> <ul style="list-style-type: none"> <li>• CSA Group, N290.4, Requirements for Reactor Control Systems of Nuclear Power Plants, Toronto, Canada.</li> <li>• CNSC, G-225, Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills, Ottawa, Canada, 2001, or successor document.</li> <li>• IEC, 60964, Nuclear Power Plants - Control Rooms – Design, Geneva, 2009.</li> <li>• IEC, 60965, Nuclear Power Plants - Control Rooms - Supplementary Control Points for Reactor Shutdown Without Access to the Main Control Room, Geneva, 2009.</li> <li>• NEI 99-03, Control Room Habitability Assessment Guidance, Washington, D.C., 2001.</li> <li>• U.S. NRC, NUREG-0696, Functional Criteria for Emergency Response Facilities, Washington, D.C., 1981.</li> <li>• U.S. NRC, Regulatory Guide 1.196, Control Room Habitability at Light-Water Nuclear Power Reactors, Washington, D.C., 2003.</li> </ul>		
8.11	The design shall include provisions to treat liquid and gaseous effluents in a manner that will keep the quantities and concentrations of discharged contaminants within prescribed limits, and that will	<p>A new requirement for the design to minimize the regeneration of radioactive and hazardous waste is introduced.</p> <p>As described in Section 13 of Part 2 of the Safety Report, the</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>support application of the ALARA principle.</p> <p>The design of the NPP shall minimize the generation of radioactive and hazardous waste. The design shall also include adequate provision for the safe onsite handling and storage of radioactive and hazardous wastes, for a period of time consistent with options for offsite management or disposal.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>• CNSC, P-290, Managing Radioactive Waste, Ottawa, Canada, 2004.</li> </ul>	<p>radioactive waste management system provides facilities that allow the station operators to limit radioactive emissions to the required target levels for each significant effluent route, while the station is within its expected range of operating conditions. Design and operation of the active waste treatment facilities are governed by the derived release limits, which are given in Part 1, Section 1.4 of the Safety Report.</p> <p>Five basic steps are used in the management of radioactive wastes, depending on their nature and activity level:</p> <ol style="list-style-type: none"> <li>1. Holding of radioactive isotopes, for natural decay.</li> <li>2. Dilution and emission of liquid and gaseous active wastes in the respective plant effluent streams in a controlled and monitored process.</li> <li>3. Treatment of liquids and gases to remove the radioactive materials, prior to release to the environment or to volume reduce and solidify for storage as radioactive waste.</li> <li>4. Containment and temporary storage of solids in facilities within the plant buildings.</li> <li>5. Transport of solid wastes is contracted to licenced disposal facilities.</li> </ol> <p>The management of solid waste is described in Section 13.2 of Part 2 of the Safety Report. Dry solid wastes, collected throughout the station on a daily basis, are nominally classified as radioactive or non-radioactive depending on the area from which they originate. Typically, non-radioactive and likely clean wastes come from Zones 1 and 2, while radioactive wastes come from Zone 3. Wastes are taken by cart to the waste handling facility located in Unit 5 for activity monitoring, final classification, and temporary storage. Dry</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>radioactive wastes are separated into four processing categories, for reasons of volume reduction, and transferred for processing (such as incineration, compaction, baling and metal melt) and/or storage at licensed and contracted disposal facilities. Non-radioactive wastes are either landfilled or packaged for recycling. Non-radioactive wastes are transferred daily to OPG's WWMF waste operations for incineration, volume reduction and landfill on BNPD site.</p> <p>The management of liquid waste is described in Section 13.3 and management of gaseous waste in Section 13.4 of Part 2 of the Safety Report [NK29-SR-01320-0001, R005].</p> <p>Bruce Power's Environmental Safety Management program [BP-PROG-00.02, R009] requires that all hazardous materials in the plant and on the site be identified so that their impact on the environment can be assessed. Thus, all of the hazardous material can be identified as required by this clause for any future hazards analyses. In addition as discussed in Section 4.7.4.3 Hazardous Wastes of this program the Hazardous Waste Management and Disposal Requirements [BP-PROC-00773, R002, November 27, 2014] provides the requirements for compliance with applicable Federal, provincial, and municipal regulations. This is in conjunction with corporate requirements affecting the generation, handling, storage, and disposal of hazardous waste. The Environmental Evaluation of Hazardous Materials procedure [DPT-ENV-00013] provides a guideline for performing environmental evaluations of the actual and potential impact of use of specific hazardous materials at the facility. This procedure is under revision with new title and purpose. The intent of the evaluation is to ensure materials used have the smallest environmental footprint possible.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>Conventional and Hazardous Waste Management Program [BP-PROC-00888 [R001, November 2015] specifies duties performed to maintain the program. Radioactive waste management is governed by BP-PROC-00878 [R000, August 2013].</p> <p>Active Liquid Waste management is governed by:</p> <ul style="list-style-type: none"> <li>" BP PROC 00029, Bruce Power Waste Acceptance Criteria, Active Liquid Effluent</li> <li>" NK29 OM 79210, Active Liquid Waste Handling</li> <li>" NK29 OM 79220, Active Liquid Waste Treatment</li> <li>" BP PROC 00107, OPG Waste Acceptance Criteria for Radioactive Waste</li> </ul> <p>A review of the same clause in RD-337 indicated the requirement for adequate provisions of on-site handling and storage of waste for a period of time consistent with options for off-site management or disposal is not applicable, as Bruce Power does not own an on-site radioactive waste facility. The WWMF operated by OPG is located on the Bruce site [NK21-CORR-00531-11005 / NK29-CORR-00531-11397].</p>	
8.11.1	<p>To ensure that emissions and concentrations remain within prescribed limits, the design shall include suitable means for controlling liquid releases to the environment in a manner that conforms to the ALARA principle.</p> <p>This shall include a liquid waste management</p>	<p>There are no changes in the requirement.</p> <p>Liquid wastes fall into the categories effluent, sanitary, and chemical liquid wastes (including aqueous and organic liquids). Effluent meeting certificate of approval requirements and provincial water quality standards generally leave the station through the condenser cooling water duct (section 13.3.1 of Part 2 of the Safety Report).</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	system of sufficient capacity to collect, hold, mix, pump, test, treat, and sample liquid waste before discharge, taking expected waste and accidental spills or discharges into account.	<p>Sanitary wastes go to the Bruce Site sewage processing plant. Both of these streams are routinely sampled and analyzed. Liquid effluents from systems that are potential sources of activity are also monitored (section 13.3.1 of Part 2 of the Safety Report). Waste organic liquids (e.g., oils and solvents), and waste aqueous liquids are sampled and monitored for radioactivity. Non-radioactive chemical liquid waste is disposed of offsite at a licensed facility. These liquid wastes are processed as necessary and removed from the station by a licensed hazardous waste disposal company. Waste turbine governing fluid is dewatered and recycled when practical.</p> <p>The liquid waste management system at Bruce Power meets this requirement. Waste containing an appreciable amount of heavy water will be retained for reclamation. Waste collected in the low activity collection tanks is sampled and analyzed for gross gamma activity, tritium and Carbon 14. If the radioactivity concentration is below the permissible limit, the waste is discharged to the condenser cooling water duct. If the concentration is higher than the allowed limit, the waste is pumped to the high activity collection tanks. As a backup to the sampling procedure, there is a liquid effluent activity monitor in the discharge line. The active liquid waste treatment system equipment consists of filters for the removal of suspended and dissolved solids from the liquid wastes. The transfer tank contents are recirculated through the active liquid waste treatment system. When sampling indicates that the transfer tank activity is acceptable, the contents are discharged to the condenser cooling water duct via the active liquid waste handling system discharge.</p> <p>There is a closed recirculation system for purifying the water</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		from each fuel storage bay. Normally there is no overflow or discharge from the systems but there are lines to permit discharging bay water to the active liquid waste collection system. In the purification systems, the exhausted resins from the ion exchangers are sluiced with bay water or high pressure water to storage. The sluice water is directed to the active liquid waste collection tanks [Section 13.3.4 of Part 2 of the Safety Report].	
8.11.2	<p>The design shall include gaseous waste management systems capable of:</p> <ol style="list-style-type: none"> <li>controlling all gaseous contaminants so as to conform to the ALARA principle and ensure that concentrations remain within prescribed limits</li> <li>collecting all potentially active gases, vapours, and airborne particulates for monitoring</li> <li>passing all potentially active gases, vapours, and airborne particulates through pre-filters, absolute filters, charcoal filters, or high efficiency particulate air filters where applicable</li> <li>delaying releases of potential sources of noble gases by way of an off-gas system of sufficient capacity</li> </ol>	<p>There are no changes in the requirement.</p> <p>As described in Section 13.4.1 of Part 2 of the Safety Report, all active or potentially active gases, vapours, or airborne particulates that originate in the station are filtered, and any release to the atmosphere is monitored. In areas such as the reactor vaults, where there is a probability of continuous activity release to the building atmosphere, a closed ventilation system recirculates the air through a system of High Efficiency Particulate Air (HEPA) filters, and dryers. HEPA filters remove particulate and dryers remove heavy water.</p> <p>A small amount of air is exhausted through the pressure balance dryer and the active exhaust system to maintain the vault at a slightly sub-atmospheric pressure. This and other potentially contaminated air, such as from the fuel storage bays, service areas, and active laboratories, are also filtered and monitored before discharge to the atmosphere.</p> <p>The vacuum building main vacuum pump discharges through the primary fuel storage bay active exhaust system.</p> <p>The station has an off-gas system designed to provide continuous on-line treatment of the noble gas contaminated</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design shall provide a ventilation system with an appropriate filtration system capable of:</p> <ol style="list-style-type: none"> <li>1. preventing unacceptable dispersion of all airborne contaminants within the plant</li> <li>2. reducing the concentration of airborne radioactive substances to levels compatible with the need for access to each particular area</li> <li>3. keeping the level of airborne radioactive substances in the plant below prescribed limits, applying the ALARA principle in normal operation</li> <li>4. ventilating rooms containing inert or noxious gases without impairing the capability to control radioactive releases</li> </ol> <p>Guidance</p> <p>Radiological zones may be established in the NPP design, according to the potential contamination hazards in each area. The ventilation system should be designed such that any air movement between various zones, due to</p>	<p>air stream from irradiated fuel transfer machine mechanism and the heat transport D2O collection tank. The off-gas system is designed to delay the release of radioactive noble gases to achieve a decontamination factor of 40 for the process streams. This system is not the release path after an accident. In that case, release from containment is isolated and decay of short-lived fission product gases occurs before release through the EFADS filters. This system however has never been used. The station relies on dilution as a result of discharge through unaffected units as its way of controlling release of noble gases. The only part of the off-gas management system requiring operator action is the PHT bleed condenser degassing stream for each unit. The bleed condenser is degassed routinely during startup to remove non-condensable gases and during operation if the accumulation of gases starts to interfere with bleed condenser operation. As depicted in Figure 13-5, when the bleed condenser is degassed, the gases pass through a high pressure recirculating-water cooled condenser, which collects any condensate. The gases then flow through a filter, pressure reducing coils, and subsequently to the vault vapour recovery system (section 13.4.2 of Part 2 of the Safety Report).</p> <p>The Bruce B design includes powerhouse unit ventilation system, service building ventilation system and miscellaneous building ventilation system (Section 11.3.2 of Part 2 of the Safety Report). The primary objectives of the ventilation systems are to remove heat from various buildings; to provide general ventilation to all areas; to minimize cross contamination between zones of least contamination and zones of increasing contamination and to minimize release of any radioactivity into the atmosphere to</p>	





