


Periodic Safety Review - Final Document Review Traveler



Bruce Power Document #: NK21-SFR-09701-00001	Revision: R001	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-421231-00011	Revision: R01
Supplier Document Title: Safety Factor 1 – Plant Design			

Accepted for use at Bruce Power by:	Signature:	Date
Name: Gary Newman Title: Chief Engineer & Sr. Vice President, Engineering		15 AUG. 2016.


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

Periodic Safety Review - Final Document Review Traveler

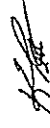
Sheet # 2 of 3

Bruce Power Document #:	NK21-SFR-09701-00001	Rev #: R001	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-421231-00011	Rev #: R01

Reviewed By:

Name	Title	Department	Signature	Date
Kevin Pickles	Division Manager	Station Engineering		Kevin Pickles P. Eng 2016.07.16 21:57:33 -04'00'

Recommended for Use By:



Name	Title	Department	Signature	Date
Kevin Pickles	Division Manager	Station Engineering		Kevin Pickles P. Eng 2016.07.16 21:58:49 -04'00'

Periodic Safety Review - Final Document Review Traveler


 Sheet # 3 of 3

Bruce Power Document #:	NK21-SFR-09701-00001	Rev #: R001	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-421231-00011	Rev #: R01

Reviewed By:

Name	Title	Department	Signature	Date
Jim Coady	Department Manager	I&C and Electrical		21 JUL 2016
Jim Slawson	Department Manager	Mechanical and Civil		21 JUL 2016

Recommended for Use By:

Name	Title	Department	Signature	Date
Gord Kozak	Division Manager	Engineering Support		21 July 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 #:

Reviewed By:				
Name	Title	Department	Signature	Date

Recommended for Use By:				
Name	Title	Department	Signature	Date

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 #:

Reviewed By:				
Name	Title	Department	Signature	Date

Recommended for Use By:			
Name	Title	Department	Date

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 #:

Reviewed By:				
Name	Title	Department	Signature	Date

Recommended for Use by:				
Name	Title	Department	Signature	Date

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 #:

Reviewed By:				
Name	Title	Department	Signature	Date

Recommended for Use By:				
Name	Title	Department	Signature	Date



Title: Safety Factor 1 - Plant Design




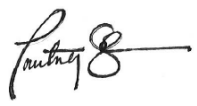




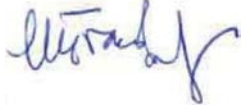

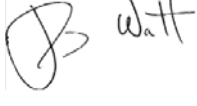
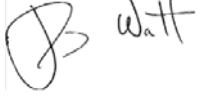
File: K-421231-00011-R01

NK21-SFR-09701-00001 R001

A Report Submitted to Bruce Power

July 8, 2016

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Issue	Reason for Issue:				
R00	For use				
Author: P. Ardenska	Verifier: G. Aldev	Reviewer: G. Archinoff	Approver: L. Watt	Date: Jul 23, 2015	
 M. Trandafirescu 	 C. Stallman 	 L. Watt 			
Issue	Reason for Issue:				
R01	High-level assessment of ANSI/NIRMA CM 1.0-2007, ASME BPVC Section III, ASME BPVC Section VIII, ASME B31.1, CSA N290.0-11, CSA N290.2-11, CSA N290.3-11, CSA N290.11-13 in Appendices A.6 to A.13, respectively. Sections 3.4, 3.5, 5.4, 7.1, 7.3, 8.0 and 9.0 updated based on these new assessments.				
Author: P. Ardenska	Verifier: G. Buckley	Reviewer: L. Watt	Approver: L. Watt	Date: Jul 8, 2016	
 M. Trandafirescu 					
Document Classification: Report		Security Classification: Client Proprietary			




 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Table of Contents


Acronyms and Abbreviations	vi
1. Objective and Description	1
1.1. Objective	1
1.2. Description	2
2. Methodology of Review	3
3. Applicable Codes and Standards	5
3.1. Acts and Regulations	5
3.2. Power Reactor Operating Licence	5
3.3. Regulatory Documents	9
3.4. CSA Standards	11
3.5. International Standards	17
3.6. Other Applicable Codes and Standards	18
4. Overview of Bruce Power Programs and Processes	20
4.1. Pressure Boundary Quality Assurance (PB QA) Program	23
4.1.1. Relevant Statutory, Regulatory, and Licensing Requirements Addressed by the Program	24
4.1.2. Implementing Procedures	25
4.2. Plant Design Basis Management	25
4.2.1. Relevant Statutory, Regulatory, and Licensing Requirements Addressed by the Program	26
4.2.2. Implementing Procedures	27
4.3. Engineering Change Control Program	28
4.3.1. Relevant Statutory, Regulatory, and Licensing Requirements Addressed by the Program	28
4.3.2. Implementing Procedures	30
4.4. Configuration Management	30
4.4.1. Relevant Statutory, Regulatory and Licensing Requirements Addressed by the Program	31
4.4.2. Implementing Procedures	31
5. Results of the Review	32
5.1. List of SSCs Important to Safety	32
5.2. Verification that Plant Design Supports Plant Safety and Performance	34
5.3. Identification of Differences Between Standards Met by NPPs Design and Modern Codes and Standards	35
5.3.1. Review Against Changes to CSA N287.1-14 General Requirements for Concrete Containment Structures for Nuclear Power Plants	36
5.3.2. Review Against Changes to CSA N287.3-14 Design Requirements for Concrete Containment Structures for Nuclear Power Plants	37
5.3.3. Review Against Changes to CSA N288.4-10 Environmental Monitoring Programs at Class I Nuclear Facilities and Uranium Mines and Mills	37
5.3.4. Review Against Changes to CSA N289.1-08 (R2013) General Requirements for Seismic Design and Qualification of CANDU Nuclear Power Plants	38

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

5.3.5.	Review Against Changes to CSA N289.2-10 Ground Motion Determination for Seismic Qualification of Nuclear Power Plants	39
5.3.6.	Review Against Changes to CSA N289.3-10 Design Procedures for Seismic Qualification of Nuclear Power Plants	39
5.3.7.	Review Against Changes to CSA N289.4-12 Testing Procedures for Seismic Qualification of Nuclear Power Plant SSCs	39
5.3.8.	Review Against Changes to CSA N289.5-12 Seismic Instrumentation Requirements for Nuclear Power Plants and Nuclear Facilities	40
5.3.9.	Review Against Changes to CSA N290.1-13 Requirements for the Shutdown Systems of Nuclear Power Plants	40
5.3.10.	Review Against CSA N291-08 (R2013) Requirements for Safety-Related Structures for CANDU Nuclear Power Plants	41
5.3.11.	Review Against CNSC REGDOC-2.5.2.....	41
5.4.	Adequacy of Design Basis Documentation.....	41
5.5.	Compliance with Plant Design Specifications	43
5.6.	Safety Analysis Report or Licensing Basis	45
5.7.	Plant SSCs Important to Safety	47
5.8.	Spent Fuel Storage Strategy	50
6.	Interfaces with Other Safety Factors	52
7.	Program Assessments and Adequacy of Implementation.....	53
7.1.	Self-Assessments	54
7.1.1.	SA-MPR-2014-08 SECNMMM Equipment Capability	56
7.1.2.	SA-COM-2014-01 Engineering Change Controls	57
7.1.3.	SA-COM-2014-03 Design Change Management.....	57
7.2.	Internal and External Audits and Reviews	58
7.2.1.	AU-2013-00015 PassPort Equipment Data Management.....	58
7.2.2.	AU-2013-00001 Pressure Boundary Quality Assurance Program Section 18 Audit.....	59
7.2.3.	AU-2012-00015 Critical Drawing Management.....	61
7.2.4.	AU-2012-00001 Pressure Boundary Quality Assurance Program Section 18 Audit.....	62
7.3.	Regulatory Evaluations and Reviews	63
7.3.1.	Action Item 2014-07-5211: Bruce A Electrical Power Systems Inspection BRPD-A-2014-004 [193].....	64
7.3.2.	CNSC Type II Compliance Inspection: Implementation of the Engineering Change Control Process [210].....	64
7.3.3.	CNSC Type II Compliance Inspection Report: BPRD-AB-2014-005 Fukushima Action Item Field Verification [185]	65
7.3.4.	Human Factors in Design Desktop Review – August 12-16, 2013 [196]	65
7.4.	Performance Indicators	65
8.	Summary and Conclusions	66
9.	References	71
	Appendix A – High-Level Assessments Against Relevant Codes and Standards	A-1
A.1.	CNSC G-149, Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors	A-1
A.2.	Changes to CSA N287.1-14, General Requirements for Concrete Containment Structures for Nuclear Power Plants	A-1


 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

A.3. CSA N287.3-14, Design Requirements for Concrete Containment Structures for Nuclear Power Plants	A-3
A.4. CSA N291-08 (R2013), Requirements for Safety-Related Structures for CANDU Nuclear Power Plants	A-4
A.5. NFPA-801 (2011), Standard for Fire Protection for Facilities Handling Radioactive Materials	A-5
A.6. ANSI/NIRMA CM 1.0-2007, Guidelines for Configuration Management of Nuclear Facilities	A-5
A.7. ASME BPVC Section III, Rules for Construction of Nuclear Power Plant Components A-18	
A.8. ASME BPVC Section VIII, Design and Fabrication of Pressure Vessels	A-21
A.9. ASME B31.1, Code for Power Piping	A-23
A.10. CSA N290.0-11, General Requirements for safety systems of nuclear power plantsA-25	
A.11. CSA N290.2-11, Requirements for emergency core cooling systems of nuclear plants	A-36
A.12. CSA N290.3-11, Requirements for the containment system of nuclear plants.....	A-47
A.13. CSA N290.11-13, Requirements for reactor heat removal capability during outage of nuclear power plants	A-59
Appendix B – Clause-by-Clause Assessments Against Relevant Codes and Standards B-1	
B.1. CSA N290.1-13, Requirements for the Shutdown Systems of CANDU Nuclear Power Plants.....	B-2
B.2. CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants.....	B-29

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


List of Tables

Table 1: Codes, Standards, and Regulatory Documents Referenced in Bruce A PROL and LCH	5
Table 2: Regulatory Documents	9
Table 3: CSA Standards	11
Table 4: International Standards	17
Table 5: Related Codes and Standards	18
Table 6: Bruce Power Programs Related to Plant Design	21
Table 7: Internal Self-Assessments and Audits Relevant to Plant Design	54
Table 8: Key Issues	67
Table B1: CSA N290.1-13, Requirements for the Shutdown Systems of CANDU Nuclear Power Plants.....	B-2
Table B2: CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plant	B-29


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Acronyms and Abbreviations


AECB	Atomic Energy Control Board
AHJ	Authority Having Jurisdiction
ANSI	American National Standards Institute
AOR	Analysis of Record
AWT	Accumulator Water Tanks
BDBA	Beyond Design Basis Accident
BP	Bruce Power
BPMS	Bruce Power Management System
CCAFF	Channel Cooling in the Absence of Forced Flow
CANDU	Canada Deuterium Uranium
CCI	Corium/Concrete Interaction
CM	Configuration Management
CNSC	Canadian Nuclear Safety Commission
COG	CANDU Owners Group
CSA	Canadian Standards Association
DBA	Design Basis Accident
DBE	Design Basis Earthquake
DCN	Design Change Notice
DCP	Design Change Package
DEC	Design Extension Conditions
DPO	Differing Professional Opinion
DRL	Derived Release Limit
DSA	Deterministic Safety Analysis
EA	Environmental Assessment
ECC	Engineering Change Control
EFPD	Effective Full Power Days
EFPH	Effective Full Power Hours
EQ	Environmental Qualification
EQSRCL	Environmental Qualification Safety Related Component List

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

ERGM	Engineering Representation of Ground Motion
ERP	Equipment Reliability Program
FASA	Focus Area Self Assessment
FCI	Facility Configuration Information
GIO	Global Improvement Opportunity
HFEPP	Human Factors Engineering Program Plan
IAEA	International Atomic Energy Agency
IBIF	Intermittent Buoyancy Induced Flow
IFB	Irradiated Fuel Bay
ISR	Integrated Safety Review
IST	Industry Standard Toolset
ITPs	Inspection and Test Plans
IUC	Instrument Uncertainty Calculation
LCH	Licence Conditions Handbook
LCMP	Life Cycle Management Plan
LOCA	Loss of Coolant Accident
LTEP	Long Term Energy Plan
MCR	Major Component Replacement
MCS	Maintenance Cooling System
MEL	Master Equipment List
MP	Maintenance Program
MSM	Management System Manual
NBC	National Building Code
NFC	National Fire Code
NIRMA	Nuclear Information and Records Management Association
NPP	Nuclear Power Plant
NSA	Nuclear Safety Assessment
NSAS	Nuclear Safety Analysis and Support
NSCA	Nuclear Safety and Control Act
OFI	Opportunities for Improvements
OLC	Operational Limit and Condition
OP&P	Operating Policies and Principles

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

OPEX	Operating Experience
OPRs	Overpressure Protection Reports
OSR	Operational Safety Requirement
PB	Pressure Boundary
PBQAP	Pressure Boundary Quality Assurance Program
PDE	Plant Design Engineering
PE	Procurement Engineering
PM	Preventative Maintenance
PRA	Probabilistic Risk Assessment
PROL	Power Reactor Operating Licence
PRVM	Pressure Relief Valve Manifold
PSA	Probabilistic Safety Assessment
PSR	Periodic Safety Review
QA	Quality Assurance
QPS	Qualified Power Supply
RLE	Review Level Earthquake
RS	Reactor Safety
SAI	Safety Analysis Improvement
SAM	Severe Accident Management
SAMG	Severe Accident Management Guidelines
SBR	Safety Basis Report
SCA	Safety and Control Area
SCR	Station Condition Record
SDC	Shutdown Cooling System
SDG2	Standby Diesel Generator 2
SFR	Safety Factor Report
SIS	Systems Important to Safety
SMA	Seismic Margin Assessment
SOE	Safe Operating Envelope
SQ	Seismic Qualification
SQUG	Seismic Qualification Utility Group
SRI	Safety Report Improvement

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

SRSL	Safety Related System List
SSCs	Structures, Systems, and Components
SSCTs	Structures, Systems, Components, and Significant Tools
TBD	Technical Basis Document
TMOD	Temporary Modification
TSSA	Technical Standards and Safety Authority

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

1. Objective and Description

Bruce Power (BP), as an essential part of its operating strategy, is planning to continue operation of Units 3 and 4 as part of its contribution to the Long Term Energy Plan (LTEP) (<http://www.energy.gov.on.ca/en/ltep/>). Bruce Power has developed plant life integration management plans in support of operation to 247,000 Equivalent Full Power Hours (EFPH). A more intensive Asset Management program is under development, which includes a Major Component Replacement (MCR) approach to replace 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 maintenance outage will be scheduled concurrently.

To support the definition and timing of practicable opportunities for enhancing the safety of Units 3 and 4, and the ongoing operation of Units 1 and 2, which have already been refurbished, Bruce Power is conducting a station-wide review of safety for Units 0A and 1-4, to be termed an Integrated Safety Review (ISR) [1]. This ISR supersedes the Bruce A portion of the interim Periodic Safety Review (PSR) that was conducted for the ongoing operation of the Bruce A and B units until 2019 [2]. This ISR is conducted in accordance with the Bruce A ISR Basis Document [1], which states that the ISR will meet or exceed the international guidelines given in International Atomic Energy Agency (IAEA) Guide SSG-25, Periodic Safety Review for Nuclear Power Plants [3]. The ISR envelops the guidelines in Canadian Nuclear Safety Commission (CNSC) Regulatory Document RD-360 [4], Life Extension for Nuclear Power Plants, with the exception of those related to the Environmental Assessment (EA), which has already been completed for Bruce A [5]¹.

1.1. Objective

The overall objective of the Bruce A ISR is to conduct a review of Bruce A against modern codes and standards and international safety expectations and provide input to a practicable set of improvements to be conducted during the Major Component Replacement in Units 3 and 4, and during asset management activities to support ongoing operation of all four units, including U0A, that will enhance safety to support long term operation. The look-ahead period will be longer than that in the interim PSR performed for Units 1-8 [2]. 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. Nuclear Safety is a primary consideration for Bruce Power and the management system must support the enhancement and improvement of safety culture and the achievement of high levels of safety, as well as reliable and economic performance.

¹ RD-360 [4] was superseded by CNSC REGDOC-2.3.3 [6] in April 2015. REGDOC-2.3.3 was in draft at the time that the ISR Basis Document [1] was prepared. The draft version of REGDOC-2.3.3 stated that it was consistent with SSG-25, and the assessments in the Safety Factor Reports were performed on that basis. The issued version of CNSC REGDOC-2.3.3 also states that it is consistent with SSG-25, and therefore it is considered that the ISR envelops the guidelines in CNSC REGDOC-2.3.3.

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 A ISR Basis Document [1], 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 ISR(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
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.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

2. Methodology of Review


As discussed in the Bruce A ISR Basis Document [1], the methodology for an ISR should include making use of safety reviews that have already been performed for other reasons. Accordingly, the Bruce A ISR 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];
- Proposed refurbishments of Bruce Units 3 and 4 (circa 2008) [10] [11] [12]; and
- Safety Basis Report (SBR) and Periodic Safety Review (PSR) for Bruce Units 1 to 8 (2013) [2].

These reviews covered many, if not all, of the same Safety Factors that are reviewed in the current ISR. A full chronology of Bruce Power safety reviews is provided in Appendix F of [13].


The Bruce A ISR 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 ISR Basis 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 ISR 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 confirming or modifying the assessment type for each of the codes and standards and guidance documents identified for consideration. The ISR 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.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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

4. **Perform gap assessment against codes and standards:** This step comprises the actual assessment of the Bruce Power programs and the Bruce A plant against the identified codes and standards. In general, this involves determining from available design or programmatic documentation whether the plant's design or programs 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 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 gap 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.
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 provide a cross section, intended to 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.
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 A 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.

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

3. Applicable Codes and Standards

This section lists the applicable regulatory requirements, codes and standards considered in the review of this Safety Factor. The list also includes any new codes or standards that came into effect after the completion of the 2013 PSR, as well as those that supersede codes or standards previously assessed. Regulatory codes and standards issued after the code effective date of August 31, 2014 were not part of the detailed review.

3.1. Acts and Regulations

The *Nuclear Safety and Control Act* (NSCA) [14] establishes the Canadian Nuclear Safety Commission and its authority to regulate nuclear activities in Canada. The NSCA has been amended on July 3, 2013 to provide the CNSC with the authority to establish an administrative monetary penalty system. The Administrative Monetary Penalties Regulations were introduced in 2013, and set out the list of violations that are subject to administrative monetary penalties, as well as the method and criteria for penalties administration. However, these changes do not impact this Safety Factor. Furthermore, following the Fukushima nuclear events of March 2011, the Fukushima Omnibus Amendment Project was undertaken and completed in 2012, and resulted in amendments to regulatory documents to reflect lessons learned from these events. Bruce Power has a process to ensure compliance with the NSCA [14] 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 Bruce Power Reactor Operating Licence (PROL) [15] and Licence Conditions Handbook (LCH) [16] are identified in Table 1². 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 PROL and LCH

Document Number	Document Title	Modern Version used for ISR Comparison	Type of Review
CNSC S-294 (2005)	Probabilistic Safety Assessment For Nuclear Power Plants	CNSC REGDOC-2.4.2 (2014) [19]	CBC

² PROL 18.00/2020 [17] and LCH-BNGS-R000 [18] came into effect on June 1, 2015. However, PROL 15.00/2015 [15] and LCH-BNGSA-R8 [16] are the versions referred to in this ISR, as these were in force when the assessments in the Safety Factor Reports were performed.