Rev Date: September 20, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00


Article No.	Clause Requirement	Assessment	Compliance Category
	pressure difference, takes place from an area of lower contamination to an area of higher contamination. Recirculation of air within one zone or room may be permitted.	<p>below the permissible limit.</p> <p>The Powerhouse Ventilation System is described in section 11.3.2.1 of Part 2 of the Safety Report. The station, exclusive of the containment envelope, has four identical ventilation systems, each serving one unit. Since no physical barrier exists between the zones of least contamination (turbine hall and turbine auxiliary bay) and those of increasing contamination (reactor auxiliary bay), the system induces unidirectional airflow from least contaminated to more contaminated areas (from south to north). Air recirculation is limited to the air handling units located on the south side of the building.</p> <p>The service building is divided into three zones according to the potential contamination hazard (section 11.3.2.2 of Part 2 of the Safety Report) as follows:</p> <p>Zone 1 - Contains no radioactive equipment and is normally free of contamination.</p> <p>Zone 2 - May contain some radioactivity caused by equipment and personnel movement into this area.</p> <p>Zone 3 - Contains items of equipment that act as sources of contamination.</p> <p>The ventilation system in the service building is designed such that any air movement between various zones, due to pressure difference, takes place from an area of least contamination to an area of increasing contamination. Recirculation of air within one zone or room is permitted, but recirculation from the central ventilation system is not permitted.</p> <p>See Section 12.3.3 Zoning, Part 2, Section 12 Radiation</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		Protection of the Safety Report presents more details of zoning arrangement for Bruce B design.	
8.11.3	<p>The ventilation system shall include filtration that will:</p> <ol style="list-style-type: none"> <li>control the release of gaseous contaminants and hazardous substances to the environment</li> <li>ensure conformation to the ALARA principle</li> <li>maintain airborne contaminants within prescribed limits</li> </ol> <p>The filtration system shall reliably achieve the necessary retention factors under the expected prevailing conditions, and shall be designed in a manner that facilitates appropriate efficiency testing.</p> <p>Guidance</p> <p>A gaseous waste management system is designed to collect all active or potentially active gases, vapours, or airborne particulates that may occur, in order to monitor and filter the effluent</p>	<p>There are no changes to the requirements.</p> <p>As described in Section 11.3.2.1.2 of Part 2 of the Safety Report the Bruce B design incorporates exhaust systems consisting of the non-contaminated exhaust system and the contaminated exhaust system. The contaminated exhaust system, used during normal operation of the plant, consists of two exhaust fans and four filter units. The system exhausts a total of 35.9 m<sup>3</sup>/s (76000 scfm) of air from potentially active areas. The air is passed through the filter system continuously whether or not activity is present in the exhaust air, before being discharged into the atmosphere through a 9.2 m (30 ft) high dispersal reactor building contaminated stack.</p> <p>The filter system consists of four units, each containing pre-filters, absolute filters and charcoal filters. The charcoal filters are used at all times. The filter units are placed in a fully enclosed room. Sufficiently thick concrete walls and floor are provided to protect station personnel from radiation. Monitors are provided in the stack to detect any activity in the effluent (section 11.3.2.1.2 of Part 2 of the Safety Report).</p> <p>The service building which houses the spent fuel bay also has two similar systems. Two fans and four filter banks with pre-filters and charcoal filters draw air from the primary spent fuel bay exhaust. The supply system introduces 118.9 m<sup>3</sup>/s (251,962 scfm) of filtered makeup air into all areas of the service building through two fan rooms and a ductwork system. A modulating damper, in the main supply duct to the primary irradiated fuel storage bay areas, maintains a</p>	C


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>before it is released to the atmosphere. The filter units should be placed in a fully enclosed room with concrete walls and floors thick enough to protect station personnel from radiation. Monitors should be provided in the stack to detect any activity in the effluent. Gaseous activity from areas such as the fuel storage pools, service areas and active laboratories should also be monitored and filtered before discharge to the atmosphere.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>• CNSC, G-129, Keeping Radiation Exposures and Doses "As Low as Reasonably Achievable (ALARA)", Ottawa, Canada, 2004.</li> <li>• CSA Group, N292.3, Management of Low-and Intermediate-level Radioactive Waste, Toronto, Canada.</li> <li>• IAEA, Safety Standards Series GS-G-3.3, The Management System for the Processing, Handling and Storage of Radioactive Waste Safety Guide, Vienna, 2008.</li> </ul>	<p>pressure of about -37.37 Pa (g) (-0.15 in WG (Inch Water Gauge)) in the bay areas with respect to adjacent room areas. The non-contaminated exhaust system exhausts 35.7 m<sup>3</sup>/s (75,700 scfm) from the non-active areas directly to atmosphere through a gravity-type roof ventilator. The system also provides ventilation for the elevator hoist way, elevator machine room, flammable stores, and truck dock. The contaminated exhaust system exhausts 50.0 m<sup>3</sup>/s (105,845 scfm) from potentially active areas. No radioactive iodine is expected in these areas; hence, there are no charcoal filters. There are four filter units upstream of the fans and each unit contains a bank of pre-filters and absolute filters. Air is passed continuously through the filters. The primary irradiated fuel storage bay exhaust system exhausts 29.8 m<sup>3</sup>/s (63,080 scfm) from the fuel bay area and other areas in which radioactive iodine and active particles could be present. There are four filter units, each containing pre-filters, absolute, and charcoal filters, upstream of the fans. Air is passed through filters continuously. Air from the contaminated exhaust and primary irradiated fuel storage bay exhaust system is discharged to atmosphere through a common 9.2 m (30 ft) high dispersal stack equipped with radioactivity monitors (section 11.3.2.2 of Part 2 of the Safety Report).</p> <p>A similar system is used for the secondary spent fuel bay in the Ancillary Services Building. The ancillary service building is kept slightly sub-atmospheric to prevent or minimize the uncontrolled escape of radioactivity from the building to the outside (section 11.3.2.3 of Part 2 of the Safety Report). Other areas in the common unit have exhaust fans with filters containing only pre-filters and absolute filters, considering</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>that there is unlikely to be iodine present.</p> <p>Following an accident, radioactive gaseous release would be controlled through the filtered air discharge system described in Clause 8.6.10.</p>	
8.12	<p>There shall be barriers to prevent the insertion of incorrect, defective or damaged fuel into the reactor.</p> <p>There shall be provisions to prevent contamination of the fuel and the reactor.</p> <p>The design shall meet the requirements found in CNSC RD-327, Nuclear Criticality Safety.</p> <p>Guidance</p> <p>The design should provide the basis for the fuel handling and storage systems. The design should include provisions for monitoring and alarming, for criticality prevention, and for shielding, handling, storage, cooling, transfer and transport of nuclear fuel.</p> <p>Considerations such as packaging, fuel accounting systems, storage, criticality prevention, fuel integrity control, foreign material exclusion</p>	<p>New requirements have been introduced. In the first three paragraphs of this clause.</p> <p>Section 10, Part 2 of the Safety Report describes the fuel and fuel handling design arrangements.</p> <p>The Nuclear Fuel Management Program [BP-PROG-12.03, R004, January 29, 2016] provides an effective framework that supports the safe and efficient execution of activities related to nuclear fuel and isotope production. It is a roadmap describing how all aspects of the program fit together and how to conduct business. This framework is established by six implementing processes, which are accountable for delivering the program objectives and meeting program expectations, standards and requirements. The implementing processes achieve these goals by specifying how work activities are planned, performed, monitored and controlled, in alignment with WANO PO&amp;C 2013 1. The program is committed to achieving excellence and embracing Bruce Power's values and behaviors as described by the Management System Manual BP MSM 1. Responsibilities and interfaces are defined throughout the program document hierarchy. The objectives of the program are defined in section 1.0 of BP-PROG-12.03 [R003] as follows:</p> <p>" Optimum reactor core operating within operating and regulatory limits;</p>	C

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>procedures and fuel security, should be taken into account in the design.</p> <p>The requirements for criticality safety requirements are provided in CNSC RD-327, Nuclear Criticality Safety. Comprehensive guidance on criticality safety and complete technical reference is provided in CNSC GD-327, Guidance on Nuclear Criticality Safety.</p> <p>The design should include provisions to prevent contamination of the fuel by foreign materials (greases, tramp uranium etc.) and prevent the spread of contamination into the reactor.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>• ANSI/ANS, 57.1, American National Standard Design Requirements for Light Water Reactor Fuel Handling Systems (as applicable), La Grange Park, Illinois, 1992.</li> <li>• IAEA, NS-G-2.5, Core Management and Fuel Handling for Nuclear Power Plants, Vienna, 2002.</li> </ul>	<p>" Operation of the reactor with fuel of an approved design, manufactured to strict quality assurance requirements;</p> <p>" Prevention of fuel damage throughout the fuel life cycle and timely removal of failed fuel from the core;</p> <p>" As low as reasonably achievable radiation exposure associated with fuel and Cobalt 60 activities;</p> <p>" Fulfilling Bruce Power's obligations under Canada's Safeguards Agreement;</p> <p>" Adequate support for fuel and fuel channel inspection;</p> <p>" Implementation of processes and procedures for all program activities required for the safe and reliable use of nuclear fuel.</p> <p>The implementing processes for Core Management program are described in section 4.3 of BP-PROG-12.03.</p> <p>Implementing and maintaining a Nuclear Criticality Safety Program is a Licence Condition 15.5 of the Bruce Nuclear Generating Stations A and B Operating Licence PROL 18.00/2020. The Low Void Reactivity Fuel (LVRF) Demonstration Irradiation program requires compliance with the relevant sections of RD-327 Nuclear Criticality Safety. As required in Licence Condition Handbook [NK21-CORR-00531-12135 / NK29-CORR-00531-12545 / LCH-BNGS-R000] Bruce Power's procedures shall be updated to reflect the level of nuclear criticality safety management required at Bruce B as a result of the suspension of the LVRF project. Bruce Power is targeting October 31, 2015 to align fully with current practices and to document compliance with RD-327</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>IAEA, NS-G-1.4, Design of Fuel Handling and Storage Systems for Nuclear Power Plants, Vienna, 2003.</li> </ul>	<p>within applicable governance for Bruce A and B. An internal gap assessment has been completed in order to identify the required changes to processes and procedures to ensure compliance with RD-327. The majority of changes are in regard to the removal of procedural references to Low Void Reactivity Fuel (LVRF), a project which is no longer being pursued at Bruce Power. Other than LVRF, the remaining implementation of the requirements of RD-327 into Bruce Power's governance deals with security sensitive elements. Since further effort is needed to finalize inclusion of these elements into governance appropriately a new target date of May 31, 2016 is requested [Letter F. Saunders to K. Lafreniere, Bruce A and Bruce B: Regulatory Document RD-327, Compliance Update, NK21-CORR-00531/NK29-CORR-00531-12854, October 28, 2015].</p> <p>Bruce Power maintains their nuclear criticality safety program in accordance with BP-PROC-00324 [R004, June 10, 2009] Nuclear Criticality Safety Management such that Upper Subcritical Limits established by the program will not be exceeded under both normal and credible abnormal conditions of operations with fissionable materials outside the reactors. Bruce Power is to ensure that out of core sub-criticality is maintained such that for all normal and credible abnormal conditions outside the reactor core, the Effective Multiplication Factor Keff does not exceed the upper sub-critical limits established by the program. Bruce Power is revising programs and procedures to reflect the decreased level of nuclear criticality safety management required at Bruce B as a result of the suspension of the LVRF Project, as the only enriched fuel from the demonstration irradiation of this project is located in the Primary and Secondary Fuel Bays. Bruce Power is targeting October 31, 2015 to align fully</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>with current practices and to document compliance with RD-327 within applicable governance for Bruce A and B. [Letter F. Saunders to M. Leblanc, Bruce Power: Requests and Supplemental Information for Licence Renewal, NK21-CORR-00531-11715 / NK29-CORR-00531-12105, November 28, 2014)</p> <p>Also, a lattice of natural uranium and light water cannot be made critical in any configuration. Hence, no criticality problem exists in the spent fuel bay of CANDU reactors as discussed in Section 1.2.2 of Part 2 of the Safety Report. Irradiated natural uranium fuel bundles stored in light water do not pose a criticality hazard (section 10.2.5.3.1 of Part 2 of the Safety Report).</p>	
8.12.1	<p>The design of the fuel handling and storage systems for non-irradiated fuel shall:</p> <ol style="list-style-type: none"> <li>1. ensure nuclear criticality safety</li> <li>2. permit appropriate maintenance, periodic inspection, and testing of components important to safety</li> <li>3. permit inspection of non-irradiated fuel</li> <li>4. prevent loss of or damage to the fuel</li> </ol>	<p>The only change is editorial, i.e., deletion of the redundant information related to maintaining an approved subcriticality margin, etc. It is redundant since a reference to RD-327 is provided.</p> <p>Section 10.2.3 of Part 2 of the Safety Report provides design details about the new fuel storage and handling. New fuel is delivered to the station in palletized crates and is stored until required. It is then transferred in the crates to the new fuel loading area to be loaded into the fuelling machines using the four new fuel transfer mechanisms. The new fuel transfer mechanisms transfer the fuel through the containment wall into the fuelling machines without exposing the operators to any tritium or radiation hazards. New fuel handling equipment is shown in Figure 10-7, Part 2 of the Safety Report. New fuel bundles are received at a new fuel storage area located at elevation 619 beside a truck passageway through the service building. The new fuel bundles are enclosed in protective</p>	C