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Document Number	Document Title	Modern Version used for ISR Comparison	Type of Review
CNSC RD-360 (2008)	Life Extension Of Nuclear Power Plants	CNSC RD-360 [4]	NR
CSA N285.0-08	General Requirements For Pressure-Retaining Systems And Components In CANDU Nuclear Power Plants	CSA N285.0-12 [20]	NR
CSA N286-05 (R2011)	Management System Requirements for Nuclear Power Plants	CSA N286-12 [21]	NR
CSA N286.7-99	Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants	CSA N286.7-99 (R2012) [22]	NR
CSA N290.13 (R2010)	Environmental Qualification Of Equipment For CANDU Nuclear Power Plants	CSA N290.13 (R2010) [23]	NR
CSA N290.15-10	Requirements for the Safe Operating Envelope of Nuclear Power Plants	CSA N290.15-10 [24]	NR
CSA N293-07	Fire Protection For CANDU Nuclear Power Plants	CSA N293-12 [25]	HL
Assessment type: Clause-by-Clause (CBC); Code-to-Code (CTC); High Level (HL); No Assessment Required (NR); Confirm Validity of Previous Assessments (CV)			

CNSC REGDOC-2.4.2: CNSC REGDOC-2.4.2 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 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 ISR Basis Document calls for a code-to-code assessment between CNSC S-294 and CNSC REGDOC-2.4.2 to be performed; however, in view of the importance of CNSC REGDOC-2.4.2 as the primary regulatory document for PSA, a clause-by-clause review has been performed and documented in Safety Factor 6.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

CNSC RD-360: This ISR is being conducted as part of ongoing operation for Units 1 and 2 and to support Major Component Replacement of Units 3 and 4, so it also envelops the guidelines in RD-360, Life Extension for Nuclear Power Plants, issued February 2008. Therefore, RD-360 [4] *de facto* continues to provide guidance on how this review should be conducted. However, RD-360 [4] was superseded by CNSC REGDOC-2.3.3 [6] in April 2015, which was in draft at the time that the ISR Basis Document [1] was prepared. The draft version of CNSC REGDOC-2.3.3 stated that it was consistent with SSG-25, and the assessments in the Safety Factor Reports were performed on that basis. The issued version of CNSC REGDOC-2.3.3 also states that it is consistent with SSG-25, and therefore it is considered that the ISR envelops the guidelines in CNSC REGDOC-2.3.3.

CSA N285.0-12: Canadian Standards Association (CSA) N285.0-12 [20] provides general requirements for pressure-retaining systems and components. As part of the licence renewal application process, a transition plan is detailed in Licence Condition 6.1 of the LCH for Bruce A [16] to comply with the version of CSA N285.0 listed in the Document Version Control table within the LCH. Since the pressure boundary program spans many other programs and processes, CNSC staff requested a table or roadmap with programs/processes that affect the pressure boundary program [26]. This roadmap would be considered sufficient as a program document. A transition directly to the 2012 version (with update 1 and 2) is currently under development and is being managed as part of Bruce Power's transition program. Therefore, while Table C-1 of the ISR Basis Document [1] calls for a code-to-code assessment between the 2008 and 2012 editions to be performed, no further assessment of this code is required. More detail is provided in Section 4.1.1.

CSA N286-12: Table C-1 of the ISR Basis Document [1] calls for a code-to-code review against CSA N286-05. 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" [27].

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 next licensing period [28]. 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 [29]. Bruce Power further stated CSA N286-12 does not establish any significant or immediate new safety requirements that would merit a more accelerated implementation. 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.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

CSA N286.7-99: CSA N286.7-99 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 [30], 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 held by Bruce Power. Therefore, while Table C-1 of the ISR Basis Document [1] calls for the confirmation of validity of previous assessments of this code to be confirmed, it is concluded that no further assessment is required.

CSA N290.13: CSA N290.13 specifies the requirements for an environmental qualification program for Canada Deuterium Uranium (CANDU) Nuclear Power Plant (NPP). The modern version of this standard is the same as that referenced in the licence. Table C-1 of the ISR Basis Document [1] calls for the confirmation of validity of previous assessments of this code to be confirmed. However, since compliance with the licence is mandatory, a review against this standard is not performed for this Safety Factor.

CSA N290.15-10: CSA N290.15-10 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 support 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 [24]. The initial SOE objectives were to comply with COG-02-901 [31], which predates CSA N290.15; however, the requirements of CSA N290.15 were considered in the development of Bruce Power SOE program. A transition plan is being developed for phasing in the SOE program in the next licensing period and accordingly no further assessment against CSA requirements are performed in this ISR. The implementation and status update of the SOE program is further discussed in Section 5.4 of Safety Factor 5.

CSA N293-12: CSA N293-12 provides the minimum fire protection requirements for the design, construction, commissioning, operation, and decommissioning of CANDU NPPs. A recent review of the Bruce Power Fire Protection Program against CSA N293-07 has been performed [32] 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 [13]. Table C-1 of the ISR Basis Document [1] calls for a code-to-code assessment to be performed of the differences between CSA N293-12 [25] 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 corresponding equivalent in CSA N293-07. 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

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 [33].

3.3. Regulatory Documents

The Regulatory Documents in Table 2 were considered for application to review tasks of this Safety Factor.

Table 2: Regulatory Documents

Document Number	Document Title	Reference	Type of Review
CNSC R-10 (1977)	The Use of Two Shutdown Systems in Reactors	[34]	NR
CNSC R-77 (1987)	Overpressure Protection Requirements for Primary Heat	[35]	NR
CNSC G-149 (2000)	Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors	[30]	HL
CNSC RD-346	Site Evaluation for New Nuclear Power Plants	[36]	NR
CNSC REGDOC-2.5.2 (2014)	Design of Reactor Facilities: Nuclear Power Plants	[37]	CBC
Assessment type: Clause-by-Clause (CBC); Code-to-Code (CTC); High Level (HL); No Assessment Required (NR); Confirm Validity of Previous Assessments (CV)			

CNSC R-10: CNSC R-10 [34] provides requirements for the shutdown systems in reactors. 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 recently 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

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

environment and as such during FY 2012-13 [38] it was identified that it is not necessary to maintain CNSC R-10 and it can be withdrawn and archived. Table C-1 of the ISR Basis Document [1] calls for the confirmation of validity of previous assessments of this code to be performed. However, since a clause-by-clause assessment of the latest edition (i.e., 2013) of CSA N290.1 standard is performed and documented in Appendix B (B.1), review against CNSC R-10 was not repeated for this Safety Factor.

CNSC R-77: CNSC R-77 [35] provides overpressure protection requirements for primary heat transport systems in CANDU power reactors fitted with two shutdown systems. This regulatory document provides guidance related to overpressure protection and thus is relevant to design. Table C-1 of the ISR Basis Document [1] calls for the confirmation of validity of previous assessments of this code to be performed. A review of Bruce A against the requirements of CNSC R-77 has demonstrated that Bruce A design fully meets the requirements [8]. This guide has not been revised since the Bruce 1 and 2 ISR and therefore the results from that review remain applicable.

CNSC G-149: CNSC G-149 [30] 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 ISR and documented in Safety Factor 5. A summary of the assessment findings is presented in Appendix A (A.1).

CNSC RD-346: CNSC RD-346 [36] came into effect after the Bruce 1 and 2 ISR. This regulatory document covers evaluation of sites for new nuclear power plants (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 IAEA in NS-R-3 "Site Evaluation for Nuclear Installations" [39]. The latest assessment was performed in the 2008 Bruce 3 and 4 ISR, which stated that the regulatory document came into effect after the Bruce 1 and 2 ISR, where "[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" as per NK21-CORR-00531-04636 [40]. The same logic applies to CNSC RD-346, and therefore, while Table C-1 of the ISR Basis Document [1] calls for the confirmation of validity of previous assessments of this code to be performed, no further assessment in support of this Safety Factor is required.

CNSC REGDOC-2.5.2: CNSC REGDOC-2.5.2 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-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 ISR Basis Document [1] calls for a code-to-code assessment between RD-337 and CNSC REGDOC-2.5.2 to be performed. However, to obtain greater confidence, it was determined that a clause-by-clause review of the current version of this standard is more appropriate. The findings of the CNSC REGDOC-2.5.2 compliance assessment are documented in Appendix B (B.2).


 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

3.4. CSA Standards


The CSA has issued standards that form the basis of the Quality Assurance (QA) programs for all Canadian nuclear power plants. These high-level documents are used primarily as a foundation or basis on which nuclear utility operators have developed specific, internal policies, programs, and procedures. The CSA Standards listed in Table 3 are relevant to plant design.

Table 3: CSA Standards

Document Number	Document Title	Reference	Type of Review
CSA B51-14 (2014)	Boiler, Pressure Vessel, and Pressure Piping Code	[41]	NR
CSA N285.2-99 (R2004)	Requirements for Class 1C, 2C, and 3C Pressure-Retaining Components and Supports in CANDU Nuclear Power Plants	[42]	NR
CSA N287.1-14	General Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants	[43]	HL
CSA N287.2-08 (R2013)	Material Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants	[44]	NR
CSA N287.3-14	Design Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants	[45]	HL
CSA N287.4-09	Construction, Fabrication, and Installation Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants	[46]	NR
CSA N287.5-11	Examination and Testing Requirements for Concrete Containment Structures for Nuclear Power Plants	[47]	NR
CSA N288.4-10	Environmental Monitoring Programs at Class I Nuclear Facilities and Uranium Mines and Mills	[48]	HL

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Document Number	Document Title	Reference	Type of Review
CSA N289.1-08	General Requirements for Seismic Design and Qualification of CANDU Nuclear Power Plants	[49]	HL
CSA N289.2-10	Ground Motion Determination for Seismic Qualification of Nuclear Power Plants	[50]	HL
CSA N289.3-10	Design Procedures for Seismic Qualification of CANDU Nuclear Power Plants	[51]	CTC
CSA N289.4-12	Testing Procedures for Seismic Qualification of CANDU Nuclear Power Plants	[52]	CTC
CSA N289.5-12	Seismic Instrumentation Requirements for CANDU Nuclear Power Plants	[53]	CTC
CSA N290.0-11 (2011)	General Requirements for safety systems of nuclear power plants	[54]	HL
CSA N290.1 (2013)	Requirements for the Shutdown Systems of CANDU Nuclear Power Plants	[55]	CBC
CSA N290.2-11 (2011)	Requirements for emergency core cooling systems of nuclear power plants	[56]	HL
CSA N290.3-11 (2011)	Requirements for the containment system of nuclear power plants	[57]	HL
CSA N290.4-11	Requirements for Reactor Control Systems of Nuclear Power Plants	[58]	CV
CSA N290.5 (2006; Reaffirmed 2011)	Requirements for Electrical Power and Instrument Air Systems of CANDU Nuclear Power Plants	[59]	CV
CSA N290.6-09	Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of an Accident	[60]	CV

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Document Number	Document Title	Reference	Type of Review
CSA N290.11-13 (2011)	Requirements for reactor heat removal capability during outage of nuclear power plants	[61]	HL
CSA N291-08 (R2013)	Requirements for Safety-Related Structures for CANDU Nuclear Power Plants	[62]	HL
Assessment type: Clause-by-Clause (CBC); Code-to-Code (CTC); High Level (HL); No Assessment Required (NR); Confirm Validity of Previous Assessments (CV)			

CSA B51-14: CSA B51-14 provides requirements for boilers, pressure vessels, pressure piping and fittings. Table C-1 of the ISR Basis Document [1] calls for a code-to-code assessment between the 2009 and 2014 editions of the code to be performed. Bruce Power has performed an assessment regarding the transition from B51 2003 edition to the 2009 edition (Enclosure 1 of NK21-CORR-00531-10576/NK29-CORR-00531-10975 [13]). CSA B51 has not been referenced in the PROL or LCH; however, specific clauses are invoked by CSA-285.0. The transition plan for CSA N285.0-12 by extension is applied to the relevant clauses of CSA B51-09, therefore compliance with N285.0-12 will infer compliance with B51-09 and therefore B51-09 was not assessed further for the purpose of this review.

CSA N285.2-99: Table C-1 of the ISR Basis Document [1] calls for a high level assessment of CSA N285.2-99 to be performed. However, this standard no longer exists as a separate publication; it is incorporated as normative (mandatory) Annex I of CSA N285.0-08 and therefore assessment of this code is not required.

CSA N287.1-14: CSA N287.1-14 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 ISR Basis Document [1] calls for a code-to-code assessment between the 1993 and 2014 editions of the code to be performed. A code-to-code followed by a clause-by-clause assessment has been performed in Safety Factor 4: Ageing. In support of the review tasks of Safety Factor 1, to obtain greater confidence, a high-level review of the current version of this standard was performed. The results of this review are presented in Appendix A (A.2).

CSA N287.2-08, CSA N287.4-09, CSA N287.5-11: CSA N287.2-08 [44], CSA N287.4-09 [46], CSA N287.5-11 [47] address requirements for the materials, construction, fabrication, installation, examination and testing of concrete containment structures. As noted in the 2013 assessment [2], in applying these standards, the relevant systems important to safety are the parts of the Bruce A 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

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 (DBAs) and events in Units 3 and 4 is established by Part 3 of the Bruce A Safety Report [63]. In the restart of Units 3 and 4 in 2003 / 2004, demonstration of the adequacy of the containment design relied on earlier analysis of containment response to accident conditions. The restart safety analysis concluded that the predicted fission product release following postulated DBAs for the restarted Units was bounded by the earlier analyses, thus the adequacy of containment design was not impacted. No new construction or permanent modifications have been made to the containment structures to necessitate compliance of the containment construction to the new standards [2]. Table C-1 of the ISR Basis Document [1] calls for a confirmation of validity of previous assessments of CSA N287.2-08, CSA N287.4-09, and CSA N287.5-11. However, due to reasons explained above, review against these codes was not repeated as part of this Safety Factor.

CSA N287.3-14: CSA N287.3-14 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 ISR Basis Document [1] calls for a code-to-code assessment between the 1993 and 2014 editions of this code to be performed. However, to obtain greater confidence, it was determined that a high-level review of the current version of this standard is more appropriate. The results are presented in Appendix A (A.3).

CSA N288.4-10: CSA N288.4-10 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: Radiological Impact on the Environment. Conformance to this standard or to its predecessor N288.4-M90 is not currently a condition of the PROL; however, the CNSC has notified Bruce Power that they expect an implementation strategy and transition provisions to be submitted for N288.4-10 [64]. Table C-1 of the ISR Basis Document [1] calls for a clause-by-clause assessment of this code to be performed. Given the above statement, it has been reviewed only with respect to Bruce Power's progress towards implementation, and therefore the review type was changed from clause-by-clause to high level. The results are provided in Section 5.3.3.

CSA N289.1-08: CSA N289.1-08 [49] defines a seismic success path as the "minimum set of SSCs that can perform the required nuclear safety functions following an earthquake." The Bruce 3 and 4 success path is defined in the seismic margin assessment [65] and subsequently accepted by the CNSC in [66]. With respect to CSA N289.1-08 [49], the adequacy of the plant design to accommodate seismic events is addressed via the Bruce Units 3 and 4 Seismic Margin Assessment [65] and the seismic probabilistic risk assessment (PRA). The seismic PRA was updated to address post-Fukushima action items [67], [68]. Table C-1 of the ISR Basis Document [1] calls for a confirmation of validity of previous assessments of this code to be performed. However, to obtain greater confidence, it was determined that a high level review of the current version of this standard and its effect on Bruce Power's Seismic Margin Assessment approach is more appropriate. This is documented in Section 5.3.4.

CSA N289.2-10: CSA N289.2-10 describes the investigations required to obtain the seismological and geological information necessary to determine, for a proposed or existing

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 have a direct or indirect effect on plant safety or operation. A high-level review of updates within CSA N289.2-10, and its effect on Bruce Power's Seismic Margin Assessment approach, is documented in Section 5.3.5.

CSA N289.3-10: CSA N289.3-10 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. Table C-1 of the ISR Basis Document [1] calls for a code-to-code assessment between the 2008 and 2010 editions to be performed. However, to obtain greater confidence, it was determined that a high level review of updates of the current version of this standard and its effect on Bruce Power's Seismic Margin Assessment approach is more appropriate. This is documented in Section 5.3.6.

CSA N289.4-12: CSA N289.4-12 provides design requirements and methods for seismic qualification of specific components and systems by testing methods. A code-to-code assessment of the differences between the 2008 and 2012 editions was performed, followed by a high-level review of identified updates within CSA N289.4-12, and its effect on Bruce Power's Seismic Margin Assessment approach. The result of this assessment is documented in Section 5.3.7.

CSA N289.5-12: CSA N289.5-12 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 and associated findings are addressed in Section 5.3.8.

CSA N290.0-11: CSA N290.0-11 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 applies to the design, procurement, installation, commissioning, operation, testing, and maintenance requirements of reactor shutdown systems (SDSs) for existing and new water-cooled NPPs. Table C-1 of the ISR Basis Document [1] calls for a code-to-code assessment between the 2001 and 2013 editions to be performed. However, due to the amount of changes in the new code, a clause-by-clause review of the new version is more appropriate. The results are presented in Appendix B (B.1).

CSA N290.2-11: CSA N290.2-11 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 (ECC) system for a water-cooled nuclear power plant. The standard also applies to all support systems required to ensure that the ECC system is able to maintain adequate heat transfer for as long as necessary to maintain the release of

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

radioactive material within reference dose limits by limiting fuel failure. The results of a high-level review of this standard are presented in Appendix A (A.11).

CSA N290.3-11: CSA N290.3-11 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 of this standard are presented in Appendix A (A.12).

CSA N290.4-11: CSA N290.4-11 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 PSR assessment [2], which identified new or different clauses. These clauses 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. Therefore, review against CSA N290.4 was not repeated for this Safety Factor.

CSA N290.5-06: CSA N290.5-06 (R2011) covers the design, procurement, qualification, construction, installation, inspection, and documentation of CANDU NPP electrical power and instrument air systems. This guide was reviewed as a clause-by-clause assessment in the 2013 PSR, where one gap was identified. That assessment stated “As was noted in the Bruce 3 and 4 ISR, a project to provide a redundant air supply to all Airlocks and Transfer Chambers was underway. This remains to be completed, and thus this previously identified non-compliance is identified as issue SF1-11 in Table 5-6.” This gap was captured as a Global Improvement Opportunity (GIO), in which Bruce Power informed the CNSC that reliability upgrades are planned for completion prior to the re-start of Units 3 and 4 after life extension refurbishment [69]. This GIO was deferred to the Units 3 and 4 Refurbishment outage and was not considered in the IIP for the current licence period. The modification has been partially installed but not fully completed, and the associated GIO has been considered as closed per the supporting documentation for [70]. Therefore, the review against CSA N290.5-06 (R2011) was not repeated for this Safety Factor.

CSA N290.6-09: CSA N290.6-09 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 PSR assessment [2], where no gaps were identified. There have been no revisions or updates of the standard and the review remains applicable. Therefore, review against CSA N290.6-09 was not repeated for this Safety Factor.

CSA N290.11-13: CSA N290.11-13 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).

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

CSA N291-08: CSA N291-08 (R2013) provides material, design, construction, fabrication, inspection, and examination requirements for safety-related structures constructed of structural steel, reinforced concrete, and reinforced masonry. Upon review of this standard, it was deemed that a clause-by-clause assessment (as identified in Table C-1 of the ISR Basis Document [1]) was not necessary, given the existing action item related to the implementation program for this standard. Therefore, a high-level review of the standard and associated findings was performed and the results are presented in Appendix A (A.4).

3.5. International Standards

The international standard listed in Table 4 is relevant to this Safety Factor and was considered for this review.

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	[71]	HL
ASME BPVC Section III	Rules for Construction of Nuclear Power Plant Components	[72]	HL
ASME BPVC Section VIII	Design and Fabrication of Pressure Vessels	[72]	HL
ASME B31.1	Code for Power Piping	[72]	HL
IAEA SSG-25	Periodic Safety Review For Nuclear Power Plants	[3]	NR
Assessment type: Clause-by-Clause (CBC); Code-to-Code (CTC); High Level (HL); No Assessment Required (NR); Confirm Validity of Previous Assessments (CV)			

ANSI/NIRMA CM 1.0-2007: ANSI/NIRMA CM 1.0-2007 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 the high-level review are presented in Appendix A (A.6).

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

ASME BPVC Section III: ASME BPVC Section III establishes rules of safety governing the design, fabrication and inspection of boilers and pressure vessels, including nuclear power systems. The results are presented in Appendix A (A.7).

ASME BPVC Section VIII: ASME BPVC Section VIII 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 are presented in Appendix A (A.8).

ASME B31.1: ASME B31.1 prescribes minimum requirements for the design, materials, fabrication, erection, test, and inspection of power and auxiliary service piping systems for electric generation stations. The results are presented in Appendix A (A.9).


IAEA SSG-25: IAEA SSG-25 [3] addresses the periodic safety review of nuclear power plants and is the governing document for the review of the ISR, as identified in the Bruce A ISR Basis Document [1]. It defines the review tasks that should be considered for this Safety Factor. However, no assessment is performed specifically on IAEA SSG-25.

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	[73]	NR
Darlington DG-38-03650-2A	Common Mode Incidents – Overview and Design Requirements	[74]	NR
Darlington DG-38-03650-2B	Common Mode Incidents – Seismic Design	[75]	NR
Darlington DG-38-03650-3	Limiting Consequential Damage of Postulated Pipe Ruptures	[76]	NR
Darlington DG-38-03650-4	Shutdown Systems	[77]	NR
Darlington DG-38-03650-5	Emergency Coolant Injection	[78]	NR
Darlington DG-38-03650-6	Containment	[79]	NR

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Document Number	Document Title	Reference	Type of Review
Darlington DG-38-03650-7	Extensions of the Containment Envelope	[80]	NR
Darlington DG-38-03650-8	Environmental Qualification of Safety Related Equipment	[81]	NR
Darlington DG-38-03650-9	Safety Assessments	[82]	NR
NBCC (2010)	National Building Code of Canada	[83]	NR
NFCC (2010)	National Fire Code of Canada	[84]	NR
NFPA-801	Standard for Fire Protection for Facilities Handling Radioactive Material	[85]	HL
Assessment type: Clause-by-Clause (CBC); Code-to-Code (CTC); High Level (HL); No Assessment Required (NR); Confirm Validity of Previous Assessments (CV)			

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 [8]). These documents have not been revised since the Bruce 1 and 2 ISR or the Bruce Power 2013 PSR, nor have the Bruce Power programs or design changed in a manner that would invalidate the applicability of the assessment for the purpose of this review. The results of the Bruce 1 and 2 reviews remain applicable to Bruce 3 and 4; in which no gaps were identified. Therefore, review against the Darlington Design Guides was not repeated for this Safety Factor.

National Building Code: The National Building Code (NBC) [83] 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 [86]). 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.

Table C-1 of the ISR Basis Document [1] calls for a code-to-code assessment of the 2005 and 2010 editions of this code to be performed. However, as explained above, it was concluded that further assessment of this code is not required for this Safety Factor.

National Fire Code: The National Fire Code (NFC) [84] contains technical requirements designed to provide an acceptable level of fire safety. It complements the NBC, and both must

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

be considered when constructing, renovating or maintaining buildings. The NFC, as well as fire protection related portions of the NBC were reviewed as part of the CSA N293 Gap Assessment [32] discussed above. This approach was taken because the provisions of CSA N293 are considered to be bounding those of the NFC. This also applies to Bruce 3 and 4.

Table C-1 of the ISR Basis Document [1] calls for a code-to-code assessment of the 2005 and 2010 editions of this code to be performed. However, as explained above, it was concluded that further assessment of this code is not required for this Safety Factor. Additionally, a comprehensive review against CSA N293-12 is provided in Safety Factor 7.

NFPA-801: NFPA-801 Standard for Fire Protection for Facilities Handling Radioactive Materials [85] addresses fire protection requirements intended to reduce the risk of fires and explosions at facilities handling radioactive materials. Table C-1 of the ISR Basis Document [1] calls for a code-to-code assessment of the 2008 and 2014 editions of this code to be performed. However, since the requirements of this code are incorporated into CSA N293-12, it was concluded that a high-level review is more appropriate. This is presented in Appendix A (A.5).

4. Overview of Bruce Power 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) [88] and associated MSM Sheets [89] [90]. As stated in BP-MSM-1 [88], 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 [91] 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 [88] and define regulatory and business requirements. BP-MSM-1 Sheet 0001 [89] 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 [89] under the functional area of Configuration Management Engineering. The Program document, Program name, Accountable program owner, Accountable document approver and CNSC Notification requirements are defined in [89]. The related program documents are listed in Table 6³.

³ Table 6 lists the key governance documents used to support the assessments of the review tasks for this Safety Factor Report. There is a continual process to update the governance documents; document versions may differ amongst individual Safety Factor Reports depending on the actual assessment review date. A full set of current sub-tier documents is provided within each current PROG document.



 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Table 6: Bruce Power Programs Related to Plant Design

First Tier Documents	Second Tier Documents	Third Tier Documents	Fourth Tier Documents
BP-MSM-1: Management System Manual [88]	BP-PROG-00.04: Pressure Boundary Quality Assurance Program [26]	BP-PROC-00915: Pressure Boundary Quality Assurance Program Oversight [96]	
	BP-PROG-10.01: Plant Design Basis Management [92]	BP-PROC-00335: Design Management [97]	
		BP-PROC-00363: Nuclear Safety Assessment [98]	
		DIV-ENG-00009: Design Authority [99]	
		BP-PROC-00582: Engineering Fundamentals [100]	
		BP-PROC-00502: Resolution of Differing Professional Opinions [101]	
	BP-PROG-10.02: Engineering Change Control (ECC) [93]	BP-PROC-00743: Site Services Engineering Change Control [102]	
		BP-PROC-00542: Configuration Information Change [103]	
		BP-PROC-00539: Design Change Package [104]	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

First Tier Documents	Second Tier Documents	Third Tier Documents	Fourth Tier Documents
		BP-PROC-00877: Modification Installation Quality Assurance [105]	
		BP-PROC-00615: Commissioning Modifications and Projects [106]	
	BP-PROG-10.03: Configuration Management [95]	BP-PROC-00470: Configuration Management Program Oversight and Trending [107]	
		BP-PROC-00584: PASSPORT Equipment Data Management [108]	
		BP-PROC-00638: Temporary Configuration Change Management [109]	
		BP-PROC-00647: PassPort Permit Request Processing [110]	
		BP-PROC-00786: Margin Management [111]	
		BP-PROC-00898: Equipment Codes [112]:	
		SEC-DO-00001: Drafting Office Work Management [113]	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

First Tier Documents	Second Tier Documents	Third Tier Documents	Fourth Tier Documents
	BP-PROG-11.01: Equipment Reliability [94]	BP-PROC-00778: Scoping and Identification of Critical SSCs [114]	DPT-RS-00012: Systems Important to Safety (SIS) Decision Methodology [115]
		BP-PROC-00169: Safety Related System List ⁴ [116]	

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

4.1. Pressure Boundary Quality Assurance (PB QA) Program

The PB QA Program 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 for the scope of activities specified.

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. These are conducted in accordance with CSA N285.0 [20]. Conventional pressure boundary activities apply to work performed in non-nuclear class registered systems. Activities on systems within Bruce A are conducted in accordance with CSA N285.0 [20]. Centre of Site activities, including the steam pipeline to the Bruce Energy Centre are performed in accordance with CSA B51 [41].

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 [92] and Engineering Change Control Program [93], together with associated implementing procedures, comply with the requirements of this PB QA Program Section 3.

The elements of PB QA design control are:

- Design process, including:

⁴ BP-PROC-00169 Section 5.2 does not identify the PROG where it takes its authority. This is identified as gap SF8-10. This gap is therefore not repeated in context of this Safety Factor.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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

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

BP-PROG-00.04 [26] 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. The document does, however, identify 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.

This Program does not apply to relief valve testing and repair conducted under Bruce Power Procedure BP-PROC-00078 *Quality Program Manual for Testing and Repair of Pressure Relief Valves* (R006, 16 September 2013). The Program does not apply to inaugural and periodic

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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.

Bruce Power is reviewing the changes from the 2008 edition of CSA N285.0 to the 2012 edition of the standard to identify the impact on its Pressure Boundary Quality Assurance Program 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 current LCH (as exceptions in the Quality Assurance requirements cited in the Compliance Verification Criteria of LCH Section 6.2) and within Bruce Power's Pressure Relief Valve Testing and Repair Program, Bruce Power is compliant with 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 is targeting revisions to BP-PROG-00.04 for alignment with N285.0-12 including updates No. 1 and No. 2 by mid-2015. This includes obtaining Technical Standards and Safety Authority (TSSA) approval of the revised program manual [33].

Bruce Power is targeting implementation of the updated PBQA Program manual, compliant with 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 TSSA approved PBQA Program manual (BP-PROG-00.04), procedural updates and training must be completed within six months; however, Bruce Power is currently targeting full implementation by the end of August 2015. When implementation is complete, Bruce Power will also complete and submit a roadmap of the PBQA Program that meets the requirements of Annex N *Pressure Boundary Program Document* of the updated N285.0 standard [33].

4.1.2. Implementing Procedures

The processes identified in PB QA Program 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 [96], PB QA Program Oversight.

4.2. Plant Design Basis Management

The objective of the plant design basis management program 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 [26], PB QA. Additionally, this program sets out requirements for engineering analysis and

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

documentation, such that the adequacy of the design can be demonstrated. At Bruce Power, effective June 1st, 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.

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

As identified in Section 5.1 of the Program, 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 A Nuclear Power Reactor Operating Licence PROL 15.00/2014;
- Bruce B Nuclear Power Reactor Operating Licence PROL 16.00/2014;
- CSA N285.0-08/N285.6 Series-08 (with Update No. 1, June/09); and
- CSA N286-05, specifically:
 - Clauses 5.5, 5.8, 5.9 and 5.10 - Management System Generic Requirements;
 - 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 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 [93] provides a mapping of relevant Statutory, Regulatory and Licensing Requirements to procedures demonstrating compliance. No gaps are identified in the Appendix.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


4.2.2. Implementing Procedures

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

- BP-PROC-00335, Design Management [97]:
 - 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 [98] to ensure that nuclear safety requirements are incorporated into the design.
- BP-PROC-00363, Nuclear Safety Assessment [98]:
 - 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.
- DIV-ENG-00009, Design Authority [99]:
 - Outlines the processes by which the Chief Engineer and Senior Vice President, Engineering execute the role of Design Authority.
- BP-PROC-00582, Engineering Fundamentals [100]:
 - 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 [101]:
 - Provides a process to initiate, track and resolve a Differing Professional Opinion (DPO) 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 [117], 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 [118], Trend Identification and Reporting of SCRs.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 [93] 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 [92] 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;
- SSCTs to be abandoned in place, removed or demolished; and
- Changes that affect documentation only.

The ECC Program 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 [93] 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 Program, the relevant Statutory, Regulatory and Licensing Requirements addressed by the Program are:


- Bruce A Nuclear Power Reactor Operating Licence, PROL 15.00/2014;

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- 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);
- 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
 - 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); and
- Professional Engineers Act, R.S.O. 1990, Chapter P.28.

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

- Bruce B OP&P [119] Section 01.6 Clause 1 (b) and (d); and
- Bruce A OP&P [120] Section 01.6 Clause 1 (b) and (d).

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Appendix A in BP-PROG-10.02 [93] provides a mapping of relevant Statutory, Regulatory and Licensing Requirements to procedures demonstrating compliance. No gaps are identified in the Appendix.

4.3.2. Implementing Procedures

The ECC Program is implemented by the following procedures:

- BP-PROC-00743, Site Services Engineering Change Control [102]:
 - 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 [103]:
 - 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.
- BP-PROC-00539, Design Change Package [104]:
 - 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 [105]:
 - 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 [106]:
 - 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 [117] and BP-PROC-00412 Trend Identification and Reporting of SCRs [118]. 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 [95] is to ensure that modifications to the plant, operation, maintenance and testing of the physical plant configuration

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 [93] governs the management of distinct changes to the plant design basis.

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

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

- Bruce A Nuclear Power Reactor Operating Licence PROL 15.01/2015
 - 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 [95] provides a mapping of relevant Statutory, Regulatory and Licensing Requirements to procedures demonstrating compliance. No gaps in compliance are identified in the Appendix.

4.4.2. Implementing Procedures

This Program is implemented by the following procedures. Refer to Appendix C in BP-PROG-10.03 [95], Document Hierarchy.

- BP-PROC-00470, Configuration Management Program Oversight and Trending [107]:
 - 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 [108]:

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- 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 [109]:
 - 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 [110]:
 - 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 [111]:
 - 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 [112]:
 - 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 [113]:
 - Governs the Work Management activity from Drafting Office initiation of Work Package through to Work Package Completion and issuance.

Program oversight is implemented through BP-PROC-00137 Focus Area Self-Assessment [117] and BP-PROC-00412 Trend Identification and Reporting of SCRs [118].


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.

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. This is clarified below.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 [116]. This procedure identifies the systems to which the QA provisions of the Bruce Power Management System will formally be applied. 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 [121] and consequently ranks safety-related systems 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 [122] is focused on testing safety-related SSCs to determine if they are available and has a direct link to equipment reliability. The Bruce A PROL and Operating Policies and Principles (OP&Ps) require that an approved testing program exist to ensure that specific SSCs are available, reliable and effective. 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 [115].

Other lists with more specific safety-related purposes include:

- The System Classification List, which categorizes 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 [123].
- The Environmental Qualification Safety Related Component List (EQSRCL) is a list of all EQ safety-related equipment and components, including their harsh/mild indicators and evaluation for degradable materials. This list is developed and maintained by procedure SEC-EQD-00031 [124].
- Seismic Qualification Success Path is a list that identifies all of the SSCs credited with safe shutdown for a seismic event. These are contained in NK21-CALC-20091-00002 [125].
- Fire Safe Shutdown Success Path is a list that identifies all of the SSCs credited for the safe shutdown of the plant in the event of a fire and is maintained by DPT-PDE-00028 [126].
- 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 where their initial conditions could impact on accident consequences. However, the systems on this list are not necessarily in the SRSL.
- The Assessment of Systems Important to Safety for the Safety & Licensing Portion of the Nuclear Asset Management Program [127] presents the various system groupings at Bruce Power that rank the importance of SSCs based on safety and production.

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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.

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 [92], the purpose of which 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 [128] and the Seismic Qualification (SQ) process [129], which establish 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. However, it is noted that there are no complementary design features in the Bruce A original design to respond to 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. Bruce Power is addressing the need for additional complementary design features through evaluation and potential design improvements as part of Fukushima Action Items.

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 [37]. The concept of defence-in-depth has been applied to the design of all CANDU reactors [130]. 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.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 AOOs. This is considered a gap and is noted as SF1-6. The source of this issue is a micro-gap against CNSC REGDOC-2.5.2 requirements as shown in Table 8.

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

The Physical Design of Bruce A is managed through the Configuration Management Engineering suite of programs. 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) and Maintenance Program (MP) [131]. 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 Safety Report, SOE or associated analyses are managed in accordance with prescribed procedures and standards in compliance with regulatory, statutory and legal requirements.

Design codes and standards


In accordance with Bruce Power's Plant Design Basis Management Policy BP-MSM-1 [88], 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 and 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 issue was noted SF1-14. SF1-14 pertains to the existing design documentation, that it does not describe all necessary suitable provisions to minimize exposure, contamination and radiological releases to the environment. The sources of this issue are micro-gaps against CNSC REGDOC-2.5.2 requirements, as shown 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 modern nuclear safety and design standards.

Bruce Power has a regulatory commitment as tracked by Action Item AI 090734 to bring all pressure retaining systems and components into compliance with licence conditions [132].

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Bruce Power is implementing the Legacy Registration Project in order to bring all pressure retaining systems and components into compliance with Licence conditions, and to provide a series of semi-annual updates to the CNSC on the transition for registrations and assessments associated with the Project compliance with the Bruce A PROL and LCH [133]. The last update was provided in [134].

Bruce Power is currently working to complete the Overpressure Protection Reports (OPRs) and Design Reports associated with these nuclear systems. To date, there are 25 OPRs and 22 Design reports remaining to be completed. 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 focus of the Legacy Registration project is Bruce A, given its regulatory commitment completion date of December 31, 2014 [133].

Gap assessments have been conducted against other fire protection-related standards (CSA N293, NBCC, NFCC and NFPA-801) and submitted to CNSC staff. New editions have been issued for these four standards, as noted in Section 3, but there have not been assessments. However, operating procedures should be developed and/or updated to incorporate the manual actions credited in the FSSA. This is considered a gap and is noted as SF1-9. The sources of this issue are micro-gaps against CNSC REGDOC-2.5.2 requirements, as shown in Table 8.

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 ISR, a high-level review of standard CSA N287.1 was conducted against the latest version of the applicable standard (CSA N287.1-14). The clauses in the standard are related to the design, construction, and testing of concrete containment structures. This standard applies to new nuclear power plants' concrete containment structures at the design level. A prior evaluation, consisting of a clause-by-clause review of CSA N287.1-93 (re-affirmed 2004), was performed in 2008 against Bruce A design documents, describing the current design of the plant's concrete containment structures. The compliance evaluation of CSA N287.1-93 (re-affirmed 2004) had identified no gaps and concluded that the design is in compliance with the standard.

The standard had been revised since (CSA N287.1-14), introducing new sets of requirements. A code-to-code assessment was performed to the previous version (CSA N287.1-93) to identify the new and different requirements brought by the current standard for assessment. A high-level review of the new and different requirements was considered appropriate for this ISR, as they do not significantly impact the design basis of the concrete containment structures. The screening has identified three main topics newly introduced compared to its previous version, namely: (1) Assessing ageing effects on containment structures; (2) Preparation and reporting of commissioning reports on SSCs; and (3) Establishment and implementation of in-service examination and testing.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

These newly introduced requirements are listed and discussed in Appendix A (A.2).

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 ISR, a high-level review of standard CSA N287.3 was conducted against the latest version of the applicable standard (CSA N287.3-14). The clauses in the standard are related to establishing specific requirements for the design of concrete containment structures and addresses their beyond design basis assessment. This standard applies to concrete containment structures of new nuclear power plants at the design level. A prior evaluation, consisting of a clause-by-clause review of CSA N287.3-93 (re-affirmed 2004), was performed in 2008 against Bruce A design documents, describing the current design of the plant's concrete containment structures. The compliance evaluation of CSA N287.3-93 (re-affirmed 2004) had identified no gaps in compliance with the standard.

The standard has been revised (CSA N287.3-14) since the previous review was completed, introducing new sets of requirements. A code-to-code assessment was performed to the previous version (CSA N287.3-93) to identify the new and different requirements in the current standard. A high-level screening to identify the new and different requirements was considered appropriate for this ISR, as the new and different requirements do not significantly impact the design basis of the concrete containment structures. The screening has identified three main topics newly introduced compared to its previous version, namely: (1) Assessing containment structures for beyond design basis; (2) Members subjected to flexure or axial loads, or both, to be designed in accordance with the requirements of CSA A23.3 [135]; and (3) Walls, slabs, shells, and domes to be reinforced in accordance with clauses of CSA A23.3.

These newly introduced requirements are listed and discussed in Appendix A (A.3).

5.3.3. Review Against Changes to CSA N288.4-10 Environmental Monitoring Programs at Class I Nuclear Facilities and Uranium Mines and Mills

As part of this ISR, a high-level review of the standard has been performed and documented in Safety Factor 14. As indicated in Section 3.4, this standard is in the process of being implemented at Bruce Power; therefore it has been reviewed only with respect to progress towards its implementation. It is recognized that the standard is substantially expanded in comparison to the earlier standard N288.4-M90. In the licence renewal application [136], Bruce Power provided implementation and transition measures, and committed to full implementation of N288.4-10 by December 2018. In subsequent correspondence with the CNSC [137], Bruce Power confirmed the completion date of December 2018.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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

CSA N289.1-80 was reviewed as part of Bruce A Units 1 and 2 Return to Service – Review Against Design Standards [138], which was submitted to the CNSC [139]. At that time (2006), because Bruce A was not originally seismically qualified and the Seismic Margin Assessment (SMA) methodology used for seismic qualification was different than that specified in CSA N289.1-80, none of the clauses was assessed as ‘Full compliance’. All clauses were determined to be either ‘Complies with intent’ or ‘Acceptable deviation’. CSA N289.1-80 has now been withdrawn and replaced with CSA N289.1-08 (R2013), where subsequently a high-level review of the differences between these editions of the standard was been performed. The results of this review are presented in Safety Factor 3.