Article No.	Clause Requirement	Assessment	Compliance Category
	5. meet Canada's safeguards requirements for recording and reporting accountancy data, and for monitoring flows and inventories related to non-irradiated fuel containing fissile material	<p>boxes containing 42 bundles. The new fuel storage area maintains a capacity of 3864 fuel bundles. Facilities are provided to store the fuel in their protective crates and to move them to the new fuel loading facilities and inspection stations using a 2,700 kg (6,000 lb) hoist and monorail system located in the new fuel loading area.</p> <p>The protective covering of the bundles is removed by hand and the bundles are raised from the boxes by a lifting attachment connected to an air balanced hoist. This lifting attachment allows the fuel to be rotated for cleaning, visually inspected for damage, and gauged for fuel spacer interlocking. After inspection, the serial numbers of the approved new fuel bundles are recorded and the bundles are transferred, using the hoist and lifting attachment, to the selected new fuel port transfer mechanism where the bundles are placed in the loading trough. Normally, a maximum of two bundles will be loaded into the loading trough, although it is possible to load only one bundle. A maximum of 16 bundles can be loaded into the transfer mechanism magazine. The fields in the new fuel loading area are quite low, less than 1E-5 Gy/h (1.0 mR/h). The damage mechanisms and the associated conditions are described in Part 2, Section 10.2.4.8.2 of the Safety Report.</p> <p>Due to the natural uranium fuel bundles an inadvertent criticality is not achievable unless the fuel bundles are closely packed and immersed in light water. Criticality assessments were made of this possibility during the construction of Bruce A and it was shown that the locations chosen for this storage provide a safe and secure storage location. The fuel storage area consists of a large area, screened in with a security fence but without solid walls. This is added insurance that it is</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		not possible to create a flooded situation.	
8.12.2	<p>The design of the handling and storage systems for irradiated fuel shall:</p> <ol style="list-style-type: none"> <li>1. ensure nuclear criticality safety</li> <li>2. permit adequate heat removal in operational states, DBAs and DEC's</li> <li>3. permit inspection of irradiated fuel</li> <li>4. permit periodic inspection and testing of components important to safety</li> <li>5. prevent the dropping of irradiated fuel in transit</li> <li>6. prevent unacceptable handling stresses on fuel elements or fuel assemblies</li> <li>7. prevent the inadvertent dropping of heavy objects and equipment on fuel assemblies</li> </ol>	<p>A new requirement for heat removal under DEC's. Additional new requirements are introduced relevant to the design of irradiated fuel storage pools.</p> <p>Section 10.2.5 of Part 2 of the Safety Report provides design details about Irradiated Fuel Handling and Storage.</p> <p>The irradiated fuel discharge mechanism transfers the fuel from the fuelling machine head into the primary irradiated fuel bay as shown in Figure 10-12 of Section 10.2.5.2.1 of Part 2 of the Safety Report. The mechanism is designed to transfer the bundles in pairs, with a minimum of exposure to air, a minimum of downgrading of the fuelling machine heavy water by natural water from the storage bay and minimum loss of heavy water to the bay water. The irradiated fuel discharge mechanism also permits the transfer of single bundles without special equipment. A fuel carrier with bundles can be transferred through the irradiated port with the mechanism removed using special equipment.</p> <p>The permissible time of the fuel transit in air is limited, so the mechanisms are provided with a vent which when open will result in flooding of the mechanism. In the event of a system malfunction, the vent can be opened regardless of the position of the port valves, and the chamber air flow is stopped. This allows the chamber to be flooded rapidly. If possible, the port valves will be closed to prevent downgrading of the heavy water in the head. The delayed neutron monitoring system can identify whether a particular channel contains a defected fuel bundle. While fuel bundle transfer dry-sip monitoring can assist in narrowing down the defected bundles to a specific bundle-pair. In the event of a</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	8. permit inspection and safe storage of suspect or damaged fuel elements or fuel assemblies	<p>defective fuel bundle, the pair containing the defective bundle is transferred to the inspection and canning area of the primary irradiated fuel bay for inspection and canning (section 10.2.5.2.1 of Part 2 of Safety Report). Shortly after discharge to the irradiated fuel bay, the defective fuel bundle is inspected in the inspection section after which, the decision is made to can, ship or store the defected bundle.</p> <p>Each fuel bundle has a specific identification number which is recorded when the bundle is loaded into the reactor. This number is input into the fuel management code NUFLASH and is tracked through the core irradiation. The fuel discharge is subject to IAEA monitoring as part of Canada's non-proliferation commitments so each bundle discharged is counted. The discharged bundle number is associated with a specific tray number and can be located within the bay as needed.</p> <p>Irradiated fuel is stored in the primary irradiated fuel storage bay (Section 10.2.5.2.3) for a minimum period of six months before being transferred underwater to the secondary irradiated fuel storage bay (Section 10.2.5.2.4). There are no soluble absorbers needed for criticality control. The fuel handling system (fuelling machines, discharge mechanisms, etc.) requires considerable routine maintenance. This was expected at the time of Bruce B design and facilities are available to cope with it within the Central Service Area (CSA) or East Service Area of the plant. The major maintenance and service facilities for the fuel handling systems are located in the service building and are described in section 10.2.7 and shown in Figure 10-13 of Part 2 of Safety Report. Decontamination facilities are available within the CSA to cope with the fuel handling and storage system</p>	
	9. provide proper means for radiation protection		
	10. permit adequate identification of individual fuel modules		
	11. facilitate maintenance and decommissioning of the fuel storage and handling facilities		
	12. facilitate decontamination of fuel handling and storage areas and equipment when necessary		
	13. ensure implementation of adequate operating and accounting procedures to prevent loss of fuel		
	14. include measures to prevent a direct threat or sabotage to irradiated fuel		
	15. meet Canada's safeguards requirements for recording and reporting accountancy data, and for monitoring flows and inventories related to irradiated fuel containing fissile material		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>A design for a water pool used for fuel storage shall include provisions for:</p> <ol style="list-style-type: none"> <li>controlling the chemistry and activity of any water in which irradiated fuel is handled or stored</li> <li>monitoring and controlling the water level in the fuel storage pool</li> <li>detecting leakage</li> <li>preventing the pool from emptying in the event of a pipe break</li> <li>sufficient space to accommodate the entire reactor core inventory at all times</li> </ol> <p>The design of irradiated fuel storage pools shall include means for preventing the uncovering of fuel in the pool in operational states, DBAs and DEC's.</p> <p>The design for a water pool used for fuel storage</p>	<p>needs.</p> <p>As described in Part 2, Section 10.2.5.4.1 of the Safety Report, the fuel bay water provides both coolant and radiation shielding. The fuel bay cooling circuits remove the heat generated by the fuel bundles in the bays to control the bay water temperatures for proper cooling of the fuel and to limit thermal stresses in the bay structures and the lining system. The purification circuits remove suspended and dissolved solids from the bay water to control the radioactivity level of the water for personnel protection and to maintain the clarity of the water for good visibility during inspection and transfer of the fuel bundles within the bay. Each section of the primary irradiated fuel storage bay (inspection section and storage section) and the secondary irradiated fuel storage bay has its own cooling and purification circuits.</p> <p>The Bruce B fuel bays do not have anti-syphon devices but the cooling circuits are designed such that any piping comes off the bays at high levels. As discussed in Section 1.5.1 of Appendix 1 of Part 3 of the Safety Report, pipe breaks in the cooling circuits of both the primary and secondary irradiated fuel bays potentially result in draining of the bay water level down to the level of the lowest circulation nozzles. Accidental draining of the bay water level down to the bottom of the lowest circulation nozzle (i.e., a reduction of 1.2 m from the normal level of 191.9 m) results in relatively benign dose rates. In all cases which result in a loss of flow in either of the cooling/purification circuits, the operator in the main control room will receive a prompt indication of a problem at the local control panel and in the main control room. Pump trouble conditions for cases involving loss of pumping is also annunciated locally and in the main control room. Failures,</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>shall include provisions for DEC's by:</p> <ol style="list-style-type: none"> <li>1. ensuring that boiling in the pool does not result in structural damage</li> <li>2. providing temporary connections to enable the refill of the pool using temporary supplies</li> <li>3. providing temporary connections to heat removal systems for power and cooling water</li> <li>4. providing hydrogen mitigation in the spent fuel pool area</li> <li>5. ensuring that severe accident management actions related to the spent fuel pool can be carried out</li> </ol> <p>Guidance</p> <p>Hydrogen mitigation in the spent fuel pool area is particularly important if it is envisaged that the pool may be used for fission product scrubbing as part of containment venting. Hydrogen mitigation in the spent fuel pool area may not be necessary</p>	<p>which result in loss of service water to the heat exchangers of one or both of the bay cooling circuits, also initiate the irradiated fuel bay cooling and purification system trouble alarms in the main control room.</p> <p>Loss of primary fuel bay water is considered in the accident analysis (section 1.5.2 Appendix 1 of Part 3 of Safety Report). This scenario postulates a leakage of primary irradiated fuel bay water through one of the irradiated fuel ports. The leakage is assumed to be caused by a simultaneous failure of all the D2O catenary hoses of a FM while it is attached to the irradiated fuel port. Under such conditions, it would take at least 10 hours for the water level to reach the fuel allowing time for possible operator intervention. Furthermore, the available time is well in excess of the maximum time, about 1 h, required to move a tray off the conveyor to the lower level of the storage frames. If the gated divider is assumed to be opened at the time of the incident, it would take about 150 h before the fuel in the top of the storage frames is exposed. Isolation of the discharge can be credited within this time. Thus, this incident does not result in any exposure of fuel to degraded cooling conditions which could cause fission product release. Even if no actions were taken the resulting potential release has been calculated to be a small fraction of the allowable release limit. This accident could require evacuation of the main control room located above the spent fuel bay, and has been considered in the secondary control area design.</p> <p>The requirement for sufficient space to accommodate the entire reactor core inventory at all times is not reflected in the design and operating documentation. Therefore, it is assessed as a gap (Gap). The Used Fuel Waste and Cobalt</p>	