The assessment [138] indicated that all clauses were either ‘Compliance with Intent’, or ‘Acceptable Deviation’, because of the use of the SMA and Seismic Qualification Utility Group (SQUG) methodologies for qualification, which were accepted by the regulator and deemed to be “an acceptable approach in lieu of seismic design” [139]. Since the SMA and SQUG methodologies are now incorporated into the CSA standard, the seismic qualification of Bruce A is now in full compliance with CSA N289.1-08 clauses 4 and 5. Note that Clause 5.2.5.2 of CSA N289.1-08 identifies the Category A and Category B seismic categories, whereas the Bruce A approach classifies components as “S”, which is equivalent to Category A, and “S, R”, which is equivalent to Category B. Bruce A is considered to be in compliance with this clause, since the terminology of ‘Category A’ and ‘Category B’ designations do not appear to be a requirement, based on the current wording, but only notation to describe to distinct categories for seismic qualification. Clause 6 includes responsibilities and duties for the operating plant, including:

- proposing and getting acceptance of the site ground motion (engineering representation of ground motion (ERGM));
- defining the SSCs needing seismic classification and their seismic categories;
- ensuring that all SSCs on the safe shutdown equipment list are seismically qualified;
- implementing controls for design, procurement, operations installation and maintenance to ensure that qualification is maintained for the life of the facility; and
- operator response to seismic events, and post-seismic recovery activities.

These requirements are addressed in procedure DPT-PDE-00017 [129] and in related procedures and documents as listed in Sections 4 and 5 of that procedure.

In conclusion, based on the above, Bruce A complies with CSA N289.1-08.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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

CSA N289.2 was not used to develop the ground motion response spectra for Bruce A, although it was used for the Bruce B design. Instead, based on the EPRI guidance for SMA, the Review Level Earthquake (RLE) for Bruce A was characterized by a Uniform Level Earthquake with a recurrence period of 10,000 years, modified for the Bruce A site, based on the Design Basis Earthquake (DBE) level defined for Bruce B (which was based on published seismic information about the area). With a lower frequency than the DBE, the RLE is more conservative than the DBE. The in-structure response spectra corresponding to the RLE were developed by scaling the DBE response spectra from Bruce B. The development of in-structure response spectra is now addressed in NK21-DG-20091-002 [140].

The current version of the standard has been updated to be consistent with CSA N289.1, and to include the latest information for the development of the seismic ground motion for a new or existing site.

In conclusion, since an accepted ground motion has been developed for Bruce A (as per the SMA reports), no further review of the requirements in this standard was required.

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

As part of this ISR, a high-level review of the 2010 edition of the code has been performed and documented in Safety Factor 3. CSA N289.3 was not used for SSC seismic qualification at Bruce A. Instead, the EPRI SMA and SQUG methodologies are used for seismic qualification of existing and replacement SSCs. This standard was updated to be consistent with the content and terminology used in CSA N289.1 (e.g., the Seismic Margin Assessment methodology), and to include more detail for the seismic design of SSCs and for seismic analyses.

In conclusion, since the Bruce A seismic qualification of SSCs was done using the SMA methodology, which is now included in CSA N289.1 and which was accepted by the CNSC (as per the SMA reports), no further review of the requirements of this standard was required.

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

As part of this ISR, a high-level review has been carried out on the 2012 edition of the standard and documented in Safety Factor 3. CSA N289.4 was not used for SSC seismic qualification at Bruce A. Instead, the EPRI SMA and SQUG methodologies are used for seismic qualification of existing and replacement SSCs. As for the above standard, this standard was updated to be consistent with the content and terminology used in CSA N289.1.

In conclusion, since the seismic qualification of the existing SSCs has been completed using the accepted SMA methodology, no further review of this standard was required.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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

As part of this ISR, a high-level review has been carried out on the 2012 edition of the standard and documented in Safety Factor 3. As part of the 2006 Bruce A Units 1 and 2 Return to Service – Systematic Review of Safety [139] Equipment Qualification Review, CSA N289.5-M91 was reviewed at a high level with respect to the seismic monitoring equipment at Bruce A. At that time, it was determined that CSA N289.5-M91 did not “explicitly mandate installation at existing Nuclear Power Plants, but rather it is required and where site specific response are required to be determined and recorded. In the case of Bruce A, no such instrumentation has been installed.” CSA N289.5-M91 has now been withdrawn and replaced with CSA N289.5-12, which includes more detailed requirements for seismic monitoring instrumentation.

In Clause 4.1.1.3, it states “to meet the objectives of Clause 1.2, seismic instrumentation systems for existing nuclear power plants and on-site facilities shall include at least one free field triaxial accelerometer” (see Clause 4.2.2). Note 2 attached to this clause refers to Table 1, which states that one accelerometer is mandatory for existing plants, but it carries an asterisk note stating “Plants undergoing a life extension follow the requirements established together with the authority having jurisdiction (AHJ)”, i.e., the CNSC. Thus, it is concluded that, for Bruce A, which is in the process of life extension, on-site seismic instrumentation is required only if agreed with the CNSC. In NK21-REP-03600-00012 [138], it was noted that “Bruce Power is relying on off-site seismic monitoring instrumentation” and that “Bruce Power closed the REGC relating to seismic monitoring instrumentation indicating that off-site monitoring is acceptable and complies with S-99...closure of the AR was based on the judgment that means of monitoring and reporting for seismic activity other than on-site instrumentation was acceptable”. The procedure DPT-PDE-00017, Bruce Power Seismic Qualification Standard [129], notes in Section 4.6 (Post Seismic Response), the notification procedure for an earthquake of magnitude 5 or greater within 500 km of the site.

In conclusion, the current provisions for monitoring, which employs off-site information from the Southern Ontario Seismograph Network and has one monitoring station within 20 km of Bruce A, satisfies the requirements of the standard [129]. Communication protocols are in place so that Bruce Power receives timely information on any seismic activity. 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 S-99.⁵

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 SF1-5 and SF1-12 in Table 8, and are documented in Appendix B (B.1).

⁵ 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.”

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

5.3.10. Review Against CSA N291-08 (R2013) Requirements for Safety-Related Structures for CANDU Nuclear Power Plants

CSA N291-08 provides material, design, construction, fabrication, inspection, and examination requirements for Safety-Related Structures for CANDU nuclear power plants. A high-level review has been performed on the 2008 version (Reaffirmed in 2013). To comply with CSA N291-08, Bruce Power plans to utilize the research described in Reference [141] 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).

5.3.11. 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 SF1-14 have been identified and are listed in Table 8.

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 [3] 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 A is defined in BP-PROG-10.01 Plant Design Basis Management [92] 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 documented design basis for Bruce A 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 [142], which interfaces with BP-PROG-10.01 [92] via its implementing documents, particularly BP-PROC-00068 Controlled Document Life Cycle Management [143] and BP-PROC-00098 Records Management [144]. Drawing management is managed through BP-PROG-10.03 [95] Configuration Management, and associated implementing procedures, including SEC-DO-00001 Drafting Office Work Management [113]. BP-PROG-10.02, Engineering Change Control [93] 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 Bruce 3 and 4 containment structures were designed and constructed in compliance with codes and standards that pre-date the code effective date for both the current versions of

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

CSA N287.2-08 [44], CSA N287.4-09 [46], and CSA N287.5-11 [47] and the versions of these standards in use at the time of the Bruce 3 and 4 ISR. These standards apply to the materials, construction, fabrication, installation, examination and testing of initial construction or modifications to the containment structure. No new construction or permanent modifications have been made to the Bruce 3 and 4 containment structures to necessitate compliance of new containment construction to the new standards.

The Plant Design Basis Management program BP-PROG-10.01 [92] 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 design life. BP-PROG-10.01 supersedes BP-POLICY-10 Plant Design and Modification and its supporting programs. 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.
- The elements of BP-POLICY-10 related to seismic qualification of SSCs that must function during an earthquake are implemented via the seismic margin assessment for Bruce 3 and 4.
- BP-PROG-10.03 on Configuration Management has been revised in 2014 to incorporate new implementing document BP-PROC-00647 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.

The review against design standards (see Reference [139]) that formed part of the Bruce 1 and 2 ISR [9], identified that requirements for design records for piping systems, components,

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

and supports may not be strictly met by the original design documentation for Bruce 1 and 2. The original records pertaining to materials, fabrication, and inspection and testing of components prepared by the vendors met the governing requirements of the day and were acceptable to the jurisdiction at that time. However, in many cases it is very difficult to retrieve these original documents now. Re-creation of these documents offers little benefit. Therefore, recovery of missing records will only proceed on an as-needed basis. Going forward, for any new installations, the records requirements of CSA N285.0 will be followed per the Bruce Power Pressure Boundary QA Program.

When the design is described in legacy documents, it may be necessary to consult a number of different documents to determine the design basis of the system. The Bruce 1 and 2 ISR [9] consequently found that for legacy (original) design documentation and records, Bruce Power programs do not meet the requirements of this review task and this is also the case for Bruce 3 and 4.

For updated and current design documentation, the Policies, Programs and Processes 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, SF1-10, SF1-11, SF1-15, SF1-16 and SF1-17 and are considered gaps. These gaps relate to the adequacy of design documentation pertaining to the guaranteed shutdown state, seismic qualification and design, lifting and handling of large loads, design extension conditions, and pressure boundary governance. The sources of these issues are micro-gaps against CNSC REGDOC-2.5.2, CSA N290.1, and ASME 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 A met all of the objectives and requirements of the Atomic Energy Control Board (AECB) that were current at the time. It complied with all current design requirements, AECB regulatory requirements, and the AECL Quality Assurance programs. However, plant design specifications were not explicitly produced as part of the design basis.

The plant design basis is the fundamental specification defining the parameters that ensure that owner and regulatory requirements are met. As well, it ensures that the plant can be operated within the SOE. The design basis is the foundation for the 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 provide a consistent basis for safe operation.

The SOE refers to the set of operational limits and conditions to ensure that the plant is operated in conformance with design assumptions and the safety analysis. These limits identify the safe boundaries for plant operation. The SOE is documented in the Operational Safety

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Requirements (OSRs), which define the operating limits for a system. The plant configuration baseline for the specification of the OSRs is the as-installed design, issued operating documentation and AOR at the time of OSR issue. OSRs are not intended to capture requirements associated with temporary modifications or engineering changes that are in progress at the time of issue. The OSRs translate the assumptions used in the safety analyses 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 that rely upon installed plant instrumentation, either to perform a safety function or to perform surveillance to ensure the availability of a safety function. The preparation and maintenance of the OSRs are governed by DPT-NSAS-00012 [145]. OSRs and IUCs are implemented with a gap analysis to ensure that the plant is being operated in accordance with specified requirements. This is administered through DPT-RS-00015 [146], Safe Operating Envelope Gap Assessment.

In 2012, the CNSC conducted a pilot Type I Inspection of the implementation of SOE program at Bruce B [147]. 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 [24]. CNSC staff has made recommendations to improve the implementation of the SOE program at Bruce Power. The Bruce Power response to CNSC recommendations on SOE was documented in Attachment A of NK29-CORR-00531-10884 [148]. The response included modifications that are being implemented. Bruce Power has raised an SCR [149] to initiate and track work to resolve gaps in the governance and implementation of CSA N290.15. The identified corrective action is to ensure implementation of CSA N290.15-10 into the hierarchy of design documentation. In addressing the identified gaps in governance, BP-PROG-10.01, BP-PROG-10.02 and BP-PROG-10.03 programs and procedures listed below have been or are to be revised. Those underlined/italicized below have been already revised, while the revision of the rest of the list is in progress.

- BP-PROC-00539 – Design Change Package [104]
- *BP-PROC-00786 – Margin Management* [111]
- *BP-PROC-00638 – Temporary Configuration Change Management* [109]
- *DPT-PDE-00006 – Design Plan* [150]
- *DPT-PDE-00024 – Preparation and Revision of Overpressure Protection Reports* [151]
- *DPT-PDE-00034 – Preparation and Revision of System Design Manuals, Design Requirements and Design Description* [152]
- DPT-PDE-00013 – Human Factors Engineering Program Plan [153]
- BP-PROC-00014 – Technical Operability Evaluation [154]
- *BP-PROC-00375 – Software Development* [155]
- *DIV-ENG-00005 – Engineering Calculations* [156]
- DPT-PDE-00044 – Preparation and Maintenance of Instrument Uncertainty Calculations [157]

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- DPT-PDE-00040 – Preparation of Instrument Calibration Specifications [158]
- SEC-RSA-00001 – Preparation of the EQ Room Conditions Manual [159]
- BP-PROC-00542 – Configuration Information Change [103]
- BP-PROG-10.01 – Plant Design Basis Management [92]
- BP-PROG-10.02 – Engineering Change Control [93]
- BP-PROG-10.03 – Configuration Management [95]

A reference to CSA N290.15 was added to the requirements listed in Section 5.1 of BP-PROC-00786 [111], DPT-PDE-00006 [150], DPT-PDE-00024 [151], BP-PROC-00375 [155], DIV-ENG-00005 [156], DPT-PDE-00040 [158] and SEC-RSA-00001 [159]. As applicable for some of these governance documents, specific steps were also added to address impacts to the SOE. Furthermore, all impacted administrative document changes for compliance sustainability in PROGs 12.02, 12.03 and 11.01 are planned to be completed by September 30, 2015.

In summary, programmatic activities have established a good basis for compliance with CSA N290.15, which includes the preparation of all OSRs, IUCs requirements that are consistent with the Operational Limits and Conditions (OLCs) and their basis derived from safety analysis. Gaps and areas for improvement in programmatic aspects identified in the self-assessment and pilot inspection are being addressed for the introduction of CSA N290.15 in the next licensing period. Bruce Power therefore 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 Bruce Power ECC program (BP-PROG-10.02) [93] and CM program (BP-PROG-10.03) [95] are the means by which plant modifications are reflected in the design basis for the facility.

BP-PROG-10.02 [93] establishes the scope of engineering change procedures and documentation. Through a screening process, engineering changes are classified by safety significance and scope, and stakeholders identified through the use of comprehensive lists, including a Design Scoping Checklist [160], Design Review of Design Change Notice [161] and Design Products Challenge Board Checklist [162]. With these, the scope of the design plan is established [150], 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 [99].

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Design engineers and system engineers of interfacing systems potentially impacted by the design modification are identified as part of the Design Scoping Checklist [160] 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 [104]. 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 [163].

The current Bruce A 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 [164].

A suite of safety analysis was performed for design basis accidents most impacted by ageing, incorporating the impacts of ageing to 2019. This suite of safety analysis was submitted to the CNSC in support of the licence renewal process, and includes:

- Loss of regulation (NOP trip setpoint calculations) for Units 1 and 2 [165] and Units 3 and 4 [166];
- Small Loss of Coolant Accident for Units 1 and 2 [167] and Units 3 and 4 [168];
- Loss of Flow for Units 1 and 2 [169] and Units 3 and 4 [170]; and
- Large Loss of Coolant Accident for Units 1 and 2 [171] and Units 3 and 4 [172].

This re-analysis demonstrates that units are safe to operate now, and processes are in place to ensure safe operation to 2019.

As described in Bruce Power's PROL renewal application [136], Bruce Power is in the process of implementing a Safety Report Improvement (SRI) initiative that includes updates to the Bruce Power Deterministic Safety Analysis (DSA) governance (programs, processes and procedures) to ensure that deterministic safety analysis is consistent with RD-310 and now CNSC REGDOC-2.4.1. The CNSC has been tracking these activities with CNSC Action Item 090739. The Safety Report Improvement Plan for Bruce A [173] and project description, including scheduled timelines was accepted by the CNSC [174]. The SRI strategy consists of two main elements:

- A three-year SRI Project will be undertaken to upgrade the Bruce A Safety Report to align with the CNSC REGDOC-2.4.1 framework. This update will include an event classification scheme of plant states (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 A 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.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- An ongoing SRI 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.

Bruce Power is targeting the adoption of CNSC REGDOC-2.4.1 [175] and implementation of the updated requirements on the same schedule described in the RD-310-based SRI plan and project description as noted above [173] and agreed by CNSC in [174].

Bruce Power will transition to CNSC REGDOC-2.4.2 for Probabilistic Safety Assessment (PSA) over the next licensing period [19]. The combination of already complete S-294 work (which includes Emergency Mitigating Equipment credits) and the Seismically Induced Fire and Flood and Irradiated Fuel Bay Analyses (i.e., Fukushima FAls related to PSA that will be complete by the end of the 2014) 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 [176]. There is an on-going industry effort to develop a methodology for site-wide PSA.

To meet the guidance in Section 5 of CNSC REGDOC-2.4.2, Bruce Power has prepared a public disclosure summary report of the results and assumptions of the Bruce Power PSAs that will be posted on the Bruce Power website. Any changes to methodologies and the PSA reports will be submitted per the Bruce Power PSA governance for the required 5 year update of the PSAs. 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 (NK21-CORR-00531-10873 [136] and NK29-CORR-00531-11252 [177]). These CSA N288.1-aligned DRLs have been added to Appendix C of the current Bruce A PROL.

Based on the assessments of topics 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 Actions (SF1-7), 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 qualifications requirements. This emphasis is graduated depending on the classifications and the safety-related functions within the listing. For example, the Safety Related System Testing program [122] is focused on testing safety related SSCs to determine if they are available and has a direct link to equipment reliability. The Bruce A PROL and OP&Ps require that an

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

approved 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 [123], 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 requirements for preparing, or updating, the System Classifications List with required information (including system classification and registration) for pressure retaining systems or components.
- The EQSRCL is identified in the EQ Dossiers. Environmental Qualification Lists are subsets of the EQSRCL and are applicable to components that are credited for harsh environments that contain material (e.g., elastomers) that could degrade during service conditions or storage.
- The Seismic Qualification Success Path identifies all of the SSCs credited with safe shutdown for a seismic event.
- The Fire Safe Shutdown Success Path 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 [145] 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”.
- The groupings in the assessment of Systems Important to Safety for the Safety and Licensing Portion of the Nuclear Asset Management Program [127] are used to establish 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 A 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” [178]. These tables are divided into three tiers:
 - Tier 1 systems, which are systems important to safety in accordance to RD/GD-98 criteria identified. These are mandatory inclusions in the performance and condition monitoring.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- Tier 2 systems, which are systems that are important to generation and asset preservation. There are also included in the performance and conditions 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 [179], Bruce Power identifies all systems important to safety. This is implemented through procedure DPT-RS-00012 [115]. The procedure describes the logic and processes involved in evaluating the modelled systems in Bruce Power's PRAs, 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.

CSA N287.2-08 [44], CSA N287.4-09 [46], and CSA N287.5-11 [47] address requirements for the materials, construction, fabrication, installation, examination and testing of concrete containment structures. Based on these standards, the relevant structures important to safety are the parts of the Bruce A containment envelope, which 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.

With respect to CSA N287.2-08 [44], CSA N287.4-09 [46], and CSA N287.5-11 [47], 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 DBAs and events in Units 3 and 4 is established by Part 3 of the Bruce A Safety Report [63]. In the restart of Units 3 and 4 in 2003 / 2004, demonstration of the adequacy of the containment design relied on earlier analysis of containment response to accident conditions. The restart safety analysis concluded [7] that the predicted fission product release following postulated DBAs for the restarted units was bounded by the earlier analyses, thus the adequacy of containment design was not impacted.

CSA N289.1-08 [49] defines a seismic success path as the minimum set of SSCs that can perform the required nuclear safety functions following an earthquake. The Bruce 3 and 4 success path is defined in the seismic margin assessment [65] and was subsequently accepted by the CNSC in [66].

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 [180]. However, the existing SSCs cannot sufficiently accommodate simultaneous severe accidents in multiple units, particularly if CCI occurs. Options for enhancing the ability of containment to accommodate severe accidents in multiple units are being evaluated as part of an integrated suite of potential enhancements [180]. This is identified as gap SF1-3. The

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

source of this issue is a micro-gap against CNSC REGDOC-2.5.2 Requirement 6.6.1, as shown in Table 8.

With respect to CSA N289.1-08 [49], the adequacy of the plant design to accommodate seismic events is addressed via the Bruce Units 3 and 4 Seismic Margin Assessment [181] and the seismic PRA. Several Unit 1 and 2 reconciliations remain active as a result of modifications completed during the Bruce A Unit 1 and 2 Restart project. These reconciliations have now been integrated into the Bruce A Legacy registration project commitment (AI 090734) to be completed by December 31, 2014. Seismic Margin Assessments are required to support the completion of the reconciliations and legacy registration project commitments. Seismic upgrade modifications for Units 1 and 2, need to be installed within 30 months after start-up of units. Currently in the detailed design phase, all DCNs have been delivered and are with field assessing, analyzing legacy containment boundary SCRs, populating SSEL and updating system flow diagrams [208].

The seismic PRA was updated to address post-Fukushima action items, as presented in Reference [67]. Bruce Power's S-294 implementation project is now complete with the submission to the CNSC (see details in NK21-CORR-00531-11324/NK29-CORR-00531-11729 [67]). Credited upgrades will be completed and tracked under the Fukushima Action Item plan (latest updates on this plan are in NK21-CORR-00531-11379/NK29-CORR-00531-11782/NK37-CORR-00531-02254 [182]).

Upon review of modern codes and standards, it was noted that reliability requirements for some SSCs do not meet requirements and/or safety goals. This is identified as gap SF1-5. 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.

Used fuel storage at Bruce A consists of the primary spent fuel bay, secondary spent fuel bay, a transfer duct between the two bays, and associated cooling systems, instrumentation and control (Safety Report Part 2, Section 10 [183]). 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. After six months, the fuel may be transferred to the secondary irradiated fuel storage bay, as described in Section 10.2.5.2.4 of Part 2 of the Safety Report [183]. The storage capacity of the primary bay is sufficient for 36000 fuel bundles. Space is also provided for handling irradiated fuel casks, inspecting and canning defected fuel. After a sufficient cooling period, fuel bundles are transferred to dry storage containers and removed from the Bruce A station. Once removed, the bundles in dry storage are managed and maintained by Ontario Power Generation.

The adequacy of the spent fuel bay design in Bruce A has been assessed in response to CNSC action items related to the Fukushima event. 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

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

that there would be no structural failure of the bay integrity that could result in a loss of inventory from the bay [184]. The only significant loss of bay inventory would result from boil-off. An assessment of the potential for hydrogen generation in the IFB area showed that significant hydrogen generation will only occur if fuel becomes exposed due to IFB draining [180]. Design modifications to allow 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 [185]. The IFB structural analysis [186] 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. Given the results, Bruce Power has no plans to structurally enhance the Bruce A IFBs. Based on the CNSC staff review of Bruce Power's Irradiated Fuel Bay Structural Integrity Analysis, the related Fukushima Action Items were closed [187].

The condition of the fuel bays and transfer duct are assessed through inspection. The primary bay, secondary bay, and transfer duct are designed to allow visual detection of leaks. The secondary bay liner leakage collection system flows out through drain pipes to open air, providing visual leakage detection [188].


Bruce Power plans to enhance the existing understanding of severe accident phenomena and SAMG capabilities undertaken under CANDU Owners Group (COG) Joint Project 4426 [189], followed by station-specific implementation. The scope of the work involves the enhancement of SAMG to include IFB events [186]. 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 station specific guidelines include:

- Severe Accident Control Room Guides;
- Diagnostic Flow Chart;
- Severe Challenge Status Tree;
- Severe Accident Guides; and
- Severe Challenge Guides.

Updates to the station specific guidelines are targeted for completion by end of Q3 2015 [33].

Analysis has been performed to disposition any potential for criticality for booster fuel rods stored at Bruce A and determined that no interim measures are required, as there are no plans to change the existing storage arrangements. Due to the presence of fissionable materials (as defined in Section 2.3.1.3 of RD-327) in the booster fuel assemblies at Bruce A, several of the requirements listed in RD-327 have been assessed as being applicable [33]. The applicable requirements are:

- Nuclear criticality safety program relative to categorization (RD-327 Sections 2.3.1.3, 2.3.1.4 and 12.8);

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- Responsibilities (RD-327 Sections 2.3.2.1, 12.3.1, 12.3.2 and 12.3.3);
- Quality management program and procedures (RD-327 Section 2.3.2.3 and 2.3.2.6);
- Materials control (RD-327 Sections 2.3.2.4 and 12.6);
- Operational control (RD-327 Section 2.3.2.7);
- Emergency procedures (RD-327 Sections 2.3.2.9 and 12.7);
- Nuclear Criticality Safety in the Storage of Fissile Materials (RD-327 Section 6.0); and
- Nuclear Criticality Safety Training (RD-327 Section 13.0).

Bruce Power's procedures will be updated to reflect the level of nuclear criticality safety management required at Bruce A as a result of the long term dry storage of the booster rods. Bruce Power is targeting October 31, 2015 to align fully with current practices and to document compliance with RD-327 within applicable governance for Bruce A [33].

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 [190]. This system provides the necessary record keeping capability to ascertain inventories and discharge dates of all fuel in the primary and secondary fuel bays.

The 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. 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 A ISR. 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 3: Equipment Qualification” in Appendix A (A.2), assesses the requirements for seismic design and qualification of CANDU plants, including the seismic margin assessment. 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. In Appendix A (A.2) of Safety Factor 5, an assessment of requirements and guidance regarding computer programs used in design and safety has been performed. The results of these assessments have been directly applied to the review tasks of this safety factor.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- “Safety Factor 6: Probabilistic Safety Analysis” in Section 5.0 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 14: Radiological Impact on the Environment” in Appendix A (A.2) has performed a high level assessment of CSA N288.1-14 Guidelines for Calculating Derived Release Limits for Radioactive Material in Airborne and Liquid Effluents for Normal Operation of Nuclear Facilities.
- “Safety Factor 15: Radiation Protection” in Appendix B.1, has assessed the state of Bruce Power’s Radiation Protection Program against applicable guidance.

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 provide a cross section, intended to demonstrate that the processes associated with this Safety Factor are implemented effectively (individual findings notwithstanding). Thus, program effectiveness can be inferred if Bruce Power processes meet

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 the assessment are compared with business needs, the Bruce Power management system, industry standards of excellence and regulatory/statutory or other legal requirements.

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 the relevant Focus Area Self Assessments (FASAs) that have been carried out since 2009. 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 and Audits Relevant to Plant Design

Assessment Number	Title
SA-BBOP-2009-07	Conduct FASA on Temporary Configuration Change
SA-CAP-2009-02	Completion and Effectiveness of SCR 'S' Type Actions
SA-BAOP-2009-02	Implementation of WANO SOER 2007-1, Reactivity Management Recommendations
SA-COM-2009-01	Component Design Basis Inspection
SA-COM-2009-04	Equivalent Design
SA-COM-2009-05	Fidelity of Configuration Information to Plant

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Assessment Number	Title
SA-PDE-2009-03	EQ Barrier Project – Baseline Complete and Sustained
SA-PDE-2009-06	Core Changes Compliance to the Engineering Change Control Process
SA-AUD-2010-03	Pressure Boundary Audit Compliance
SA-BS-2010-04	Oversight to Pressure Boundary Program Requirements
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-RS-2010-03	Fuel Defect Management
SA-COM-2011-10	Fidelity of Configuration Information to Plant
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-FASA-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)

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Assessment Number	Title
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
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)

7.1.1. SA-MPR-2014-08 SECNMMM Equipment Capability

SECNMMM, which is the Mechanical Maintenance Section within the Outage and Maintenance Services Section, provides support to the broader organization by ensuring fast turnaround on critical maintenance and manufacturing activities. This self-assessment focused on the identification of critical areas of equipment and technologies within SECNMMM to determine if action is required to replace or upgrade such technologies and equipment. The Focus Area Self Assessment (FASA) examined:

- Procedures or guidance related to asset management;
- Tools, technology and processes used by the site weld and machine shop crews;
- Measuring and drafting technologies associated with reverse engineering; and
- Information management systems in support of these programs.

At the time of the self-assessment, there was no formally accepted effective industry guidance for evaluating the current state of equipment and technologies to determine whether these should be disposed of, maintained, or whether new assets and technologies should be acquired. This lack of guidance was noted as an adverse condition. In total, two adverse

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

conditions were noted and one opportunity for improvement, which were all assigned SCR numbers and as appropriate are being monitored. Given such improvements these are not identified as gaps within the review task areas for the purpose of this assessment.

7.1.2. SA-COM-2014-01 Engineering Change Controls

This self-assessment focused on the installation and commissioning activities pursued as part of the modifications completed at Bruce A under the auspices of BP-PROG-10.02 "Engineering Change Control". As part of this FASA, modifications that were currently active and in the midst of installation and commissioning were selected for review. Each modification was reviewed for compliance with CSA N286-05 and Bruce Power procedures/programs. Common opportunities for improvement were identified, resulting in the identification of six adverse conditions. The adverse conditions identified have been appropriately assigned SCR numbers and have been given prescribed assignments to be managed by the corrective action process. Given that planned and monitored initiatives are underway for improvements, these are not identified as gaps for the purpose of this assessment.

7.1.3. SA-COM-2014-03 Design Change Management

This self-assessment focused on the effectiveness of identifying, evaluating and documenting changes in margins resulting from design changes, engineering calculations and to review applicable operating experience (OPEX). This FASA was performed as a result of station events which were believed to stem from process deficiencies. The effectiveness was measured against WANO PO&C CM1-4 and CM1-7:

- CM1-4: the effects of planned design and operational changes on margins are identified evaluated and documented before the changes are approved for implementation. The potential impact on plant operation, safety and reliability is evaluated when margins are reduced.
- CM1-7: Engineering calculations and analysis address design and operating margins and the bases for the margins.

A review of procedures, design change notices and calculations determined that the intended results were not always achieved; gaps and corrective actions were identified. The following conclusions were reached upon the completion of this self-assessment which included:

- Knowledge-based stakeholders (e.g., Nuclear Safety Specialists, Managers) are those that identify margin issues versus procedure-based preparers (e.g., verifier). It was recommended that the identification of margins become procedure-based rather than knowledge-based.
- The communication of margin reductions has not been adequately incorporated into the Design Change Package Procedure BP-PROC-00539.
- Margin management has been incorporated within the Engineering Calculations procedure DIV-ENG-00005. However, this procedure only requires a review of margins if the engineering calculation is for a safety-related system or system important to safety.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

It was recommended that a review of margins also be required if the calculation impacts production. As an extension of the Engineering Calculations procedure, margin management has not been incorporated into the Design Calculations Template, nor has it been incorporated into the Calculation Verification Checklist FORM-11365.

- Margin management has not been incorporated into the Design Plan Procedure DPT-PDE-00006, the Design Plan Template, or the Design Plan Verification Checklist FORM-12585.

These gaps resulted in two adverse conditions and one opportunity for improvement, which were appropriately assigned SCR numbers and have been given prescribed assignments managed by the corrective action process. Given that planned and monitored initiatives are underway for improvements in the efficiency of the Design Change Management process, the gaps identified in this FASA are not identified as gaps for the purpose of this assessment.

7.2. Internal and External Audits and Reviews

The objective of the audit process as stated in BP-PROG-15.01 [191] 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 4.11.2 of [21]).

As specified in BP-PROC-00295 Planning & Scheduling Audits, 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.

7.2.1. 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 [108]. 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:

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- 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 SPOC is not performed;
- CMT-66415-00001 "Passport V10 Configuration Management and Master Data Rollout" (referred to in BP-PROC-00584 R006 [108]) is out of data 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 records leads to increased burdens for the work groups on site. The audit found that instructions to BP-PROC-00584 R006 are not consistently adhered to. Master Equipment List records have numerous information gaps compared to the requirements of BP-PROC-00584. Thus, BP-PROC-00584 is not effective at satisfying its purpose of ensure 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
 - 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 its 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.

7.2.2. AU-2013-00001 Pressure Boundary Quality Assurance Program Section 18 Audit

An audit of the Bruce Power Pressure Boundary Quality Assurance Program (PBQAP) was completed in November 2013 by an Ontario Power Generation Audit Team. It was performed to determine the effectiveness of the implementation of the PBQAP and to ensure that it satisfied the code requirements to maintain the Certificate of Authorization issued by the Technical


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Standards and Safety Authority. The applicable requirements stated in Section 1 (Organization), Section 2 (QA Program), Section 16 (Corrective Action), Section 17 (QA records), Section 6 (Document Control), as well as the training requirements for the PB audit personnel were included in the audit. In addition, the audit evaluated the performance of the activities associated with the 2012 Audit (AU-2012-00002) on the PB Program.

Overall, it was found that the PBQAP was effectively implemented and compliant with the applicable requirements of the Program. Personnel interviewed were found to be knowledgeable with the PBQAP requirements and their respective areas. The OPG Lead Auditor noted that the issues raised from the 2012 Audit were satisfactorily completed. There were no adverse conditions noted as a result of this audit. The two OFIs that were observed during this audit from Section 6 (Document Control) and Section 2 (QA Program) are listed below.

OFI No. 1: Documents and Record Control

- In regards to the 2012 Audit:
 - The validation of the PB Design Control element was not satisfactorily documented in the Audit Working Records (Checklist).
 - The Audit Criteria Checklist does not provide a clear conclusion of the audit results.
 - The Observation Report MW-002-03 was found not completely dispositioned, addressed, and documented in the Audit Report.
 - Findings were qualified as low significance when they should be qualified as significant.
- In BP-PROC-00635 R007, Audits, a statement should be added to clarify that the CAP completion status will be included the following year's audit report.
- In the PBQAP Manual, BP-PROG-00.04 R019:
 - The word "reconcile" should be deleted in Section 4, Clause 5.2, because reconciliation does not require AIA approval or registration.
 - A clear definition of "Pressure Boundary" is needed.
 - The frequency of audits for Class 6 systems can be reduced as there are no requirements for annual audits in N286-05 or B51.
- The box "Regulatory Concern" on Pre-Job Brief, N-FORM-11378, page 2, "Consequence Factors" for PB Audits is recommended to be checked off.
- Revise the audit scope statement in the Audit Plan (AP-2012-00002) to describe the audit's extent and boundaries. The Audit Plan also needs to provide an identification number that relates it to a specific Audit.
- Audit Criteria Checklist lacks control and traceability of the handwritten note changes.
- Revise the Audit Observation Record form (FORM-11039 R006) to include a unique identification number.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- Establish electronic folders/files and working files for the signed observation reports and audit criteria checklists.

OFI No. 2: Training and Qualification

- A reference to a specific qualification should be provided in BP-PROC-00635 R007 or a statement added in TQD-00029 that defines the required qualifications of the Audit Verifier.
- Minimum qualification requirements should be defined for all staff positions in TQD-00029.

7.2.3. 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 [209], to ensure time at risk for critical drawings is managed. The audit supports BP-PROC-10.03, Configuration Management. For this audit, a sample of data and records was reviewed to assess compliance. At the Client's request, 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 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 to 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 was inadequate as the procedure was not fully implemented and not all work is 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 action process was followed for this audit to improve the adequacy of the implementation of this procedure. This was documented in SCR 28266458; "Investigate Obsolete DPT-COM-00004

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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.

7.2.4. AU-2012-00001 Pressure Boundary Quality Assurance Program Section 18 Audit

An audit of the Bruce Power PBQAP was completed in November 2012. The objective was to determine the effectiveness of the implementation of Section 18 (Audit) of the PBQAP and to ensure that it satisfies the Code requirements to maintain the Certificate of Authorization issued by the Technical Standards and Safety Authority. The scope of the audit included the completed PBQAP audits, the audit reports issued since the 2011 audit (AU-2011-00021), the personnel training requirements, and the applicable aspects of the PB program, such as Organization, QA Program, QA Records, Document Control and Corrective Action.

In the 2011 Audit, there were two adverse conditions identified. The Lead Auditor from the 2012 Audit, evaluated the CAPs raised from these conditions and concluded that they were addressed and completed as required. The 2012 Audit raised three adverse conditions:

- AU-2011-00003 did not provide sufficient information on the adverse conditions required by the CSA N285.0 and Bruce Power procedures. Corrective actives could not be put in place based on the audit information alone.
- Deficiencies in Governance
 - Deficiencies in the governance were noted in the role of the ASME NQA-1 Lead Auditor and procedures not reflective of current practices.
- Lack of attention to detail in the Audit Working File
 - Discrepancies and omissions were noted in the Audit Working File.

Overall, it was found that the PBQAP was effectively implemented and in compliance with the relative sections in the program manual. Only minor issues were observed in Section 6 (Document Control) and 18 (Audit). In the Audit Report, two opportunities for improvement were noted. The opportunities for improvement are listed below:

- No governance or expectations on the quorum requirement for Audit Exit Meetings. Adverse conditions were raised during the audit, however there were no representatives from the affected groups at the Audit Exit Meeting.
- Editorial Corrections are required for procedures and documents as errors, misalignments, and omissions were found during the audit.

In the 2012 Audit, it was found that the PBQAP was effectively implemented and in compliance with the section 1 (Organization), 2 (QA Program), 16 (Corrective Action) and 17 (QA records) in the program manual. Only minor issues were observed in Sections 6 (Document Control) and 18 (Audit). As appropriate, the corrective action process was followed for this audit to improve the adequacy of the implementation of DPT-COM-00004. Given that planned and

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 operators 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 that all items are quickly corrected.

The CNSC Staff Integrated Safety Assessment of Canadian Nuclear Power Plants for 2013 ("2013 NPP Report") [192] summarizes the CNSC staff's assessment of the Canadian nuclear power industry's safety performance during 2013 and details the progress of regulatory issues and initiatives up to May 31, 2014. 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 3.1.5. Physical Design, that the physical design Safety and Control Area (SCA) at Bruce A met performance objectives and all applicable regulatory requirements. As a result, Bruce A received a "satisfactory" rating, unchanged from the previous year. The CNSC staff observations related to Bruce A Physical Design are listed below:

- Design governance
 - Equipment qualification – The EQ program is fully implemented at all Bruce A operating units. Bruce Power demonstrated EQ compliance with the related governing document, by maintaining adequate EQ program sustainability.
 - Human factors in design – Bruce Power is in the process of updating the Human Factors Engineering Program Plan in advance of the relicensing application. CNSC staff will continue to monitor these updates.
- System design
 - Electrical power systems – The qualification of the qualified power supply (QPS) standby diesel generator 2 (SDG2) at Bruce A remains an on-going issue. Bruce Power is in the process of qualifying the QPS SDG2 using the industry-proven process defined in EPRI NP-5652, Guideline for the Utilization of Commercial

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Grade Items in Nuclear Safety-Related Applications [197] in time for the licence renewal process. The SDG2 qualification issue has minimal impact on safety.

- Fire protection design – The fire protection program at Bruce A met applicable CNSC requirements. Bruce Power continued its activities to improve fire protection at all facilities through the implementation of procedural and physical upgrades as recommended within the code compliance review of the facilities with respect to N293-07, Fire Protection for CANDU Nuclear Power Plants [87], and the revised Fire Hazard Assessments and Fire Safe Shutdown Analysis. The proposed modifications are expected to increase the safety margins of the facility with respect to fire protection.
- Components design
 - Fuel design – Bruce Power has a well-developed reactor fuel inspection program. In 2013, Bruce Power began loading 37M fuel, which will offset the effects of ageing in the heat transport system.