Rev Date: September 20, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	if draining of the pool beyond make- up capability can be precluded.	<p>60 Agreement defines the Buffer Capacity and discusses the required capacity of Used Fuel Pools in respect of either the Bruce A or Bruce B. The Used Fuel Pools should be sufficient to hold one reactor core dump plus the amount of used fuel waste reasonably projected by Bruce Power to be generated during one year by the number of operational Bruce A reactors or Bruce B reactors associated with such used fuel pools. The term Used Fuel Pools does not include the primary water pools associated with Bruce A or Bruce B.</p> <p>Design modifications have been implemented to allow emergency water to be added to the spent fuel bays. The installation of piping to allow makeup water to be added to the primary and secondary irradiated fuel bays is complete for Bruce A and Bruce B [NK21 -CORR-00531 -10963/NK29-CORR-00531 -11349/NK37-CORR-00531 -02162]. In addition the IFB structural analysis demonstrated that the heatup (to boiling) and subsequent cooldown cycle of the IFBs will not result in through-wall cracking of the concrete and thus will not result in draining of the IFBs. The analysis recommended that cooling mitigation measures should be initiated within the first few hours of an accident, to control the propagation of any cracks [Letter, F. Saunders to R. Lojk, "Bruce Power Irradiated Fuel Bay Structural Integrity Analysis", March 26, 2013, NK21-CORR-00531-10341 I NK29-CORR-00531-10750].</p>	
8.12.3	The design shall provide a means for allowing reliable detection of fuel defects in the reactor, and the subsequent removal of failed fuel, if action levels are exceeded.	<p>There are no changes to this requirement.</p> <p>Continuous monitoring of fuel defects is facilitated by the Gaseous Fission Product (GFP) Monitor system, and supplemented through PHT system chemistry sampling. Section 11.2.4.2 of Part 2 of the Safety Report provides</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Guidance</p> <p>The amount of failed fuel left in the core may impact the safety case of the design. The design should specify the criterion for continued operation with failed fuel in the core, or to unload the fuel assembly from the core. The design should allow for the removal of failed fuel in as timely a manner as possible. The design should provide for the inspection and quarantine of failed fuel in the fuel handling and storage facilities.</p>	<p>further details of GFP monitor system.</p> <p>The Delayed Neutron (DN) monitoring system is used to locate failed fuel bundles when the reactor is on power. Should a fuel bundle fail during normal operation, fission products are released into the heat transport coolant. Some of them (Br-87 and I-137) emit delayed neutrons during decay. The DN system uses BF3 neutron counters to measure the delayed neutrons emitted by a coolant sample extracted from all fuel channels. When a channel indicates a higher delayed neutron count with respect to other similar power channels, then it is inferred that failed fuel is present in that channel.</p> <p>The delayed neutron monitoring system can identify whether a particular channel contains a defected fuel bundle. Shortly after discharge to the irradiated fuel bay, the suspected defective fuel bundles are inspected in the inspection area after which, the decision is made to can, ship or store the defect bundle. Further details are provided in Part 2, Section 10.2.5.2.1 and 11.2.4.3 of the Safety Report.</p> <p>HTS coolant activity limits are defined on radioactive Iodine-131 concentration in the HTS coolant and radioactive tritium concentration in the HTS coolant. The safety limits for HTS coolant activity are provided in Section 5.0 Coolant Activity of Bruce NGS B Operational safety Requirements for Heat Transport System [NK29-OSR-33000-00001, R000, June 2009].</p>	
8.13	The design and layout of the plant shall make suitable provision to minimize exposure and contamination from all sources. This shall include	<p>There are no changes to this requirement.</p> <p>The design provisions include appropriate shielding, filtration, venting and sampling in order to limit the exposure of plant</p>	Gap




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>the adequate design of SSCs to:</p> <ol style="list-style-type: none"> <li>control access to the plant</li> <li>minimize exposure during maintenance and inspection</li> <li>provide shielding from direct and scattered radiation</li> <li>provide ventilation and filtering to control airborne radioactive materials</li> <li>limit the activation of corrosion products by proper specification of materials</li> <li>minimize the spread of active material</li> <li>monitor radiation levels</li> <li>provide suitable decontamination facilities</li> </ol> <p>Guidance</p>	<p>personnel as low as reasonably achievable. The Radiation Protection Program [BP-PROG-12.05, R003] is in place to support this goal.</p> <p>As described in Part 2, Section 12.2 of the Safety Report, all systems considered to have significant radiological implications for station personnel during operation or maintenance were reviewed in the design phase. The review process included a series of Man-Rem Audit meetings on a system-by-system basis. AECL design, operations, health physics, and physics and analysis groups were represented. Each system design was examined with respect to reliability, maintainability, ease of handling, ease of access, shielding, etc. Radiation exposure was estimated for each system in man-rem per year, and the estimate compared with budgeted exposure figures prepared earlier as targets. (All estimates were based on Douglas Point radiation exposure data as reported for 1970). Proposals to reduce radiation exposure by improving system design were analyzed and, wherever feasible, implemented. Special attention was also directed to system chemistry, equipment simplicity, service intervals, and ease of component removal. In general, it was recognized that the fundamental approach of improving component reliability or system chemistry is more effective than secondary measures such as installation of additional shielding. Improved station design has contributed significantly to the reduction of both collective and individual dose expenditures, and to the productivity of those dose expenditures which do take place.</p> <p>Limiting personnel exposure is achieved by incorporating protective features into the initial station design, by controlling access to areas with elevated radiation levels, and by</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The NPP should be divided into zones based on predicted dose rates, radioactive contamination levels, concentration of airborne radionuclides, access requirements and specific requirements (such as the need to separate safety trains). The criteria and rationale for radiation zone designations – including zone boundaries for normal, refuelling and accident conditions – should be provided. These criteria should be used as the basis for the radiation shielding design.</p> <p>From a radiological protection perspective, careful assessment should be made of the access requirements for operation, inspection, maintenance, repair, replacement and decommissioning of equipment; these considerations should be incorporated into the design. The design should also provide lay down space for special tools and ease for servicing activities. The design should also have features such as platforms or walkways, stairs, or ladders that permit prompt accessibility</p> <p>for servicing or inspection of components located in higher radiation zones.</p> <p>The use of remote technology for maintenance and surveillance in high radiation areas should be considered and incorporated. Preference should</p>	<p>excluding personnel who are approaching certain administrative dose limits from further exposure. Requirements are in place that govern the use of Radiation Protection Protective Equipment, which protect personnel from internal radiation resulting from the uptake of airborne and surface contamination. Decontamination facilities are provided to restrict the spread of contamination. Dosimetry and personnel monitoring devices are used extensively to monitor the doses that staff members receive, and to ensure that these doses are within allowable limits.</p> <p>The station is divided into three zones according to the potential for contamination and other radiological hazards, as described in Part 2, Section 12.3.3 of the Safety Report. Figures 12-1 to Figure 12-6 show the general zoning arrangement for Bruce B. For any movement of personnel or material between zones, actions must be taken to prevent possible contamination from a zone of higher number to a zone of lower number. For this purpose, contamination monitors are located on all approved routes between zones. The radiation levels are provided in Table 12-1.</p> <p>Zoning procedure [BP-RPP-00015, R012, January 12, 2016] details the requirements for movement of personnel and equipment around the zoned areas of Bruce Power Facilities and specifies the requirements for the transfer of radioactive material outside the zoned areas but within the site boundary. The contamination limits for Zone 1 and Unzoned area surfaces are presented in Appendix B. These surface contamination levels are linked to the action levels in SEC-RPR-00022 Action Levels, which are dictated by the station Power Reactor Operating Licence for Bruce A and B.</p> <p>There are numerous decontamination centres within the</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>be given to the use of appropriate engineering controls and design features over process or administrative controls.</p> <p>Reliable equipment that requires minimum surveillance, maintenance, testing and calibration should be chosen.</p> <p>Operating experience should be reflected in the criteria and rationale provided in the design.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>• CNSC, G-129, Keeping Radiation Exposures and Doses "As Low as Reasonably Achievable (ALARA)", Ottawa, Canada, 2004.</li> <li>• IAEA, Safety Guide RS-G-1.1, Occupational Radiation Protection, Vienna, 1999.</li> <li>• IAEA, Safety Standards Series NS-G-1.13, Radiation Protection Aspects of Design for Nuclear Power Plants, Vienna, 2005.</li> </ul>	<p>plant, located at appropriate locations, to handle contaminated equipment, e.g., Fuelling Machine Dismantling and Decontamination Room, Small Parts Decontamination Room, fuel shipping cask decontamination area is provided in the shipping area, CSA decontamination facilities etc.</p> <p>The criteria and rationale for radiation zone designations - including zone boundaries for accident conditions are not provided in the design documentation as suggested in guidance. The criteria and rationale seem, however, to be limited to what systems and qualitative probability of contamination there are in the area. There does not seem to be any consideration of predicted dose rates or airborne radionuclides. There is no documentation of the basis for station zoning for normal operations including consideration of the predicted dose rates or anticipated airborne radionuclides in the areas. Zone boundaries are not provided in the design. Therefore, it is assessed as a gap (Gap). It is recognized that such expectations are more relevant to new reactor designs.</p>	
8.13.1	The shielding design shall prevent radiation levels in operating areas from exceeding the prescribed	The changes are editorial and do not affect the requirements, e.g., "DBAs and DEC's" replaced "accident conditions".	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>limits. This shall include provision of appropriate permanent layout and shielding of SSCs containing radioactive materials, and the use of temporary shielding for maintenance and inspection work.</p> <p>To minimize radiation exposure, the plant layout shall provide for efficient operation, inspection, maintenance, and replacement. In addition, the design shall limit the amount of activated material and its build-up.</p> <p>The design shall account for frequently occupied locations, and support the need for human access to locations and equipment.</p> <p>Access routes shall be shielded where needed.</p> <p>The design shall enable operator access for actions credited for post-accident conditions. Adequate protection shall be provided against exposure to radiation and radioactive contamination during DBAs and DECAs for those parts of the facility to which access is required.</p> <p>Guidance</p> <p>Shielding should be designed based on the zone</p>	<p>The shielding requirements as specified in the guidance are listed in Section 12.3.1.1 of Part 2 of the Safety Report. The design incorporates primary shielding, which attenuates radiation from the reactor; secondary shielding, which attenuates radiation from the heat transport coolant; auxiliary shielding, which attenuates radiation from auxiliary systems such as the moderator, fuelling machine, and failed fuel; and supplementary shielding in addition to these. The radiation levels are specified in Table 12-1.</p> <p>The use of temporary shielding is a standard practice in Bruce B. Procedures for controlling temporary shielding at the station are documented.</p> <p>The design includes provisions for shielding as required. For example, as described in Section 3.1 of Part 2 of the Safety Report, the steam generators are enclosed by shielding walls to permit access, during operation, to the central area directly above the reactor. In areas, where it is not possible to provide shielding, access is controlled by the Access Control System as described in Section 12.3.1.3.2 of Part 2 of the Safety Report. In addition, personnel monitoring, dosimetry facilities and protective clothing are available.</p> <p>Details about design provisions for access for maintenance and inspections are provided in Section 5.2.5.6 of Part 2 of the Safety Report.</p> <p>Each material, which forms a part of the reactor coolant pressure boundary, has been chosen to be compatible with the expected service and environmental conditions at the location at which it is used. Table 5-6 in Part 2 of the Bruce B Safety Report, lists the materials used for the major components in the HT system. The major materials exposed</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	delineation described in section 8.13. The shielding design criteria (including the methodology for shield parameters and choice of shield material) should be provided. In establishing specifications for shielding, account should be taken of the buildup of radioactive materials over the lifetime of the NPP.	<p>to the reactor coolant are zirconium alloys, 400 series steels, carbon steel, Inconel and Incoloy (section 5.2.3.1 of Part 2 of the Safety Report). Part 2, Section 5.3.3 of the Safety Report contains details on the zirconium alloy and 400 series steels. Carbon steel is used for the piping, feeders and headers. The coolant chemistry has been chosen to give acceptable low carbon steel corrosion rates. The use of carbon steel gives low cobalt and nickel concentrations in the coolant and so assists in the objective of minimizing the quantities of Co-58 and Co-60 in the HT system. Inconel is used as the steam generator tubing as it combines a high corrosion resistance to pitting, cracking and localized attack with a low corrosion product release rate in both the HT and secondary side water. Incoloy is used for the pressurizer heaters.</p> <p>The operator actions credited in the Safety Report during accidents, as listed in section 1.3 of Part 3 of the Safety Report; do not require field action and thus they would not be subject to radiation exposure. Following the accident, if repairs to systems in use are required, then procedures for such repairs would be required to take into account the shielding available and, if necessary, be prepared to add more temporary shielding. Unless there was life-saving action required, the staff would still be limited to their normal allowable doses, which would limit the time available for them to participate in the repair.</p> <p>The shielding design criteria and the methodology for shield parameters and choice of shield material are not sufficiently described in the design documentation. The buildup of radioactive materials over the lifetime of the NPP is not reflected in the shielding specifications as required in the guidance section; therefore it is assessed as a gap (Gap 1).</p>	