7.3.1. Action Item 2014-07-5211: Bruce A Electrical Power Systems Inspection BRPD-A-2014-004 [193]

CNSC staff completed a Type II compliance inspection of the Bruce A electrical power systems. The objective of the inspection was to verify that the electrical power systems and components are capable of performing the intended safety functions and that the equipment is tested and maintained as required. Based on the scope of the inspection, CNSC staff concluded that the electrical systems at Bruce A are being maintained and tested to ensure that they will be able to perform their design functions. However, there were some areas for improvement identified. In total, five action notices and four recommendations were raised as a result of this inspection. Positive observations included the implementation of the electrical emergency mitigating equipment, general monitoring of the systems, and testing of the Emergency Transfer Scheme. Areas for improvement included mission time testing of the generators, assigning appropriate priority to maintenance work, and implementation of an ageing management program for cables. As appropriate the corrective action process was followed for this audit. 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.

7.3.2. CNSC Type II Compliance Inspection: Implementation of the Engineering Change Control Process [210]

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 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

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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. 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.

7.3.3. CNSC Type II Compliance Inspection Report: BPRD-AB-2014-005 Fukushima Action Item Field Verification [185]

The purpose of this compliance inspection was to verify the completion of the Fukushima Action Items [193] as communicated by Bruce Power in the semi-annual progress reports [194], [180], [67], [195]. CNSC staff were satisfied that Bruce Power has procured equipment and made modifications consistent with that communicated in the semi-annual progress reports [194], [180], [67], [195]. CNSC staff noted one small area for improvement and as a result provided one recommendation, which was that Bruce Power consider making changes to the Unit 4 BSRV instrument air hoses and emergency connection fittings to make them compatible with the other Bruce A Units.

7.3.4. Human Factors in Design Desktop Review – August 12-16, 2013 [196]

A desktop review of Human Factors activities in Engineering Changes was carried out at Bruce Power from August 12 to 16, 2013. The objective of the desktop review was to verify that Bruce Power is properly taking into account Human Factors in the design processes of a sample of six selected Engineering Change packages. The review concluded that Bruce Power generally uses the approved process for taking into account Human Factors in the design process, and the Human Factors activities generally followed the DPT-PDE-00013, Human Factors Engineering Program Plan (HFEPP). However, areas for improving the adherence to procedures were noted. No regulatory actions have been placed on Bruce Power as a result of this desktop review.

7.4. Performance Indicators

Performance indicators are defined as data that are sensitive to and/or signals 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 [94], and are included in system health reporting:

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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

In addition, the CNSC produces an annual report on the safety performance of Canada's NPPs. The report for 2013, "CNSC Staff Integrated Safety Assessment of Canadian Nuclear Power Plants for 2013", issued in September 2014 [192], summarizes the 2013 ratings for Canada's NPPs in each of the 14 CNSC SCAs, including physical design. The physical design SCA relates to activities that affect the ability of SSCs to meet and maintain their design basis, as new information arises over time and taking into account changes in the external environment. For 2013, the Bruce A rating for the physical design SCA was "satisfactory".

8. Summary and Conclusions

The overall objective of the Bruce A ISR is to conduct a review of Bruce A against modern codes and standards and international safety expectations and provide input to a practicable set of improvements to be conducted during the Major Component Replacement in Units 3 and 4, 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.




 <div>Division of Kinectrics Inc.</div>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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>Section 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, Gap 2) 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 7.6.3 REGDOC-2.5.2 - Clause 7.13.1 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 8.6.12 (Gap 2) REGDOC-2.5.2 - Clause 9.2 CSA N290.0 - Clause 4.2 CSA N290.0 - Clause 4.8 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 A PRA meet the safety goal limits set up for Bruce A PRAs, they do not meet the more stringent quantitative safety goal targets set up in the requirement clause.</p>	<p>Section 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>Section 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 7.15.1 CSA N290.3 - Clause 10.1 CSA N290.11 - Clause 5.2.2.10</p>

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Issue Number	Gap Description	Source(s)
SF1-4	Legacy Design Analysis The original design analyses predate CSA N286.7-99.	Section 5.6 Micro-gaps against requirement clauses: REGDOC-2.5.2 - Clause 5.3
SF1-5	Design for Reliability Reliability requirements for some SSCs do not meet the requirements and/or safety goals.	Sections 5.3.9 and 5.7 Micro-gaps against requirement clauses: REGDOC-2.5.2 - Clause 7.6.2 CSA N290.1 - Clause 4.2.1.1 CSA N290.0 - Clause 4.5.2.1 CSA N290.0 - Clause 4.7.3 CSA N290.3 – Clause 14.1 Micro-gaps against guidance clauses: REGDOC-2.5.2 - Clause 8.4.2
SF1-6	Overpressure Protection of pressure-retaining SSCs There is not a systematic analysis of the control system capability to cope with AOOs.	Section 5.2 Micro-gaps against requirement clauses: REGDOC-2.5.2 - Clause 7.7
SF1-7	Operator Actions The current design documentation does not specifically address the timing requirements introduced in this clause.	Sections 5.3.9 and 5.6 Micro-gaps against requirement clauses: REGDOC-2.5.2 - Clause 8.10.4 CSA N290.11 – Clause 5.2.2.4
SF1-8	Guaranteed Shutdown State Current design documentation does not reflect required functional test frequency.	Section 5.4 Micro-gaps against requirement clauses: REGDOC-2.5.2 - Clause 7.11
SF1-9	Fire Safety Operating procedures should be developed and/or updated to incorporate the manual actions credited in the FSSA.	Section 5.3 Micro-gaps against requirement clauses: REGDOC-2.5.2 - Clause 9.3

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Issue Number	Gap Description	Source(s)
SF1-10	Lifting and handling of large loads Identification and justification of traversing routes for large loads does not exist in current Bruce Power design documentation.	Section 5.4 Micro-gaps against requirement clauses: REGDOC-2.5.2 - Clause 7.15.3 (Gap 1, Gap 2)
SF1-11	Design Extension Conditions The current design documentation does not explicitly consider the load conditions during DEC's.	Section 5.4 Micro-gaps against requirement clauses: REGDOC-2.5.2 - Clause 8.6.12 (Gap 1) REGDOC-2.5.2 - Clause 8.8 CSA N290.3 - Clauses 5.5 and 5.7
SF1-12	Electrical Power Systems Design limits are not specified for electromagnetic emissions. The DMs and OSR do not explicitly state that the SSCs employed are qualified for electromagnetic noise disturbances and mechanical vibrations. The capacity requirements and design provisions for periodic testing are not sufficiently documented. The existing safety analysis does not consider events with station blackout.	Sections 5.3.9 and 5.6 Micro-gaps against requirement clauses: 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
SF1-13	Fuel Handling and Storage 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 are not addressed in Part 3 of the Safety Report. A limited set of Fuel Handling System Failures is discussed in Appendix 1 and Section 3.5.5 Fuel Bay Accidents of Part 3 of the Safety Report.	Section 5.8 Micro-gaps against requirement clauses: REGDOC-2.5.2 - Clause 8.12.2 REGDOC-2.5.2 - Clause 9.1

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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>Section 5.2</p> <p>Micro-gaps against requirement clauses:</p> <p>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 1, Gap 2) REGDOC-2.5.2 - Clause 10.1</p>
SF1-15	<p>Revision Changes to Stress Limit</p> <p>The impact on pressure boundary design governance documentation due to changes of the stress limit for “membrane longitudinal stress plus discontinuity longitudinal stress” has not been assessed.</p>	<p>Section 5.4</p> <p>Micro-gaps against requirement clauses:</p> <p>ASME Section III</p>
SF1-16	<p>Bellows Design</p> <p>The impact on pressure boundary design governance due to changes to bellow design requirements has not been assessed.</p>	<p>Section 5.4</p> <p>Micro-gaps against requirement clauses:</p> <p>ASME Section VIII</p>
SF1-17	<p>Safety Basis Report Findings</p> <p>Potential issues mentioned in the SBR [2] regarding changes to ASME B31.1 from 2007 to 2011 have not been addressed.</p>	<p>Section 5.4</p> <p>Micro-gaps against requirement clauses:</p> <p>ASME B31.1</p>

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

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

9. References


- [1] 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.
- [2] NK21-CORR-00531-11005/NK29-CORR-00531-11397, Submission of Safety Basis Report, Bruce Power Letter, F. Saunders to R. Lojk, December 30, 2013.
- [3] IAEA SSG-25, Periodic Safety Review of Nuclear Power Plants, 2013.
- [4] CNSC RD-360, Life Extension of Nuclear Power Plants, 2008.
- [5] NK21-CORR-00531-03839, Bruce A Environmental Assessment Study Report, December 7, 2005.
- [6] CNSC REGDOC-2.3.3, Operating Performance: Periodic Safety Reviews, CNSC, April 2015.
- [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-00531-04059, Bruce A Refurbishment for Life Extension – Systematic Review of Safety: Plant Design, Bruce Power Letter, F. Saunders to P. Webster, March 30, 2006.
- [9] 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.
- [10] 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.
- [11] 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.
- [12] 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.
- [13] 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.
- [14] Nuclear Safety and Control Act, 1997, c. 9, N-28.3, Assented to March 20, 1997.
- [15] NK21-CORR-00531-11272, Nuclear Power Reactor Operating Licence, Bruce Nuclear Generating Station A (PROL 15.00/2015), May 1, 2014.
- [16] NK21-CORR-00531-11391, Bruce Nuclear Generating Station A Nuclear Power Reactor Operating Licence: Licence Conditions Handbook (LCH-BNGSA-R8), June 4, 2014.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


- [17] PROL 18.00/2020, e-Doc 4723908, Nuclear Power Reactor Operating Licence, Bruce Nuclear Generating Station A and Bruce Nuclear Generating Station B, June 1, 2015.
- [18] LCH-BNGS-R000, e-Doc 4659316, Bruce Nuclear Generating Station A and Bruce Nuclear Generating Station B Power Reactor Operating Licence, June 1, 2015.
- [19] CNSC REGDOC-2.4.2, Probabilistic Safety Assessment for Nuclear Power Plants, 2014.
- [20] CAN/CSA N285.0-12, General Requirements for Pressure-Retaining Systems and Components in CANDU Nuclear Power Plants, 2012 (Update 1, 2013).
- [21] CAN/CSA N286-12, Management System Requirements for Nuclear Power Plants, June 2012.
- [22] CAN/CSA N286.7-99, Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants, March 1999 (Reaffirmed in 2012).
- [23] CAN/CSA N290.13, Environmental Qualification of Equipment for CANDU Nuclear Power Plants, 2005 (reaffirmed 2010).
- [24] CAN/CSA N290.15-10, Requirements for the Safe Operating Envelope of Nuclear Power Plants, 2010.
- [25] CAN/CSA N293-12, Fire Protection for Nuclear Power Plants, 2012.
- [26] BP-PROG-00.04-R020, Pressure Boundary Quality Assurance Program, March 21, 2014.
- [27] NK21-CORR-00531-11494, 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.
- [28] 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.
- [29] NK21-CORR-00531-11563, CSA N286-12 - Management System Requirements for Nuclear Facilities, Action Item 1307-4697, Bruce Power Letter, F. Saunders to K. Lafrenière, September 9, 2014.
- [30] CNSC G-149, Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors, 2000.
- [31] 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.
- [32] B-REP-00701-29NOV2013-059, Assessment of Fire Protection at Bruce Power, November 29, 2013.
- [33] NK21-CORR-00531-11715, Bruce Power: Requests and Supplemental Information for Licence Renewal, Bruce Power Letter, F. Saunders to M. Leblanc, November 28, 2014.
- [34] CNSC R-10, The Use of Two Shutdown Systems in Reactors, Canadian Nuclear Safety Commission, January 11, 1977.

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- [35] 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.
- [36] CNSC RD-346, Site Evaluation for New Nuclear Power Plants, 2008.
- [37] CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants, 2014.
- [38] 13-M25, Regulatory Framework Program Update, CNSC, May 16, 2013.
- [39] IAEA NS-R-3, Site Evaluation for Nuclear Installations, International Atomic Energy Agency, Safety Requirements, November 2003.
- [40] 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. Desjardins, December, 22, 2006.
- [41] CAN/CSA B51-14, Boiler, Pressure Vessel, and Pressure Piping Code, 2014.
- [42] CAN/CSA N285.2-99, Requirements for Class 1C, 2C, and 3C Pressure-Retaining Components and Supports in CANDU Nuclear Power Plants, 2004.
- [43] CAN/CSA N287.1-14, General Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, February 2014.
- [44] CAN/CSA N287.2-08, Material Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, March 2008 (Reaffirmed 2013).
- [45] CAN/CSA N287.3-14, Design Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, 2014.
- [46] CAN/CSA N287.4-09, Construction, Fabrication, and Installation Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, October 2009.
- [47] CAN/CSA N287.5-11, Examination and Testing Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, May 2011.
- [48] CAN/CSA N288.4-10, Environmental Monitoring Programs at Class I Nuclear Facilities and Uranium Mines and Mills, 2010.
- [49] CAN/CSA N289.1-08, General Requirements for Seismic Qualification for CANDU Nuclear Power Plants, September 2008.
- [50] CAN/CSA N289.2-10, Ground Motion Determination for Seismic Qualification of Nuclear Power Plants, 2010.
- [51] CAN/CSA N289.3-10, Design Procedures for Seismic Qualification of CANDU Nuclear Power Plants, 2010.
- [52] CAN/CSA N289.4-12, Testing Procedures for Seismic Qualification of CANDU Nuclear Power Plants, 2012.
- [53] CAN/CSA N289.5-12, Seismic instrumentation requirements for nuclear power plants and nuclear facilities, 2012.
- [54] CSA Group N290.0-11, General Requirements for Safety Systems of Nuclear Power Plants, October 2011.

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- [55] CAN/CSA N290.1, Requirements for the Shutdown Systems of CANDU Nuclear Power Plants, 2013.
- [56] CSA Group N290.2-11, Requirements for Emergency Core Cooling Systems of Nuclear Power Plants, October 2011.
- [57] CSA Group N290.3-11, Requirements for the Containment System of Nuclear Power Plants, October 2011.
- [58] CAN/CSA N290.4-11, Requirements for Reactor Control Systems of Nuclear Power Plants, 2011.
- [59] CAN/CSA N290.5, Requirements for Electrical Power and Instrument Air Systems of CANDU Nuclear Power Plants, 2006 (Reaffirmed 2011).
- [60] 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).
- [61] CSA Group N290.11-13, Requirements for Reactor Heat Removal Capability During Outage of Nuclear Power Plants, December 2013.
- [62] CAN/CSA N291-08 Requirements for Safety-Related Structures for CANDU Nuclear Power Plants, March 2008 (Reaffirmed 2013).
- [63] NK21-SR-01320-00003-R004, Bruce A 2012 Safety Report, Part 3: Accident Analysis, Bruce Power, January 3, 2012.
- [64] NK21-CORR-00531-11045, CNSC RDs and CSA Standards to be Referenced in the PROLs, CNSC email, A. Robert to M. Burton, June 17, 2014.
- [65] NK21-CORR-00531-00784, Bruce A: Submission #3 (May 15, 2002) in Support of Bruce A Return to Service, Bruce Power Letter, F. Saunders to J.H.M. Douglas, May 14, 2002.
- [66] NK21-CORR-00531-01008, Attachment A to Submission #3 in Support of Bruce A Return to Service, CNSC Letter, M.P. Burton to F. Saunders, August 12, 2002.
- [67] NK21-CORR-00531-10560, Bruce Power Progress Report #3 on CNSC Action Plan – FAIs, Bruce Power Letter, F. Saunders to R. Lojk, July 17, 2013.
- [68] NK21-CORR-00531-11324, Submission of S-294 Probabilistic Risk Assessment Final Reports, Bruce Power Letter, F. Saunders to K. Lafrenière, July 31, 2014.
- [69] NK21-CORR-00531-06559, Bruce A Units 1 and 2 Return to Service, Integrated Safety Review – Category 3 Issues 5.5.18, 5.9.9, 5.10.21 and 5.23.4, Bruce Power Letter, F. Saunders to K. Lafrenière, December 15, 2008.
- [70] NK21-CORR-00531-11567, Integrated Implementation Plan for Bruce A, Bruce B and Centre of Site in the Next Licence Period, Bruce Power Letter, F. Saunders to K. Lafrenière, October 31, 2014.
- [71] ANSI/NIRMA CM 1.0 – 2007, American National Standard for Guidelines for Configuration Management of Nuclear Facilities, August 2007.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- [72] ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components", Revision 9, Reedy Engineering, September 19, 2014.
- [73] Darlington-DG-38-03650-1, Purpose and Application of Nuclear Safety Design Guides.
- [74] Darlington-DG-38-03650-2A, Common Mode Incidents – Overview and Design Requirements.
- [75] Darlington-DG-38-03650-2B, Common Mode Incidents – Seismic Design.
- [76] Darlington-DG-38-03650-3, Limiting Consequential Damage of Postulated Pipe Ruptures.
- [77] Darlington-DG-38-03650-4, Shutdown Systems.
- [78] Darlington-DG-38-03650-5, Emergency Coolant Injection.
- [79] Darlington-DG-38-03650-6, Containment.
- [80] Darlington-DG-38-03650-7, Extensions of the Containment Envelope.
- [81] Darlington-DG-38-03650-8, Environmental Qualification of Safety Related Equipment.
- [82] Darlington-DG-38-03650-9, Safety Assessments.
- [83] National Building Code of Canada, Government of Canada, 2010.
- [84] National Fire Code of Canada, Government of Canada, 2010.
- [85] NFPA-801, Standard for Fire Protection for Facilities Handling Radioactive Material, 2003 Edition.
- [86] 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.
- [87] CAN/CSA N293-07, Fire Protection for CANDU Nuclear Power Plants, Reprinted January 2008.
- [88] BP-MSM-1-R012, Management System Manual, Bruce Power, June 23, 2014.
- [89] BP-MSM-1 Sheet 0001-R020, MSM-Bruce Power Program Matrix, Bruce Power, January 2015.
- [90] BP-MSM-1 Sheet 0003-R005, MSM-List of Applicable Governing Acts, Regulations, Codes & Standards, Bruce Power, September 2014.
- [91] BP-PROG-01.02-R008, Bruce Power Management System (BPMS) Management, Bruce Power, December 18, 2014.
- [92] BP-PROG-10.01-R009, Plant Design Basis Management, Bruce Power, December 4, 2014.
- [93] BP-PROG-10.02-R009, Engineering Change Control, Bruce Power, December 13, 2013.
- [94] BP-PROG-11.01-R004, Equipment Reliability, Bruce Power, October 8, 2013.
- [95] BP-PROG-10.03, R006, Configuration Management, Bruce Power, February 5, 2015.
- [96] BP-PROC-00915-R000, Pressure Boundary Quality Assurance Program Oversight, Bruce Power, April 3, 2013.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- [97] BP-PROC-00335-R006, Design Management, Bruce Power, May 24, 2013.
- [98] BP-PROC-00363-R003, Nuclear Safety Assessment, Bruce Power, January 24, 2013.
- [99] DIV-ENG-00009-R005, Design Authority, November 1, 2013.
- [100] BP-PROC-00582-R003, Engineering Fundamentals, Bruce Power, July 25, 2014.
- [101] BP-PROC-00502-R002, Resolution of Differing Professional Opinions, Bruce Power, October 12, 2010.
- [102] BP-PROC-00743-R003, Site Services Engineering Change Control, Bruce Power, November 28, 2012.
- [103] BP-PROC-00542-R005, Configuration Information Change, Bruce Power, July 25, 2013.
- [104] BP-PROC-00539-R015, Design Change Package, Bruce Power, August 26, 2014.
- [105] BP-PROC-00877-R000, Modification Installation Quality Assurance, Bruce Power, October 29, 2012.
- [106] BP-PROC-00615-R001, Commissioning Modifications and Projects, Bruce Power, September 20, 2013.
- [107] BP-PROC-00470-R004, Configuration Management Program Oversight and Trending, Bruce Power, October 1, 2012.
- [108] BP-PROC-00584-R006, PassPort Equipment Data Management, Bruce Power, December 4, 2012.
- [109] BP-PROC-00638-R012, Temporary Configuration Change Management, Bruce Power, May 7, 2014.
- [110] BP-PROC-00647-R002, PassPort Permit Request Processing, Bruce Power, September 11, 2013.
- [111] BP-PROC-00786-R003, Margin Management, Bruce Power, August 5, 2014.
- [112] BP-PROC-00898-R000, Equipment Codes, Bruce Power, June 19, 2013.
- [113] SEC-DO-00001-R009, Drafting Office Work Management, November 29, 2012.
- [114] BP-PROC-00778-R001, Scoping and Identification of Critical SSCs, April 11, 2013.
- [115] DPT-RS-00012-R001, Systems Important to Safety (SIS) Decision Methodology, Bruce Power, September 24, 2013.
- [116] BP-PROC-00169-R002, Safety-Related System List, Bruce Power, September 28, 2007.
- [117] BP-PROC-00137-R014, Focus Area Self-Assessment, Bruce Power, June 17, 2014.
- [118] BP-PROC-00412-R006, Trend Identification and Reporting of SCRs, Bruce Power, August 18, 2014.
- [119] BP-OPP-00001-R015, Operating Policies and Principles-Bruce B, Bruce Power, October 8, 2013.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- [120] BP-OPP-00002-R013, Operating Policies and Principles-Bruce A, Bruce Power, March 31, 2014.
- [121] CAN/CSA N286.0-92, Overall Quality Assurance Program Requirements for Nuclear Power Plants, September 1992 (Reaffirmed 2003).
- [122] BP-PROC-00268-R005, Safety System Testing (SST) Program Procedure, Bruce Power Procedure, August 27, 2014.
- [123] DIV-ENG-00017-R001, System and Item Classification, Bruce Power Procedure, June 29, 2012.
- [124] SEC-EQD-00031-R002, Preparation of Environmental Qualification Dossiers (EQD), Bruce Power Procedure, June 27, 2011.
- [125] NK21-CALC-20091-00002-R06, Bruce NGS A Seismic Assessment Seismic Success Path and Equipment List, Bruce Power, March 18, 2011.
- [126] DPT-PDE-00028-R004, Fire Safe Shutdown Analysis Maintenance, Bruce Power, October 28, 2013.
- [127] 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.
- [128] BP-PROC-00261-R005, Environmental Qualification, Bruce Power, November 7, 2012.
- [129] DPT-PDE-00017-R005, Bruce Power Seismic Qualification Standard, Bruce Power, July 4, 2012.
- [130] RABA 0804 Review of Bruce NGSA Against Modern Safety Standards Draft Regulatory Document RD-337 Design of New Nuclear Power Plants, October 16, 2008.
- [131] NK21-CORR-00531-10874, Performance Review for Bruce A and Bruce B – October 2013, Bruce Power Letter, F. Saunders to M. Leblanc, November 1, 2013.
- [132] NK21-CORR-00531-11279, Action Items 090734 and 091413: Bruce A and Bruce B: Legacy Registration Project Update, Bruce Power Letter, F. Saunders to K. Lafrenière, May 22, 2014.
- [133] NK21-CORR-00531-10178/NK29-CORR-00531-10588/eDoc 4057030, Action Item 091413: Bruce Legacy Registration Transition Plan, CNSC Letter, R. Lojk to F. Saunders January 9, 2013.
- [134] NK21-CORR-00531-11672/NK29-CORR-00531-12061, Action Items 090734 and 091413, Bruce A and Bruce B Legacy Registration Project Update, Bruce Power Letter, F. Saunders to K. Lafrenière, November 27, 2014.
- [135] CAN/CSA A23.3-14, Design of Concrete Structures, June 2014.
- [136] NK21-CORR-00531-10873, Application to Renew Reactor Operating Licence for Bruce Nuclear Generating Station A (PROL 15.00/2014), Bruce Power Letter, F. Saunders to R. Lojk, November 2013.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