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>It is noted that although the criteria and rationale for radiation zone designations (for normal operations) are given in Section 12.3.3 of Part 2 of the Safety Report, the criteria and rationale are limited to what systems are in the area and qualitative probability of contamination. Predicted dose rates or airborne radionuclides have not been explicitly considered. Therefore, this is assessed as a gap (Gap 2): There is no design documentation of the basis for station zoning for normal operations including consideration of the predicted dose rates or anticipated airborne radionuclides in the areas. Contamination levels are addressed in the definitions given in the Safety Report Section 12.3.3 and Appendix A of BP-RPP-00015, R012 Zoning (January 12, 2016).</p> <p>The predicted dose rates used to be average dose rates for each zone given in BP-RPP-00002 R001, Radiation Protection Requirements (February 6, 2012); however these have been revoked in the reorganization of the RP Program.</p> <p>Additional details about radiation protection program are provided in Safety Factor 15.</p>	
8.13.2	<p>The plant layout and procedures shall control access to radiation areas and areas of potential contamination.</p> <p>The design shall minimize the movement of radioactive materials and the spread of contamination, and to provide appropriate decontamination facilities for personnel.</p>	<p>There are no changes in the requirements. Only guidance needs to be addressed.</p> <p>As described in Section 12.3.1.3 of Part 2 of the Safety Report, the plant is laid out to minimize the need for personnel to enter areas with high radiation fields. In general, operational procedures restrict access to the reactor building to qualified personnel and those escorted by qualified personnel. Access to areas that either have or could have high radiation fields is strictly controlled by the Access Control System. Extensive use is made of physical barriers, permanent and temporary signs, and other means to clearly</p>	C




Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Guidance</p> <p>Provisions should be made for controlling the exit(s) from the radiation zones. Monitoring of personnel and materials should be established at the access and egress points for the radiation zones. Access to areas of high dose rates or high levels of radioactive contamination should be controlled through the provision of lockable doors and interlocks. Routes for personnel through radiation zones and contamination zones should be minimized in order to reduce the time spent in transiting these zones. Radiation zones where personnel spend substantial time should be designed to the lowest practical dose rates and ALARA.</p> <p>Within the radiation zones, changing areas for personnel should be provided at selected locations to prevent the spread of radioactive contamination during maintenance and normal operation. Within these change areas, consideration should be given to the need for decontamination facilities for personnel, radiation monitoring instruments and storage areas for protective clothing. A physical barrier should clearly separate the clean area from the potentially contaminated area.</p>	<p>warn and instruct personnel of any possible danger from radiation. Access controlled areas have locks and keys controlled by the shift manager. The keys are kept in the control room. When personnel are working in a controlled area, the access control key is retained in the lock while the door is unlocked, whether open or closed. Visible signals are provided in the control room to warn of unlocked doors (section 12.3.1.3.2 of Part of the Safety Report).</p> <p>Access control areas are listed in Tables 12-3 and 12-4 of Part 2 of the Safety Report.</p> <p>As described in Part 2, Section 12 of the Safety Report, the Bruce B plant has decontamination facilities available for personnel located at several points throughout the plant. Decontamination facilities for equipment provide the capability for controlled decontamination of equipment. When the size of the equipment permits, contaminated items are transported under wrap to the decontamination centre or to the active maintenance bays. Here, the equipment is dismantled, and cleaned with special equipment. Special ventilation can prevent the spread of activity. Such work is performed in contamination control areas. Effluent from decontamination is directed to the Active Liquid Waste System and solid wastes.</p> <p>Radioactive wastes are handled via the solid and liquid waste management systems. Dose rates outside containment are minimized due to shielding provided in the design.</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
8.13.3	<p>Equipment shall be provided to ensure that there is adequate radiation monitoring in operational states, DBAs and DEC's.</p> <p>Stationary alarming dose rate meters shall be provided:</p> <ol style="list-style-type: none"> <li>for monitoring the local radiation dose rate at places routinely occupied by operating personnel</li> <li>where the changes in radiation levels may be such that access may be limited for periods of time</li> <li>to indicate, automatically and in real-time, the general radiation level at appropriate locations in operational states, DBAs and DEC's</li> <li>to give sufficient information in the control room or at the appropriate control location for operational states, DBAs and DEC's, to enable plant personnel to initiate corrective actions when necessary</li> </ol> <p>Monitors shall be provided for measuring the activity of radioactive substances in the</p>	<p>A new requirement for monitoring in DEC's is introduced. Stationary alarming dose meters to indicate automatically and in-real time the radiation levels during operational states, DBAs and DEC's. Compliance with the requirement for radiation monitoring equipment that indicate automatically and in real time the radiation levels cannot be confirmed in the design documentation. Therefore, this is assessed as a gap (Gap).</p> <p>Fixed area gamma monitors are intended to warn the personnel by audio and visual alarms of hazardous changes in radiation levels under all operating and non-operating conditions. They also provide information of gamma dose rates. The fixed area gamma monitors are located in the areas listed in Table 12-2 of Part 2 of the Safety Report. The alarm criteria depend on the analysis of the potential hazard in the area (Section 12.3.1.2 of Part 2 of the Safety Report).</p> <p>Contamination monitoring stations are provided throughout the station so that personnel may monitor themselves for contamination on their clothing and exposed body surfaces and on equipment. Whole body monitors utilize large area detectors (Plastic Scintillators) to detect beta contamination of hands, feet, head and most parts of the body of personnel. In select locations, alpha detection capability is also deployed where risk of alpha contamination is considered significant. Friskers utilizing handheld detectors suitable for the assessment of beta/gamma contamination levels are located at all whole body monitoring locations to assist in localizing contamination if detected with the whole body monitor. Portal monitors have a set of detectors to monitor personnel as they pass through. The detectors are suitable for the assessment of gamma contamination levels. On detection of</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>atmosphere:</p> <ol style="list-style-type: none"> <li>for areas routinely occupied by personnel</li> <li>for areas where the levels of activity of airborne radioactive materials may, on occasion, be expected to necessitate protective measures</li> <li>to give an indication in the control room, or in other appropriate locations, of when a high concentration of radionuclides is detected</li> </ol> <p>Facilities shall be provided for monitoring individual doses to and contamination of personnel.</p> <p>Stationary equipment and laboratory facilities shall be provided to determine the concentration of selected radionuclides in fluid process systems as appropriate, and in gas and liquid samples taken from plant systems or the environment.</p> <p>Stationary equipment shall be provided for monitoring the effluents prior to or during discharge to the environment.</p>	<p>contamination in excess of the acceptable level, an audible and visual annunciation will occur at the monitor and for some monitors in the control room (Sections 12.3.4.1 and 12.3.4.2 of Part 2 of the Safety Report).</p> <p>Tritium monitoring is done by various instruments depending on the location, application and sensitivity required. Tritium diffuser sampler units are used in most areas for obtaining samples of airborne tritium for subsequent analysis. Collected samples are analyzed in a laboratory environment, free from interference from ambient gamma radiation fields. Portable tritium meters are also available to give direct measurement of airborne tritium concentration (section 12.3.2.1 of Part 2 of Safety Report). These instruments are routinely issued to work groups doing certain specific jobs such as heat transport (HT) or moderator resin slurring activities and tritiated heavy water handling.</p> <p>As described in Section 6.5.2.11 of Part 2 of the Safety Report, the Post-Accident Radiation Monitoring System (PARMS) provides on-line radioisotopic analysis for noble gases, gross gamma detection and off-line radioisotopic analyses for particulates, iodine and tritium. The detected and analyzed parameters are presented on a local and a remote display unit, located in the Unit 2 control equipment room.</p> <p>As specified in section 12.5 of Part 2 of the Safety Report the site is equipped with a Health Physics laboratory that is operated by the health physics group, which continually reviews and assesses the effectiveness of the station radiation control program. They are also responsible for the maintenance of individual dose records. They collect, edit and issue reports on radiological dose data to the licensing</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		body as specified in the operating procedures.	
8.13.4	<p>The design shall provide for:</p> <ol style="list-style-type: none"> <li>appropriate disposal of radioactive materials, either to onsite storage or through removal from the site</li> <li>reduction in the quantity and concentration of radioactive materials produced</li> <li>control of dispersal within the plant</li> <li>control of releases to the environment</li> <li>decontamination facilities for equipment, and for handling any radioactive waste arising from decontamination activities</li> <li>minimization of radioactive waste generation</li> </ol>	<p>There are no changes in the requirements in this clause.</p> <p>An extensive Environmental Assessment [NK29-REP-07730-00001] for the New Fuel Project for Bruce B was conducted in 2004 in support of introducing a new fuel type, i.e. Low Void Reactivity Fuel Design. The review assessed the impact of the Bruce B units on the environment and contains further information on some of these topics. Section 2.0 of the EA Study Report describes the operation of Bruce B and all on-site maintenance and materials and waste handling activities. The key Bruce Power safety, environmental management, criticality safety programs, as well as aging issues and potential malfunctions and accidents are also presented in this study.</p> <p>Dry solid wastes, collected throughout the station on a daily basis, are nominally classified as radioactive or non-radioactive depending on the area from which they originate. Non-radioactive wastes are transferred daily to OPG's WWMF waste operations for incineration, volume reduction and landfill on BNPD site.</p> <p>Dry radioactive waste is collected on a daily basis and temporarily stored in Unit 1 facilities for monitoring. It is then transported to OPG's WWMF service department waste operation, where the waste goes through volume reduction; incineration or it is stored in OPG's WWMF site.</p> <p>Spent resin from the heat transport, moderator, end shield cooling, primary irradiated fuel storage bay systems and the liquid force system are transferred into two stainless steel storage tanks located in concrete vaults below the reactor</p>	C

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>auxiliary bay floor of Unit 2. These tanks provide temporary storage before transfer to OPG's WWMF waste operation site.</p> <p>Filter solids from the active liquid waste treatment system and heat transport system, spent resin from other systems, and other radioactive solid waste material are stored at, the OPG's WWMF waste operations site.</p> <p>Bruce Power is committed to minimizing radioactive wastes per BP-PROC-00878, R000, Radioactive Waste Management, which is governed by BP-PROG-12.05, R003, Radiation Protection Program</p>	
8.13.5	<p>The design shall provide the means for monitoring radiological releases to the environment in the vicinity of the plant, with particular reference to:</p> <ol style="list-style-type: none"> <li>1. pathways to the human population, including the food-chain</li> <li>2. the radiological impact, if any, on local ecosystems</li> <li>3. the possible accumulation of radioactive materials in the environment</li> <li>4. the possibility of any unauthorized discharge routes</li> </ol>	<p>There are no changes in the requirements</p> <p>A summary of the environmental monitoring program is presented in Section 12.5 of Part 2 of the Safety Report.</p> <p>Bruce Power carries out a monitoring program beyond the site boundary for the Bruce Power site as a whole, called the Radiological Environmental Monitoring Program (REMP). This environmental surveillance program was originally authorized by the AECB and later upgraded in 1999 [section 12.5 of Part 2 of the Safety Report]. The purpose of the program is:</p> <ol style="list-style-type: none"> <li>1. To confirm that emissions of radioactive materials are properly controlled.</li> <li>2. To verify that the assumptions made in calculating facility Derived Release Limits (DRLs) remain valid.</li> <li>3. To permit an independent estimate to be made of doses to the public resulting from emissions.</li> </ol>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Guidance</p> <p>Additional guidance can be found in CSA N288.4, Environmental Monitoring Programs at Class I Nuclear Facilities and Uranium Mines and Mills.</p>	<p>4. To provide data to aid in the development and evaluation of models which adequately describe the movement of radionuclides through the environment.</p> <p>The Bruce Power Health Physics Laboratory performs the sampling and analysis in support of the program. All analyses are performed by Bruce Power Health Physics Laboratory except TLDs, which are analyzed by OPG Health Physics Laboratory (see Table 12-5).</p> <p>Results of the Radiological Environmental Monitoring Program are published in report format in the Annual Summary and Assessment of Environmental Radiological Data. The program is summarized in Table 12-5 of Part 2 of Safety Report. The monitoring sites are shown in Figure 12-7 and Figure 12-8 of Part 2 of Safety Report. Monitoring and sampling of the environment beyond the site boundary is also conducted by both federal and provincial government agencies.</p> <p>Management of the Off-Site Radiological Environmental Monitoring Program [BP-PROC-00076, R006] outlines the elements of the REMP. The REMP design includes the sampling or direct measurements in the significant pathways which contribute to the radiation dose to the public. The Bruce Power REMP is designed to meet the requirements of CSA N288.4-10, Guidelines for the Radiological Monitoring of the Environment.</p> <p>The EM7 - Radiological Environment Monitoring Program Routines [DPT-ENV-00007, R003] describes the process and methods for collecting and analyzing environmental samples, calculating dose to the public, and preparing reports.</p> <p>A high level assessment of CSA N288.4 is performed and</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		documented in Safety Factor 14.	
9.1	<p>A safety analysis of the plant design shall include hazard analysis, deterministic safety analysis, and probabilistic safety assessment (PSA) techniques. The safety analysis shall demonstrate achievement of all levels of defence in depth, and confirm that the design is capable of meeting the applicable expectations, dose acceptance criteria and safety goals.</p> <p>Radioactive sources other than the reactor core, such as the spent fuel pool and fuel handling systems, shall be considered. Impacts for multiple units at a site if applicable, shall be included.</p> <p>The first step of the safety analysis shall be to identify PIEs using a systematic methodology, such as failure modes and effects analysis. Both direct and indirect events shall be considered in PIE identification. Requirements and guidance for identification of PIEs is given in section 7.4 of this document.</p>	<p>New requirements have been introduced in the second and third paragraph of this clause.</p> <p>The radioactive sources other than the reactor core are not addressed in Part 3 of the Safety Report. A limited set of Fuel Handling System Failures is discussed in Appendix 1 Section 1.5 of Part 3 of the Safety Report. Therefore, it is assessed as a gap (Gap 1).</p> <p>Additional details, related to the requirements and guidance for identification of PIEs are provided in Safety Factor Report 5. The requirements of this clause relevant to probabilistic safety analysis are covered in detail in the assessment of CNSC REGDOC-2.4.2 as documented in Safety Factor 6.</p> <p>As for clause 7.4 requirements, systematic methodology for event identification is not demonstrated (Gap 2).</p>	Gap
9.2	<p>The safety analysis shall be iterative with the design process, and result in two reports: a preliminary safety analysis report, and a final safety analysis report.</p>	<p>New requirements for accounting the postulated aging effects and demonstration for sufficient design margins.</p> <p>As mentioned earlier the original safety analyses are based on the as built station. In the original design ageing effects are taken into account, usually by conducting conservative and bounding analyses. The condition of the pressure tubes,</p>	Gap


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The preliminary safety analysis shall assist in the establishment of the design-basis requirements for the items important to safety, and demonstrate whether the plant design meets applicable requirements.</p> <p>The final safety analysis shall:</p> <ol style="list-style-type: none"> <li>1. reflect the as-built plant</li> <li>2. account for postulated aging effects on SSCs important to safety</li> <li>3. demonstrate that the design can withstand and effectively respond to identified PIEs</li> <li>4. demonstrate the effectiveness of the safety systems and safety support systems</li> <li>5. derive the OLCs for the plant, including: <ol style="list-style-type: none"> <li>a. operational limits and set points important to safety</li> <li>b. allowable operating configurations, and</li> </ol> </li> </ol>	<p>as a result of fuel bundle wear, has been taken into account with new bundle designs and the consequences of this have been factored into the safety analyses. Current NSA and ageing management programs require safety analysis to be updated to reflect actual plant condition taking into consideration ageing effects on SSCs.</p> <p>The main gap is that AOOs acceptance criteria are not assessed separately since AOOs are not identified explicitly (Gap). For more details see assessment against CNSC REGDOC-2.4.1 requirements. Further details are presented in Safety Factor 5.</p> <p>The effectiveness of the safety systems and their support systems is demonstrated by showing that regulatory requirements are met and that releases to the public are within acceptable limits. The operational limits and conditions including setpoints for the process and control systems as well as all of the operator actions credited in the accident analysis are identified in the Safety Report.</p> <p>Plant operating limits and conditions are taken into account in the analysis assumptions and inputs of Part 3 of the Safety Report. Analysis of the main events impacted by ageing is revised to reflect plant conditions applicable to the licence duration. The results of new analysis are consistently used to demonstrate that dose and derived acceptance criteria are met: the design incorporates sufficient safety margins: and confirm the adequacy of the OLCs and if necessary used to derive a more suitable value for use as a new OLC. Operational limits and set points important to safety, allowable operating configurations, and constraints for operational procedures based on safety analysis are also documented in OP&amp;Ps and IMs. In addition, safety analysis</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>constraints for operational procedures</p> <p>6. establish requirements for emergency response and accident management</p> <p>7. determine post-accident environmental conditions, including radiation fields and worker doses, to confirm that operators are able to carry out the actions credited in the analysis</p> <p>8. demonstrate that the design incorporates sufficient safety margins</p> <p>9. confirm that the dose and derived acceptance criteria are met for all AOOs and DBAs</p> <p>10. demonstrate that all safety goals have been met</p> <p>Guidance</p> <p>The Class I Nuclear Facilities Regulations requires a preliminary safety analysis report demonstrating the adequacy of the NPP design to be submitted in support of an application for a</p>	<p>provides the inputs to determine post-accident environmental conditions, including radiation fields and worker doses, to confirm that operators are able to carry out the actions credited in the analysis.</p> <p>The requirements of this clause relevant to probabilistic safety analysis are covered in detail in the assessment of CNSC REGDOC-2.4.2. Further details are presented in Safety Factor 6.</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	licence to construct a Class I nuclear facility. A final safety analysis report demonstrating the adequacy of the design is required for an application for a licence to operate a Class I nuclear facility.		
9.3	<p>Hazard analysis shall collect and evaluate information about the NPP to identify the associated hazards and determine those that are significant and must be addressed. A hazard analysis shall demonstrate the ability of the design to effectively respond to credible common-cause events.</p> <p>As discussed in section 9.1, the first step of the hazard analysis is to identify PIEs. For each common-cause PIE, the hazard analysis shall identify:</p> <ol style="list-style-type: none"> <li>1. applicable acceptance criteria (i.e., the success path criteria)</li> <li>2. the hazardous materials in the plant and at the plant site</li> <li>3. all qualified mitigating SSCs credited during and following the event all non-qualified safety or safety support systems are assumed to fail,</li> </ol>	<p>There are no changes to this section.</p> <p>Section 2.5 of Bruce B Safety Report Part 2 (NK29-SR-01320-00001) describes design criteria for seismic events, missile protection, effects of pipe rupture and environmental qualification. All external and most internal hazards that could potentially serve as the initiator of common-cause events were subjected to a first level of screening in order to eliminate ones which are inapplicable to Bruce B or with too low a frequency. The first level screening report was submitted to CNSC staff in NK21-CORR-00531-09809/NK29-CORR-00531-10287. The remaining hazards were submitted to a second level screening (submitted in NK21-CORR-00531-10848/NK29-CORR-00531-11226) which eliminated from consideration for further assessment all but the following events:</p> <p>" Fire</p> <p>The detailed hazard analysis of protection against fire is documented in NK29-REP-71400-00004, NK29-REP-71400-00003 and NK29-REP-71400-00002. As well, Bruce Power has submitted in NK21-CORR-00531-11324/NK29-CORR-00531-11729 a Fire PRA report.</p> <p>" Earthquake</p> <p>The safety-related systems in Bruce B requiring seismic qualification against earthquakes are defined in Design Guide</p>	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>except in cases where their continued operation would result in more severe consequences</p> <p>4. operator actions and operating procedures for the event</p> <p>5. plant or operating procedure parameters for which the event is limiting</p> <p>The hazard analysis shall confirm that:</p> <p>1. the plant design incorporates sufficient diversity and separation to cope with credible common-cause events</p> <p>2. credited SSCs are qualified to survive and function during and following credible common-cause events, as applicable</p> <p>3. the following criteria are met:</p> <p>a. the plant can be brought to a safe shutdown state</p> <p>b. the integrity of the fuel in the reactor core can</p>	<p>NK29-DG-03650-002. The seismic qualification is carried out as per DPT-PDE-00017. As well, Bruce Power has submitted in NK21-CORR-00531-11324/NK29-CORR-00531-11729 a Seismic PRA Report.</p> <p>" Tornado;</p> <p>The risk from tornados is evaluated and addressed in Bruce Power Probabilistic Risk Assessment Guide - High Wind Hazard [B-REP-03611-00012, Rev 00, November 2012]. The Guide documents the high wind hazard assessment methodology suitable for application at multi-unit stations. The guide supports Bruce Power in its implementation of DIV-ENG-00010 [Probabilistic Risk Assessment Process, DIV-ENG-00010, R000].</p> <p>" External flooding and extreme waves.</p> <p>Bruce Power has submitted in NK21-CORR-00531-09969/NK29-CORR-00531-10409 a methodology for analysis tornados, high winds and external flooding, and has submitted in NK21-CORR-00531-11324/NK29-CORR-00531-11729 a High Wind PRA Report and an External Flooding Assessment.</p> <p>For fire hazards assessments, the fire protection goals are, as per CSA N293-12:</p> <p>(a) to minimize the risk of radiological releases to the public that are a result of fire;</p> <p>(b) to protect plant occupants from death or injury due to fire;</p> <p>(c) to minimize economic loss resulting from fire damage to structures, equipment, and inventories; and</p> <p>d) to minimize the impact of radioactive and hazardous</p>	