- [137] NK21-CORR-00531-10988, Bruce A and B – Response to Notification on Completeness of Licence Renewal Applications, Bruce Power Letter, F. Saunders to R. Lojk, February 4, 2014.
- [138] NK21-REP-03600-00012-00, Bruce A Units 1 and 2 Return to Service Review against Design Standards, NSS, July 31, 2006.
- [139] 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.
- [140] NK21-DG-20091-002-R001, Bruce A Seismic Design Guide Units 034, Bruce Power Design Guide, February 2004.
- [141] NK21-CORR-00531-11339, 2014 Annual COG Research and Development Reporting, F. Saunders to K. Lafrenière, June 16, 2014.
- [142] BP-PROG-03.01-R015, Document Management, Bruce Power, August 18, 2014.
- [143] BP-PROC-00068-R021, Controlled Document Life Cycle Management, Bruce Power, August 22, 2014.
- [144] BP-PROC-00098-R014, Records Management, Bruce Power, December 5, 2013.
- [145] DPT-NSAS-00012-R003, Preparation and Maintenance of Operational Safety Requirements, Bruce Power, September 8, 2011.
- [146] DPT-RS-00015-R000, Safe Operating Envelope Gap Assessment, Bruce Power, May 31, 2011.
- [147] 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.
- [148] 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.
- [149] SCR 28390834, Inadequate Implementation of CSA N290.15 into BP-PROG-10, September 24, 2013.
- [150] DPT-PDE-00006-R013, Design Plan, Bruce Power, June 26, 2014.
- [151] DPT-PDE-00024-R006, Preparation and Revision of Overpressure Protection Reports, Bruce Power, May 6, 2014.
- [152] DPT-PDE-00034-R001, Preparation and Revision of System Design Manuals, Design Requirements and Design Descriptions, Bruce Power, June 21, 2007.
- [153] DPT-PDE-00013-R008, Human Factors Engineering Program Plan, Bruce Power, June 16, 2014.
- [154] BP-PROC-00014-R009, Technical Operability Evaluation, Bruce Power, October 23, 2014
- [155] BP-PROC-00375-R001, Software Development, Bruce Power, October 7, 2014.
- [156] DIV-ENG-00005-R009, Engineering Calculations, Bruce Power, July 30, 2014.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


- [157] DPT-PDE-00044-R000, Preparation and Maintenance of Instrument Uncertainty Calculations, Bruce Power, December 9, 2014
- [158] DPT-PDE-00040-R001, Preparation of Instrument Calibration Specifications, Bruce Power, July 29, 2014.
- [159] SEC-RSA-00001-R002, Preparation of the EQ Room Conditions Manual, Bruce Power, July 30, 2014.
- [160] FORM-10700-R020, Design Scoping Checklist, Bruce Power.
- [161] FORM-12608-R002, Design Review of Design Change Notice, Bruce Power.
- [162] FORM-13200-R006, Design Products Challenge Board Checklist, Bruce Power.
- [163] CNSC REGDOC-3.1.1, Reporting Requirements for Nuclear Power Plants, CNSC, May 2014.
- [164] 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.
- [165] NK21-63720/63730 P NSAS, Bruce NGS A Units 1&2: Assessment of NOP Trip Coverage at 2019 Aged Core Conditions, October 15, 2013.
- [166] NK21-63720/63780 P NSAS, Bruce NGS A Units 3&4: Assessment of NOP Trip Coverage at 2019 Aged Core Conditions, August 21, 2013.
- [167] NK21-03507.1 P NSAS, Bruce NGS A Unit 1&2 Small LOCA Assessment to the End of 2019, December 11, 2013.
- [168] NK21-03507.1 P NSAS, Bruce A Units 3&4 Small LOCA Analysis in Support of Operation to 2019 of Operation to 2019, December 11, 2013.
- [169] NK21-REP-03507.1 P NSAS, RD-310 PILOT Project – Electrical System Failures, December 2013.
- [170] NK21-03507.1 P NSAS, Bruce NGS A Units 3&4 Loss of Flow Analysis in Support of Operation to 9950 EFPD, December 11, 2013.
- [171] NK21-03503.7 LOF NSAS, Assessment of Impact of Change in Coolant Void Reactivity on Large Break LOCA Analysis for Bruce A Units 1 and 2, December 11, 2013.
- [172] NK21-03503.7 LOF NSAS, Analysis of Large Break Loss of Coolant Accident for Bruce A NGS Units 3 and 4 in Support of Operation to 9950 EFPD, November 28, 2013.
- [173] NK21-CORR-00531-10774, Safety Report Improvement Plan for Bruce A and B, Bruce Power, November 20, 2013.
- [174] NK21-CORR-00531-11214, 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.
- [175] CNSC REGDOC-2.4.1, Safety Analysis: Deterministic Safety Analysis, May 2014.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- [176] NK21-CORR-00531-11710, 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.
- [177] NK29-CORR-00531-11252, Application for the Renewal of the Power Reactor Operating Licence for Bruce Nuclear Generating Station B, Bruce Power Letter, F. Saunders to M. Leblanc, October 31, 2013.
- [178] BP-PROC-00781-R002, Performance Monitoring, Bruce Power Procedure, September 22, 2012.
- [179] CNSC RD/GD-98, Reliability Programs for Nuclear Power Plants, June 2012.
- [180] NK21-CORR-00531-10063, Bruce Power Progress Report No. 2 on CNSC Action Plan – Fukushima Action Items, Bruce Power Letter, F. Saunders to R. Lojk, January 31, 2013.
- [181] NK21-CORR-00531-01414, Addendum to Attachment A to Submission #3 (May 15, 2002) in Support of Bruce A Return to Service, Bruce Power Letter, F. Saunders to J.H.M. Douglas, January 20, 2003.
- [182] NK21-CORR-00531-11379, Bruce Power Progress Report No. 5 on CNSC Action Plan – Fukushima Action Items, Bruce Power Letter, F. Saunders to K. Lafrenière, July 15, 2014.
- [183] NK21-SR-01320-00002-R005, Bruce A 2012 Safety Report – Part 2: Plant Components and Systems, Bruce Power, February 2013.
- [184] B-REP-00701-09DEC2013-060, Summary of Bruce Power Fukushima Action Items for the 2014 Interim Periodic Safety Review, Bruce Power, December 9, 2013.
- [185] NK21-CORR-00531-11381, 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.
- [186] NK21-CORR-00531-10341, Bruce Power Irradiated Fuel Bay Structural Integrity Analysis, Bruce Power Letter, F. Saunders to R. Lojk, March 26, 2013.
- [187] NK21-CORR-00531-10565, 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.
- [188] NK21-DM-24400, Ancillary Service Building Substructure and Spent Fuel Bay, Bruce Power, February 1976.
- [189] COG-JP-4426-005-R0, Multi-Unit Events Update of SAMG and Technical Basis Documents, CANDU Owners Group, June 2013.
- [190] NK21-OM-35030-R001, Bruce Nuclear Generating Station A Operating Manual – NUFLASH, Bruce Power, January 3, 2008.
- [191] BP-PROG-15.01-R004, Nuclear Oversight Management, Bruce Power, December 18, 2013.
- [192] CC171-11/2013E, CNSC Staff Integrated Safety Assessment of Canadian Nuclear Power Plants for 2013, September 2014.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- [193] NK21-CORR-00531-11443, Action Item 2014-07-5211: Bruce A Electrical Power Systems Inspection BRPD-A-2014-004, CNSC Letter, K. Lafrenière to F. Saunders, July 2, 2014.
NK21-CORR-00531-09307, Opening of Fukushima Action Items (FAIs) on Bruce Power, CNSC Letter, G. Rzentkowski to F. Saunders, February 17, 2012.
- [194] NK21-CORR-00531-09676, Bruce Power Progress Report No. 1 on CNSC Action Plan – Fukushima Action Items, Bruce Power Letter, F. Saunders to R. Lojk, February 17, 2012.
- [195] NK21-CORR-00531-10963, Bruce Power Progress Report No. 4 on CNSC Action Plan – Fukushima Action Items, Bruce Power Letter, F. Saunders to R. Lojk, January 30, 2014.
- [196] NK21-CORR-00531-11184, Human Factors in Design Desktop Review – August 12 to 16, 2013, CNSC Letter, K. Lafrenière to F. Saunders, March 13, 2014.
- [197] EPRI NP-5652, Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications, EPRI, September 2014.
- [198] DPT-NSAS-00011-R004, Configuration Management of Safety Analysis Software, Bruce Power, October 11, 2013.
- [199] DPT-NSAS-00013-R003, Guidelines for Managing Reference Data Sets, Bruce Power Procedure, September 20, 2011.
- [200] COG-09-9030 R03, Principles & Guidelines for Deterministic Safety Analysis Used in Licensing of Current Nuclear Power Plants Operating in Canada, CANDU Owners Group, November 2014.
- [201] ISTR-12-5044, Code Validation Guidelines Document, IST Report/COG, November 2012.
- [202] ISTO-09-5092, Guidelines for Generic Methodology for Estimation of Computer Code Accuracy, IST Report/COG, September 2012.
- [203] NK21-CORR-00531-10460, CNSC Review of Bruce Power Status Update #2 on Fukushima Action Items – New Action Items 1307-3676, 1307-3692, 1307-3790, 1307-3791, 1307-3793 to 1307-3797, CNSC Letter, R. Lojk to F. Saunders, April 30, 2013.
- [204] BP-PROC-00400-R002, Life Cycle Management for Critical SSCs, Bruce Power, July 5, 2013.
- [205] B-PLAN-20000-00001-R000, Life Cycle Management Plan for Civil Structures, Bruce Power, July 5, 2010.
- [206] NK21-PIP-20000-00001-R000, CSA N291 In-Service Inspection Program for Bruce NGS A Safety Related Structures, September 2014.
- [207] NK21-CORR-00531-10183, Action Item 1207-3890: Bruce Power CSA N293-07 Site Transition Plan, Bruce Power Letter, F. Saunders to R. Lojk, May 28, 2013.
- [208] NK21-CORR-00531-11170, Action Item 1407-4602: Bruce A Seismic Margin Assessment Upgrades Semi-annual Update, Bruce Power Letter, F. Saunders to K. Lafrenière, April 8, 2014.
- [209] DPT-COM-00004 R002, Critical Drawing Management, Bruce Power, Obsolete.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

[210] NK21-CORR-00531-10926, 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.

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 [30] 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 framework of developing a computer code program from code coding, verification, validation, maintenance and documentation.

As documented in Safety Factor 5, a high level assessment of G-149 requirements is performed to confirm that these are covered by CSA N286.7-99 [22]. This high level assessment concludes that all G-149 requirements are encompassed by those of CSA N286.7-99 which is in the operating licence. Accordingly, meeting CSA N286.7-99 requirements will satisfy the intent of G-149 guidance.

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

- BP-PROG-10.01, Plant Design Basis Management [92],
- BP-PROC-00363, Nuclear Safety Assessment, Bruce Power [98],
- DPT-NSAS-00011 Configuration Management on Safety Analysis Software [198]
- DPT-NSAS-00013, Guidelines for Managing Reference Data Sets [199].

Moreover, DPT-NSAS-00011, Configuration Management on Safety Analysis Software [198] also indicates its consideration to CNSC G-149 guidance.

The Safety Analysis Improvement (SAI) task team of the CANDU industry has established guidelines for performing Deterministic Safety Analysis [200], for conduct of computer code validation [201], and for computer code accuracy assessment [202]. 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 [173] is based on the use of these guidelines.

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

As part of this ISR, a high-level review of standard CSA N287.1 was conducted against the latest version of the applicable standard (CSA N287.1-14). The clauses in the standard are related in general to ensure that the design, construction, and testing of concrete containment

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

structures will meet a quality and standard commensurate with the safety principles necessary to comply with the Canadian nuclear safety philosophy. This standard applies to new nuclear power plants' concrete containment structures at the design level. A prior evaluation consisting of a clause-by-clause review of standard CSA N287.1-93 (re-affirmed 2004) was performed in 2008 against Bruce A design documents, describing the current design of the plant's concrete containment structures. The compliance evaluation of the CSA N287.1-93 (re-affirmed 2004) standard had identified no gaps and concludes that the design is in compliance with the standard.

The standard had been revised since (CSA N287.1-14), introducing new sets of requirements. A code-to-code assessment was performed to the previous version (CSA N287.1-93) to identify the new and different requirements brought by the current standard for assessment. A high level screening to identify the new and different requirements was considered sufficient for the purpose of this ISR, as the new and different requirements do not significantly impact the design basis of the concrete containment structures. The screening has identified three main topics newly introduced comparing to its previous version, which are: (1) Assessing ageing effects on containment structures; (2) Preparation and reporting of commissioning reports on SSCs; and (3) Establishment and implementation of in-service examination and testing. These main, newly introduced, requirements are listed and discussed below.

Ageing – The objective of this new requirement is to consider the ageing effects on containment structures. Bruce Power has established a Life Cycle Management Plan for Civil Structures (B-PLAN-20000-00001) that outlines a plan to detect and mitigate ageing mechanisms for civil structures and components, along with the acceptance criteria and safety margins for ageing degradations of civil structures and components. An incremental clause-by-clause assessment of CSA N287.14 and consideration of the effect of ageing is addressed in detail under Safety Factor 4 Ageing, which concluded that all new requirements were met.

Commissioning – The objective of this new requirement is to establish commissioning test requirements and reports on SSCs. The commissioning requirements do not apply to Bruce A since the concrete containment structures are already installed and in operation. As such, this new requirement is not a design requirement; therefore compliance was not required.

In-Service Examination and Testing – The objective of this new requirement is to establish and implement an in-service examination and testing program. Bruce Power has established an In-Service Testing and Inspection to satisfy CSA N287.7-08 Requirement; NK21-PIP-21100-00001 CSA N287.7-08 Periodic Inspection Program for Bruce NGS A Concrete Containment Structures and Appurtenances (Excluding Vacuum Building) and NK21-PIP-25100-00001 CSA N287.7-08 Periodic Inspection Program For Bruce NGS A Vacuum Building (BP-PROC-00361 R001). This procedure can be used as part of this assessment since it describes the program required for monitoring and maintaining the structural integrity of concrete containment structures during the operating life of the station. As such, this was deemed as in compliance, despite the clause and sub-clauses not classified as design requirements.

Conclusion – In general, the newly introduced requirements listed above were determined not to have an impact on the design basis of existing concrete containment structures since these requirements are applicable at a design level.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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

As part of this ISR, a high-level review of standard CSA N287.3 was conducted against the latest version of the applicable standard (CSA N287.3-14). The clauses in the standard are related to establishing specific requirements for the design of concrete containment structures and addresses their beyond design basis assessment. This standard applies to new nuclear power plants' concrete containment structures at the design level. A prior evaluation consisting of a clause-by-clause review of standard CSA N287.3-93 (re-affirmed 2004) was performed in 2008 against Bruce A design documents, describing the current design of the plant's concrete containment structures. The compliance evaluation of the CSA N287.3-93 (re-affirmed 2004) standard had identified no gaps in compliance with the standard.

The standard has been revised since (CSA N287.3-14) the previous review was completed, introducing new sets of requirements. A code-to-code assessment was performed to the previous version (CSA N287.3-93) to identify the new and different requirements in the current standard. A high level screening to identify the new and different requirements was considered sufficient for the purpose of this ISR, as the new and different requirements do not significantly impact the design basis of the concrete containment structures. The screening has identified three main topics newly introduced comparing to its previous version, which are: (1) Assessing containment structures for beyond design basis; (2) Members subjected to flexure or axial loads, or both, to be designed in accordance with the requirements of CSA A23.3 [135]; and (3) Walls, slabs, shells, and domes to be reinforced in accordance with clauses of CSA A23.3. These main, newly introduced, requirements are listed and discussed below.

Beyond design basis – The objective of this new requirement is to assess containment structures for beyond design basis to ensure adequate safety margins against containment failure. The Summary of Bruce Power Fukushima Action Items for the 2014 Interim Periodic Safety Review [184] identifies the Bruce Power Fukushima Action Item 1.3.1 where “Assessments of adequacy of the existing means to protect containment integrity and prevent uncontrolled release in beyond-design-basis accidents including severe accidents”. This FAI is closed based on “submission of information from the supporting analysis for the level 2 PRA which showed that containment integrity can be challenged during a multi-unit severe accident, particularly if no mitigating measures are available or are credited”.