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>be maintained</p> <p>c. the integrity of the reactor coolant pressure boundary and containment can be maintained</p> <p>d. safety-critical parameters can be monitored by the operator</p> <p>The hazard analysis report shall include the findings of the analysis and the basis for those findings. This report shall also:</p> <ol style="list-style-type: none"> <li>include a general description of the physical characteristics of the plant that outlines the prevention and protection systems to be provided</li> <li>include the list of safe shutdown equipment</li> <li>define and describe the characteristics associated with hazards for all areas that contain hazardous materials</li> <li>describe the performance criteria for detection systems, alarm systems, and mitigation systems, including requirements such as seismic or environmental qualification</li> </ol>	<p>materials on the environment as a result of fire.</p> <p>" For common-mode hazards other than fires, the assessment acceptance criteria are to maintain the four basic nuclear safety functions (i.e. safely shutdown the reactor and maintain it in a safe shutdown condition; remove residual and decay heat from the reactor after shutdown; limit release of radioactive material and ensure that dose to public is within prescribed limits and ensure monitoring of safety-critical parameters).</p> <p>" Bruce Power's Environmental Safety Management program (BP-PROG-00.02) requires that all hazardous materials in the plant and on the site be identified so that its impact on the environment can be assessed. Thus, all of the hazardous material can be identified as required by this clause for any future hazards analyses.</p> <p>" Section 8.0 of NK29-DG-03650-002 defines the level of seismic qualification of all safety-related system components to ensure that the hazard acceptance criteria are met. The environmental qualification requirements for safety-related systems when subjected to the harsh environment of the most limiting DBA are defined in Appendices A and B of NK29-DG-03650-003.</p> <p>" In regards to point 4, the manual actions credited in the Fire Safe Shutdown Assessment have been identified in operating procedures as discussed in the compliance notes for clause 7.4.1. 4. Section 1.3 of Bruce B Safety Report Part 3 (NK29-SR-01320-00002) summarizes operator actions credits for various initiating events. Emergency Operating Procedures and the Abnormal Incidents Manual NK29-AIM-03600.1 address DBAs regardless of the hazard initiating the</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>5. describe the control and operating room areas and the protection systems provided for these areas, including additional facilities for maintenance and operating personnel</p> <p>6. describe the operator actions and operating procedures of importance to the given analysis</p> <p>7. identify the plant parameters for which the event is limiting</p> <p>8. explain the inspection, testing, and maintenance parameters needed to protect system integrity</p> <p>9. define the emergency planning and coordination requirements for effective mitigation, including any necessary measures to compensate for the failure or inoperability of any active or passive protection system or feature</p> <p>Guidance</p> <p>The objective of the hazard analysis is to determine the adequacy of protection of the NPP</p>	<p>DBA. For fires, the majority of the actions are via automated systems. However, the Fire Safe Shutdown Assessment FSSA (NK29-REP-71400-00003) identifies fire zones where manual actions could be credited, and identifies procedures needed to be updated to incorporate these operator actions.</p> <p>" Section 1.5 of Bruce B Safety Report Part 3 (NK29-SR-01320-00002) provides details of limiting parameters of all initiating events regardless of the hazard causing the accident.</p> <p>As per "Bruce B Location and Separation Requirements for Safety Related Systems" NK29-DG-29-03650-005, the Bruce B design incorporates diversity, redundancy and separation requirements, such as incorporation of a two-group philosophy applied to each of the basic safety functions (control, cool, contain, monitor) following common-mode effects. Only SSCs qualified to withstand conditions during and after credible initiating events are credited. The requirements to control, cool, contain and monitor the reactor are part of the success path of hazard analysis. Regarding the monitoring of safety-critical parameters, Bruce Power has constructed an SCA in each of the four reactor buildings and an additional common SCA in the Emergency Water and Power Supply Building. The purpose of these SCAs is to provide an alternate location for control and monitoring of the reactors should the MCR become unavailable. Thus, these parameters can be monitored following a fire The SCA has been designed to be seismically qualified and available for monitoring of safety-critical parameters.</p> <p>It is noted that there is no single Hazard Analysis Report which collects all the noted information in the elements of this paragraph. Instead, the information is listed in documents</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>against internal and external hazards, while taking into account the plant design and site characteristics. To ensure the availability of required safety functions and operator actions, all the SSCs important to safety (including the main control room, secondary control room and emergency support facilities) should be adequately protected against relevant internal and external hazards.</p> <p>The hazard analysis should establish a list of relevant internal and external hazards that may affect plant safety. For the relevant hazards, the review should demonstrate, by using deterministic and probabilistic techniques, that the probability or consequences of the hazard are sufficiently low so that no specific protective measures are necessary, or that the preventive and mitigating measures against the hazard are adequate.</p> <p>All internal and external hazards are considered as part of PIEs. The hazards that make an insignificant contribution to plant risk can be screened out from the detailed analysis; however, the rationale for this screening should be provided. The remaining PIEs constitute the scope of the hazard analysis. The design should specify design-basis hazards, establishing clear criteria. The design-basis hazards should be analyzed using the deterministic safety analysis</p>	<p>already cited in the assessment of the preceding paragraphs: NK29-SR-01320-00001, NK29-SR-01320-00002, BP-PROG-00.02, NK29-REP-71400-00003, NK29-REP-71400-00002, BP-PLAN-00001, NK29-AIM-03600.1.</p> <p>Detailed assessment is provided in Safety Factor 7 Hazard Analysis.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>rules and criteria</p> <p>provided in section 9.4. Such analysis should also demonstrate the adequacy of the complementary design features in mitigating radiological consequences of design extension conditions.</p> <p>The hazard analysis should demonstrate that the design incorporates sufficient safety margins.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>• CNSC, RD-346, Site Evaluation for New Nuclear Power Plants, Ottawa, Canada, 2008.</li> <li>• CNSC, RD/GD-369, Licence Application Guide: Licence to Construct a Nuclear Power Plant, Ottawa, Canada, 2011.</li> <li>• CSA Group, N293, Fire protection for nuclear power plants, Toronto, Canada, 2012.</li> <li>• CSA Group, N289.4, Testing procedures for seismic qualification of nuclear power plants, Toronto, Canada.</li> <li>• IAEA, NS-G-3.3, Evaluation of Seismic Hazards for Nuclear Power Plants, Vienna, 2002.</li> </ul>		




Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>IAEA, NS-G-1.5, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Vienna, 2003.</li> <li>IAEA, NS-G-3.1, External Human Induced Events in Site Evaluation for Nuclear Power Plants, Vienna, 2002.</li> <li>IAEA, NS-G-3.5, Flood Hazard for Nuclear Power Plants on Coastal and River Sites, Vienna, 2003.</li> <li>IAEA, NS-G-3.4, Meteorological Events in Site Evaluation for Nuclear Power Plants, Vienna, 2003.</li> <li>IAEA, SSG-18, Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations, Vienna, 2011.</li> <li>IAEA, NS-G-1.7, Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants, Vienna, 2004.</li> <li>IAEA, NS-G-1.11, Protection Against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, Vienna, 2004.</li> <li>IAEA, NS-G-1.6, Seismic Design and Qualification for Nuclear Power Plants, Vienna, 2003.</li> <li>IAEA, SSG-9, Seismic Hazards in Site Evaluation for Nuclear Installations, 2 Vienna, 2010.</li> </ul>		

Article No.	Clause Requirement	Assessment	Compliance Category
9.4	<p>The deterministic safety analysis shall be conducted in accordance with the requirements specified in CNSC regulatory document REGDOC-2.4.1, Deterministic Safety Analysis.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>• CNSC, REGDOC-2.4.1, Deterministic Safety Analysis, Ottawa, Canada, 2014.</li> <li>• CNSC, RD/GD-369, Licence Application Guide: Licence to Construct a Nuclear Power Plant, Ottawa, Canada, 2011.</li> <li>• CSA Group, N286.7.1, Guideline for the Application of N286.7-99, Quality Assurance of Analytical, Scientific, and Design Computer Programs for Nuclear Power Plants, Toronto, Canada.</li> <li>• CSA Group, N286.7, Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants, Toronto, Canada.</li> <li>• IAEA, SSG-2, Deterministic Safety Analysis for Nuclear Power Plants, Vienna, 2009.</li> <li>• IAEA NS-G-1.2, Safety Assessment and</li> </ul>	<p>The introductory remarks about the purpose of the deterministic safety analysis in RD-337 are deleted. A reference to CNSC REGDOC-2.4.1 instead of RD-310 is provided.</p> <p>A clause-by-clause assessment against CNSC REGDOC-2.4.1 identified gaps in the deterministic safety analysis that are related to event identification and classification, treatment of modeling uncertainty, and the use of legacy tools for some analysis.</p> <p>The results of the assessment are documented in Safety Factor 5.</p>	RNA


Article No.	Clause Requirement	Assessment	Compliance Category
	Verification for Nuclear Power Plants, Vienna, 2001.		
9.5	<p>The probabilistic safety assessment shall be conducted in accordance with the requirements specified in CNSC REGDOC-2.4.2, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> <li>ASME/ANS, RA-Sa-2009, Standard for Level 1/Large Early Release Frequency PRA for Nuclear Power Plant Applications, La Grange, Illinois, 2009.</li> <li>CNSC RD/GD-369, Licence Application Guide: Licence to Construct a Nuclear Power Plant, Ottawa, Canada, 2011.</li> <li>CNSC, REGDOC-2.4.2, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, Ottawa, Canada, 2014.</li> <li>IAEA, SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 2010.</li> </ul>	<p>The introductory remarks about the purpose of the probabilistic safety assessment in RD-337 are deleted. A reference to CNSC REGDOC-2.4.2 instead of S-294 is provided.</p> <p>A clause-by-clause assessment against CNSC REGDOC-2.4.2 is documented in Safety Factor 6.</p>	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>IAEA, SSG-4, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 2010.</li> <li>IAEA, Safety Series No. 50-P-10, Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 1995.</li> <li>IAEA Safety Reports Series No. 25, Review of Probabilistic Safety Assessments by Regulatory Bodies, Vienna, 2002.</li> <li>IAEA, Safety Series No. 50-P-7, Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 1995.</li> <li>IAEA, Safety Report Series No.10, Treatment of Internal Fires in Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 1998.</li> </ul>		
10.1	<p>The design shall make adequate provision to protect the environment and to mitigate the impact of the NPP on the environment. A review of the design shall confirm that this provision has been met.</p> <p>A systematic approach shall be used to assess the potential biophysical environmental effects of the NPP on the environment, and the effects of</p>	<p>There are no changes to the requirement.</p> <p>Section 2 Site Description of Part 1 of the Safety Report [NK29-SR-01320-00001, R005] describes the potential effect of the plant on population, agriculture, industry, transportation, fishing and recreation.</p> <p>The original Bruce B design did not incorporate explicitly the best available technology and techniques economically achievable principle as recommended in the guidance section (although it is recognized that this principle did not</p>	Gap

 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>the environment on the NPP.</p> <p>Guidance</p> <p>The design should incorporate the “best available technology and techniques economically achievable” (BATEA) principle for aspects of the design related to environmental protection.</p>	explicitly exist at the time). Therefore, it is assessed as a gap (Gap).	
10.2	<p>The design shall demonstrate through process, monitoring, control, prevention, and mitigation measures that the releases of nuclear and hazardous substances will conform to the ALARA principle.</p> <p>The lifecycle assessment shall identify various sources of nuclear and hazardous substances in design, operation, and decommissioning, along with their possible environmental impacts on human and non-human biota.</p> <p>Some of the factors that shall be considered include:</p> <p>1. resource requirements for the NPP such as fuel, energy, and water</p>	<p>A new requirement for pollution prevention is added to this clause.</p> <p>Bruce Power Environmental Management Policy documented in BP-MSM-1, R012 Management System Manual is the driver for implementing and improving the Bruce Power Environmental Safety Management Program and establishes guiding principles for environmental management and environmental performance for employees and those working on behalf of Bruce Power. The Environmental Management Policy reflects the commitment of Bruce Power's management to comply with applicable legal and other requirements, to prevent pollution, and to continually improve. Bruce Power's Environmental Safety Management program [BP-PROG-00.02 R009] requires that all hazardous materials in the plant and on the site be identified so that their impact on the environment can be assessed. A stated in section 4.7.4.3 of BP-PROG-00.02, R009, the Hazardous Waste Management and Disposal Requirements procedure [BP-PROC-00773, R002] provides the requirements for compliance with applicable federal, provincial, and municipal regulations. The Environmental Evaluation of Hazardous</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2. depletion of ground and surface water resources</p> <p>3. contamination of air, soil and water resources</p> <p>4. nuclear and hazardous substances used</p> <p>5. types of waste generated – gaseous, liquid and solid</p> <p>6. quantities of waste generated</p> <p>7. impact of cooling water intake on entrainment and impingement</p> <p>8. impact of water output on the thermal regime of the receiving environment</p> <p>Technological options shall be considered in establishing design objectives for controlling and monitoring releases during start-up, normal operation, shutdown, and potential abnormal and emergency situations. Appropriate limits shall be</p>	<p>Materials procedure DPT-ENV-0013 provides a guideline for performing environmental evaluations of the actual and potential impact of use of specific hazardous materials at the facility. Thus, all of the hazardous material can be identified as required by this clause for any future hazards analyses.</p> <p>DPT-ENV-00016, R006 Environmental Risk Assessment - Aspect/Impact, describes the process used for identifying and ranking environmental aspects (EAs) to determine which aspects are considered Significant Environmental Aspects (SEAs). Risks and compliance associated with SEAs are considered when setting environmental objectives and targets. Bruce Power maintains an EA database to assist in management of all environmental aspects, which are listed and reviewed on a regular basis.</p> <p>Items 7 and 8 were addressed in the Environmental Assessment for the New Fuel Project for Bruce B (i.e., Low Void Reactivity Fuel Design) [NK29-REP-07730-00001, R001, October 22, 2004]. Impingement and entrainment result from the withdrawal of water from Lake Huron through the intake structure located offshore at 13 m water depth. Entrainment refers to the capture of organisms within the Condenser Cooling Water (CCW) System. Impingement refers to the entrapment of aquatic organisms against the travelling screens (1 cm mesh) that prevent debris from entering the internal circulating water system (i.e., the component of the system that travels inside the built area of the station). Impinged organisms are removed from the station as waste debris. Peak impingement rates at large water-taking facilities in the Great Lakes are often associated with upwelling events. Entrained organisms are either removed from the natural population because they become</p>	


 <small>Division of Kinectrics Inc.</small>	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>included in the plant OLCs.</p> <p>Pollution prevention principles shall be applied when considering the technological design options for cooling water systems, in order to minimize adverse environmental impact.</p> <p>Guidance</p> <p>The design authority should demonstrate adherence to the principles of optimization and pollution prevention, through the demonstration of the application of the ALARA and BATEA principles.</p> <p>The lifecycle assessment referenced in this regulatory document should include an initial estimate of the total inventory of all radioactive and hazardous materials which will be used or generated during the plant's lifetime. All systems at the reactor site should be accounted for, and consideration given to substances such as hydrazine, carbon dioxide, chloro-fluoro-carbons, volatile organic compounds, nitrogen oxides, total organic carbon, dust or suspended solids, detergent, solvents, heavy metals (e.g., copper), chlorine, phosphorous, ammonia and ammonium, morpholine, oil, or grease. The nature of such</p>	<p>resident in the intake forebay, or, if they are small enough to pass through the intake screens are subjected to the mechanical effects of travelling through the CCW System through to the discharge channel. The Bruce B intake structure is fitted with a fish-deterrent chain-rope net designed to reduce intake of forage species, primarily alewife, rainbow smelt and gizzard shad. The specific effects of entrainment and impingement are discussed for each of the individual VECs selected for the assessment of the Aquatic Environment.</p> <p>As described in section 5.4.1.1 of the Environmental Assessment [NK29-REP-07730-00001, Rev. 001] the aquatic habitat may be directly affected by near-shore circulation resulting from existing operations of the Turbine Generator and Feedwater System (specifically, flow from the CCW System) and the Ancillary Systems (specifically, flow from the Service Water Supply System). As discussed in sub-section 4.4.3.1, intake of water to the Condenser Cooling Water (CCW) System and Service Water Supply System results in impingement and entrainment of aquatic organisms. Existing mitigation measures include the maintenance of a fish-deterrent chain-rope net over the intake structure which is designed to reduce impingement and entrainment of forage fish species. While exploratory analysis indicated that the fish deterrent is generally effective for the target species, it does not necessary result in a decrease in the overall impingement of all species. The assessment concluded that the effect of near-shore circulation from normal operations of Bruce B are not likely to have a residual adverse effect on the aquatic habitat which is limited to a small, isolated portion of the Local Study Area. Consequently, this effect is not considered further. Since there are no adverse effects, additional</p>	



Article No.	Clause Requirement	Assessment	Compliance Category
	<p>substances (solid, liquid, gas, pH, and temperature), their management and the wastes created should be accounted for.</p> <p>Pollution prevention principles should be conducted through an assessment of various technological options, in order to identify the technology and techniques that are BATEA. The technological option selected for the design of cooling water systems should minimize the impact on the environment to the extent practicable given nuclear safety requirements. The economically achievable assessment of a technology option is not determined on the basis of a specific project, but rather at the industry level. Technical feasibility of an option depends upon site-specific conditions taking into account environmental risk and socio-economic factors. The technology option of choice should be the one that best balances costs with environmental benefits resulting from application of a structured process of options analysis (e.g. cost-benefit analysis, multi criteria decision analysis). It should include an assessment of:</p> <ul style="list-style-type: none"> <li>the age of equipment and facilities involved</li> <li>how the option is designed, built, maintained, operated and decommissioned</li> </ul>	<p>mitigation measures are not considered or warranted.</p> <p>In addition as noted in [NK29-REP-07730-00001, R001, October 22, 2004] impingement and entrainment numbers have historically been low at Bruce B]. Higher impingement and entrainment have occurred at Bruce A, presumably due to its proximity to spawning habitat associated with shallow banks. Effects assessment for normal operations of Bruce B is discussed individually for each of the seven environmental components, first for adverse effects due to existing Bruce B operations and secondly, for the new or changed adverse effects due to the New Fuel Project. Malfunctions and accidents were assessed also.</p> <p>When the plant was designed, it was recognized that various systems would be required to control emissions to the environment and waste management systems were provided. The environmental reviews, as indicated above, demonstrate Bruce Power's commitment to review, identify, and deal with any ongoing significant environmental impacts from the station. For normal operation of the plant, the Derived Release Limits are documented in [BP-PROC-00171, R018]. As per recommendation and guidance related to condition 9.1 Environmental Protection Program of current Bruce A and B licence "... the licensee should review and, if necessary, revise and reissues the DRLs specified at least once per licence period." Bruce B Radiological Emission Levels are documented in Table 2, section 4.7.2 of BP-PROC-00171 Radiological Emissions Monitoring: Limits, Action Levels. Limits for release following accidents are included in the Appendix to the Operating Policies and Principles - Bruce B [BP-OPP-00001, R019] Principles as well as in the OSRs. Appropriate limits will be incorporated into the Safe Operating</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>the process employed</li> <li>the engineering aspects of the application of various types of control techniques</li> <li>process changes</li> <li>technological advances or changes in scientific knowledge and understanding</li> <li>cost of achieving the environmental benefits or reducing the environmental impacts</li> <li>socioeconomic factors</li> <li>time limits for installation of new and existing plants</li> <li>other environmental impacts (including energy requirements)</li> <li>other such factors as deemed appropriate by the regulator</li> </ul> <p>The selected condenser cooling technology should incorporate the latest in mitigation technology and techniques.</p> <p>Additional information</p> <p>Additional information may be found in:</p>	<p>Envelope Project documentation.</p> <p>Bruce Power's most recent updates to the Derived Release Limits (DRLs) for Bruce A and Bruce B were completed in accordance with the guidance and methodology specified in CSA N288.1-08, Update No. 1 and documented in Derived Release Limits and Action Levels for Bruce Nuclear Generating Station B [NK29-REP-03482-00003, Rev. 002]. The DRLs for Bruce A and B nuclear facilities are summarized in the Compliance Verification Criteria for Licence Condition 9.1 of the Licence Conditions Handbook [LCH-BNGS-R000]. In addition Bruce Power is targeting full compliance with N288.4 and N288.5 by December 31, 2018.</p> <p>As specified in the implementation strategy for licence condition 9.1 Environmental Protection Program of the Licence Condition Handbook "Bruce Power is in full compliance with all requirements of REGDOC 2.9.1, with two exceptions:</p> <ol style="list-style-type: none"> <li>1) There is currently no industry "best practice" for the assessment of risks related to non-human biota and there are gaps in Bruce Power's EMS in this regard. These gaps will be addressed with implementation of the N288 series.</li> <li>2) Administrative documentation updates are required.</li> </ol> <p>Consistent with the transition plan for the N288 series of standards, the foregoing actions are targeted for completion by December 31, 2018. No additional transition measures are required.</p> <p>Pollution prevention principles have been incorporated into Appendix A of the Bruce Power Environmental Management Policy documented in BP-MSM-1, R012 Management</p>	

	Rev Date: September 20, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00201-R00

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> <li>CNSC, G-296, Developing Environmental Protection Policies, Programs and Procedures at Class I Nuclear Facilities and Uranium Mines and Mills, Ottawa, Canada, 2006.</li> <li>CNSC, REGDOC-2.9.1, Environmental Protection: Policies, Programs and Procedures, Ottawa, Canada, 2013.</li> <li>CNSC P-223, Protection of the Environment, Ottawa, Canada, 2001.</li> </ul>	<p>System Manual, where it states that:</p> <p>"Bruce Power is committed to ... minimizing our environmental footprint in pursuit of target net zero by preventing pollution in the area of emissions, spills, waste and reducing impacts on the environment."</p>	