Flexure or axial loads – The objective of this new requirement is to design the members subjected to flexure or axial loads in accordance with the requirements of CSA A23.3. Bruce A concrete containment structures were designed based on the National Building Code, CSA standards A23.1, A23.3, S16 and ACI standards applicable at the time. CSA N287 series standards were later developed based on the design practices employed for concrete containment structures of a CANDU Nuclear Power Plant. As such, this new requirement is not applicable for the current concrete containment structures at the post-design level.

Walls, slabs, shells, and domes – The objective of this new requirement is to reinforce these structures in accordance with clauses of CSA A23.3. This requirement is related to seismic qualification. Bruce A qualification is established in the Seismic Margin Assessment (SMA), based on the evaluation of SSCs (Section 2.5 of the Bruce A Safety Report NK21-SR-01320-00002). The containment structures were designed based on the National Building Code, CSA

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

standards A23.1, A23.3, S16 and ACI standards applicable at the time. CSA N287 series standards were later developed based on the design practices employed for concrete containment structures of a CANDU Nuclear Power Plant. As such, this new requirement is not applicable for the current concrete containment structures at the post-design level.

Conclusion – In general, the newly introduced requirements listed above were determined to not have an impact on the design basis of existing concrete containment structures since these requirements are applicable at a design level with the exception of beyond design basis. As noted, a Fukushima Action Item was established to assess the adequacy of the existing means to protect containment integrity in beyond design-basis accidents. Bruce Power has addressed this issue and the action item has been closed as per NK21-CORR-00531-10460 [203].

A.4. CSA N291-08 (R2013), Requirements for Safety-Related Structures for CANDU Nuclear Power Plants

A high-level review has been performed on the 2008 version (Reaffirmed in 2013). As part of the discussions with the CNSC on Action Item 1107-2185 on the Life Cycle Management Program for Civil Structures, Bruce Power has proposed an implementation plan and transition measures for the future inclusion of CSA N291-08, “Requirements for Safety-Related Structures for CANDU Nuclear Power Plants” into the Station PROLs and LCHs. CSA N291 is related to the physical design of SSCs, fitness for service (or Condition Assessment), and safety analysis supporting design. The standard is referenced in BP-MSM-1 Sheet 0003-R005 (page 12 of 17), and is identified as a typical source document in BP-PROC-00498 R006, Condition Assessment of Generating Units in support of Life Extension, January 19, 2011. A number of civil structures at Bruce Power (i.e., Bruce A and B) have been identified [116] as structures whose degradation or failure could have serious safety or economic consequences. Bruce Power’s Equipment Reliability Program [94] requires that all SSCs identified, be part of the Ageing Management program. The requirement is to prepare a civil structure Life Cycle Management Plan (LCMP) as per [204] and subsequent condition assessments for the remaining structures in this list. Similar structures can be grouped for the purpose of optimizing condition assessments. The LCMP for civil structures is outlined in [205]. 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. Condition Assessments are being developed for those structures that are shown to be critical to safety and generation. The governance requires that Preventive Maintenance (PM) procedures be developed for the other civil structures, if required.

CSA N291-08 provides material, design, construction, fabrication, inspection, and examination requirements for Safety-Related Structures for CANDU nuclear power plants. To comply with CSA N291-08, Bruce Power plans to utilize the research described in Reference [141] and the experience gained from the aforementioned LCMP, 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. Walkdowns and inspections of both stations were performed by certified Professional Engineers and civil field technicians qualified to CSA N287 General Requirements for Concrete Containment Structures for CANDU Nuclear Power

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Plants. Areas covered at Bruce A included Units 0, 3, and 4, East Services Area, Vacuum Building, Ancillary Services Building, Accumulator Building, Unit 3 and 4 pump houses, and the old water treatment plant. Team members followed the visual inspection procedures. As noted in References [136] and [13], detailed results of inspection findings were photographed, summarized and documented in reports.

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; and
- Facilities for the storage of irradiated fuel and other radioactive waste material.


The in-service examination program required by CSA N291-08 is documented in NK21-PIP-20000-00001, R000, CSA N291 In-Service Inspection Program for Bruce NGS A Safety Related Structures, September 2014 [206]. Included in the NK21-PIP-20000-00001 are the inspection schedule and the report names for the safety-related structures to be inspected

A.5. NFPA-801 (2011), Standard for Fire Protection for Facilities Handling Radioactive Materials

Section 1.1.2 of NFPA 801, states that it shall not be applied to commercial power reactors that are covered by NFPA 804, Standard for Fire Protection for Advanced Light Water Reactor Electric Generating Plants, and NFPA 805, Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants. Accordingly, NFPA 805 (2010 edition) was reviewed at a high level against Bruce Power's Fire Protection Program to ensure that it incorporates all requirements relevant for CANDU reactors. During the review it was evaluated that NFPA 805 was subsumed into CSA N293-12 in regards to the fire protection concepts and performance requirements. The review assessed that CSA N293-12 is an objective-based standard, whereas NFPA 805 is a performance-based standard that included specific plant safety design requirements. CSA N293-12 references NFPA 805 for specific guidance on economic loss prevention, preparation and review of probabilistic safety assessments, and design guidance. Based on the communications to CNSC in May 2013 [207], CNSC staff states that Bruce Power has effectively completed the transition to CSA N293-07. Analysis of CSA N293-07 against CSA N293-12 is completed as part of an additional review in Safety Factor 7 Hazards Analysis.

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.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

A high level review of Bruce Power programs against the requirements in this standard is performed. 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' 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 SF10 and results summarized in section 5.3.10 of the SFR, as well as in SF11 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) [1] and associated MSM sheets define and document Bruce Power's Management System.

Bruce Power uses programs to implement the MSM [1] and define regulatory and business requirements. BP-MSM-1 Sheet 0001 [2] 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 [2] under the functional area of Configuration Management Engineering.

The BPMS Management Program [3] establishes the framework for the ongoing implementation to and change management of the BPMS. As specified in section 4.5.2 of the BPMS Management Program [3] 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 [4]. 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 [1]. The President and Chief Executive Officer is "personally committed to the Bruce Power Management System and expect the leadership, management and staff of

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Bruce Power to be individually and collectively committed to this Management System and to performing within its requirements and principles". As stated in Appendix A of the MSM [1] 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 [5] is established to ensure 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 main principles that define the CM Program are listed in Appendix A Configuration Management Program Principles [5]. The Plant Design Basis Management Program [6] and the Engineering Change Control Program BP-PROG-10.02 [7] govern the management of distinct changes to the plant design basis.

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. Physical changes are covered via BP-PROC-00539 Design Change Package.

The link to Safety Analysis is captured in BP-PROC-00363 Nuclear Safety Assessment. Lower tier procedures under BP-PROC-00363, including DPT-NSAS-00011 Configuration Management of Safety Analysis Software, DPT-NSAS-00012 Preparation and Maintenance of Operational Safety Requirements, DPT-NSAS-00015 Planning and Execution of Nuclear Safety Assessments, [8] 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.

Configuration Management Program [5] 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.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 [5] 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 [9].

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 program [7] 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 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 A 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 [10]. 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-R001, Systems Important to Safety (SIS) Decision Methodology [11]. 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.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

The configuration management concepts, terminology and definitions are established and documented in section 3.1 and in Appendix A of [5]. As required in clause 3.1.4, these definitions are incorporated into the associated facility procedures. As specified in C.1 of Appendix A [5], 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 [6] and BP-PROG-10.02, Engineering Change Control [7]. 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 [5]. 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 [5].

As described in section 4.6 of BP-PROC-00335 Design management [12] 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 [7] and BP-PROG-10.03, Configuration Management [5].

DPT-PDE-00025, Engineering Change Paper Management [13], 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 [14].

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 [5].

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. The Plant Design Basis Management [6] defines the elements, functional requirements, implementing procedures and key responsibilities associated with the management of 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 [7].

The procedure DPT-PDE-00034 Preparation and Revision of System Design Manuals, Design Requirements and Design Description [15] provides a systematic and uniform process for preparation and revision of System Design Manuals (SDM) for Bruce Power. It includes

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

instructions for the preparation of Design Requirements (DR) 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 [16], Safe Operating Envelope Gap Assessment) to ensure that the plant is being operated in accordance with specified requirements.

As described in [17] 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 [18] 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 [19]. 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 [5]), as documented in BP-PROC-00898 [19], 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 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 [20], 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.

As specified in section 1.0 of [5] “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 [5] applies to all SSCs. Since there are no exceptions (section 2.0 in [5]) to 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 [5] 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 [6]) “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 [12] 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

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

selection and modification is reviewed, verified and approved by the responsible design organization.

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 [21] 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 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 [12]. As described in section 4.7 of [12] "Design information, including changes, shall be communicated from one organization to another, and 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 [22]. 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 [12] 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 [23], and BP-PROC-00098, Records Management [24]. Retention of records is managed through BP-PROC-00238, Retention Process for Bruce Power Records [25]. The process for managing the life cycle of Bruce Power Controlled documents is defined in BP-PROC-00068 [27].

All records are managed according to Records Management procedure BP-PROC-00098 [24] to ensure all records regardless of media are properly categorized. BP-PROC-00972, Records Retrieval and Secure Storage [23], 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 [25] for Bruce Power Records.

The control and tracking of records is performed through the PassPort system. According to BP-PROC-00584 [26] PassPort Equipment Data Management (section 4.3.3): Configuration

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 [28] for Configuration Information Changes (CIC) or BP-PROC-00539 [17] for Design Change Packages depending on the type of Engineering Change (EC). 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 [27], to be submitted. Design Engineering and Drafting Office representatives are responsible for restoring plant configuration by updating PassPort MEL database and design documents (section 7 of [26]). 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 [23] (section 4.2.2) for records that have been approved by the Records Officer to be retained in electronic medium are stored in a secure environment that prevents unauthorized access and protection from physical disaster (i.e., Content Server). Electronic records that are stored in Content Server have controls such as user authentication and permissions 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 [29].

The facility information is available in a database and readily retrievable. BP-PROC-00972 Records Retrieval and Secure [23] applies to all records and defines the controls applied for records retrieval. Records are designated permanent or non-permanent. For non-permanent records minimum retention period is defined to minimize redundant information. The records access is controlled to ensure the integrity of all records as defined in section 4.2.6 of BP-PROC-00972 Records Retrieval and Secure [23]. The document management program is subject to records management oversight activities per BP-PROC-00238 Retention Process for Bruce Power Records [30].

As specified in C.5 of BP-PROG-10.03 [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. Data is controlled at its source and resides in one location. Redundant plant configuration information is minimized”. Section 1 of BP-PROG-10.03 [5] 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 and plant operation for normal and abnormal operation are governed by BP-PROG-12.01, Conduct of Plant Operations [31]. 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 [31]).

Operating procedures are created as controlled documents, in accordance with the requirements of BP-PROG-03.01, Document Management [32] to ensure that document

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

lifecycle management requirements defined in BP-PROC-00068, Controlled Document Life Cycle Management [27].

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 [5], 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 (C.4, Appendix A of [5]).

The BP-PROG-10.02, Engineering Change Control (ECC) Program [7] 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 [7]). The ECC Program [7] defines the steps necessary to ensure that proper reviews are 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 [7], the Program includes the following implementing procedures:

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

Non-physical changes to the design are covered via BP-PROC-00542 Configuration Information Change [28] whereas the physical changes are covered via BP-PROC-00539 Design Change Package [17].

The ECC program applies a graded approach based on risk. Section 4.0 of [7] 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 [33] 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 [33]). As described in section 4.0 of [33], Nuclear Safety Assessment addresses proposed or planned changes such as design changes, changes to operating procedures, maintenance and surveillance requirements, or plant status changes.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Section 4.7 of BP-PROG-10.03 [5] requires configuration management control of the temporary changes. The Temporary Configuration Change Management process is documented in BP-PROC-00638 [34] 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 [7], the Configuration Information Change process, BP-PROC-00542 [26], 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.

The Design Change Package process, as documented in BP-PROC-00539 [17], 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 [7]).

The Configuration management program requires that the impact on the plant simulator to be identified. Section C.4 of Appendix A of [5] 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 [35], 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 engineering change (EC) is the electronic PassPort record of a design change or modification. The EC provides information necessary to develop and prepare an ITP that 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 [7]).

BP-PROC-00703 [36] 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 [36] 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 [36].

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

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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

The Nuclear Oversight Management Program [37] 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 [1], 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 [37]. 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 [38]. The Configuration Management program [5], Document Management [32], Plant Design Basis Management [6] and Engineering Change Control Program [7] 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 is reflected in BP-PROC-00539 Design Change Package [17], BP-PROC-00615 Commissioning of Modifications and Projects [39] and BP-PROC-00877 Modification Installation Quality Assurance [35]. The objective of the Bruce Power Corrective Action Program BP-PROC-01.07 [40] 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 [40], 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 the BP-PROC-00060 [41], the Station Condition Record (SCR) 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 [40] corrective actions are tracked to completion through PassPort system as defined in BP-PROC-00019, Action Tracking [42]. 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-PROC-11.01 [43] and assessed in detail in SF2 and SF4.

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 [44]. 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 [44]). 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 [45]. 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 [46]. 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

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

expectations, the indicator owner is responsible to produce an action plan that will close the gap (section 4.8 of [5]). Effectiveness of Bruce Power's configuration management activities is also addressed in Section 5.3.10 of SF10 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 section C.1 of Appendix A of [5] as follows: "CM awareness is promoted and training is included in initial and continuing training programs if required by the position". Section C.4 of Appendix A of [5] further requires that "training materials should coincide with or precede each plant modification".

Section 3.1.3 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.


Appendix 1 Specific Qualifications of TQD-00082 R001 presents the qualifications that 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 [47].

References:

- [1] BP-MSM-1-R012, Management System Manual, Bruce Power, June 23, 2014.
- [2] BP-MSM-1 Sheet 0001-R021, MSM - Bruce Power Program Matrix, January 05, 2016.
- [3] BP-PROG-01.02-R009, Bruce Power Management System (BPMS) Management, December 15, 2015.
- [4] BP-MSM-1 Sheet 0002-R015, MSM - Approved Reference Chart Authorities and Responsibilities – Sheet 0002, January 20, 2015.
- [5] BP-PROG-10.03-R006, Configuration Management, February 5, 2015.
- [6] BP-PROG-10.01-R009, Plant Design Basis Management, December 4, 2014.
- [7] BP-PROG-10.02-R010, Engineering Change Control, November 12, 2014.
- [8] DPT-NSAS-00015-R004, Planning and Execution of Nuclear Safety Assessments, October 16, 2013.
- [9] DIV-ENG-00009-R005, Design Authority, November 1, 2013.
- [10] BP-PROC-00169-R002, Safety Related System List, September 28, 2007.
- [11] DPT-RS-00012-R001, Systems Important to Safety (SIS) Decision Methodology, R001, September 24, 2013.
- [12] BP-PROC-00335-R007, Design Management, July 30, 2015.
- [13] DPT-PDE-00025, Engineering Change Paper Management, June 14, 2013.
- [14] DPT-NSAS-00012-R004, Preparation and Maintenance of Operational Safety Requirements, October 28, 2014.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- [15] DPT-PDE-00034-R001, Preparation and Revision of System Design Manuals, Design Requirements and Design Description, June 21, 2007.
- [16] DPT-RS-00015-R000, Safe Operating Envelope Gap Assessment, May 31, 2011.
- [17] BP-PROC-00539-R016, Design Change Package, June 23, 2015.
- [18] B-LIST-08133-00001-R011, Controlled Document Numbering List for PASSPORT, February 7, 2014.
- [19] BP-PROC-00898-R000, Equipment Codes, June 19, 2013.
- [20] BP-PROC-00320-R004, Management of System/Subject Classification Indexes, June 2, 2010.
- [21] BP-PROC-00786-R003, Margin Management, August 5, 2014.
- [22] DPT-PDE-00006-R013, Design Plan, June 26, 2014.
- [23] BP-PROC-00972-R000, Records Retrieval and Secure Storage, November 21, 2014.
- [24] BP-PROC-00098-R015, Records Management, November 27, 2014.
- [25] BP-PROC-00238-R011, Retention Process for Bruce Power Records, December 6, 2013.
- [26] BP-PROC-00584-R008, PassPort Equipment Data Management, October 19, 2015.
- [27] BP-PROC-00068-R023, Controlled Document Life Cycle Management, December 11, 2015.
- [28] BP-PROC-00542-R007, Configuration Information Change, November 24, 2015.
- [29] BP-PROG-03.02-R004, Information Technology, June 02, 2014.
- [30] BP-PROC-00238-R012, Retention Process for Bruce Power Records, November 26, 2014.
- [31] BP-PROG-12.01-R007, Conduct of Plant Operations, August 13, 2013.
- [32] BP-PROG-03.01-R016, Document Management, August 31, 2015.
- [33] BP-PROC-00363-R003, Nuclear Safety Assessment, January 24, 2013.
- [34] BP-PROC-00638-R012, Temporary Configuration Change Management, May 7, 2014.
- [35] BP-PROC-00877-R000, Modification Installation Quality Assurance, October 29, 2012.
- [36] BP-PROC-00703-R001, Change Management Guidance, December 1, 2010.
- [37] BP-PROG-15.01-R004, Nuclear Oversight Management Program, December 18, 2013.
- [38] BP-PROC-00295-R003, Audit Basis and Approach, December 19, 2013.
- [39] BP-PROC-00615-R001, Commissioning of Modifications and Projects, September 20, 2013.
- [40] BP-PROG-01.07-R010, Corrective Action, August 30, 2013.
- [41] BP-PROC-00060-R028, Station Condition Record Process, November 05, 2015.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- [42] BP-PROC-00019-R009, Action Tracking, October 04, 2012.
- [43] BP-PROG-11.01-R005, Equipment Reliability, December 16, 2015.
- [44] BP-PROC-00470-R004, Configuration Management Program Oversight and Trending, October 1, 2012.
- [45] BP-PROC-00137-R015, Focus Area Self-Assessment, March 10, 2015.
- [46] BP-PROC-00412-R006, Trend Identification and Reporting of SCRs, August 18, 2014.
- [47] TQD-00082-R001 Configuration Management and Support, Training and Qualification Description, May 31, 2011.

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][3] 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 QA provisions
- Changes allowing new or alternative materials
- Changes that incorporate code cases, 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.

The Safety Basis Report states that, in the 2008 Safety Factor 1: Plant Design report, a review was conducted for Bruce A (Units 1 to 4) from the basis of the Bruce 1&2 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

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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.

- 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.

This issue was included in the Bruce Units 3 and 4 Integrated Implementation Plan from the 2008 Integrated Safety Review as item # IIP-50, "Complete Re-registration Activities and Recover Original Design Documentation" [3] as well as the Bruce Units 1/2 Integrated Implementation Plan [4]. The Bruce A legacy registration project has been completed [6], resolving this IIP item.

- 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 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

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 was included in the Bruce Units 3 and 4 Integrated Implementation Plan from the 2008 Integrated Safety Review as item # IIP-68, "Perform fatigue analysis for cyclic operation transient loads on Class 4 Containment Penetrations" [3]. As part of the closure of AI 020718, an assessment concluded that fatigue damage to penetrations under service loading conditions will not be an issue over the extended operating life of the Bruce A reactors. Therefore, the design of the Bruce A Class 4 penetrations is acceptable and meets the fatigue analysis requirements of the ASME Code. This issue is considered to be closed for Bruce A.

- **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 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 was included in the Bruce Units 3/4 Integrated Implementation Plan from the 2008 Integrated Safety Review as item # IIP-69, "Perform fatigue assessment for Class 2, 3 and 4 bellows expansion joints" [3]. This gap is identified as SF1-9 in Table 13. As part of the closure of AI 020718, Bruce Power evaluated a sample number of typical Class 2, 3, 4 bellows expansion joints and demonstrated that all designs meet the applicable sections of ASME Code. These typical assessments constitute an evaluation of the impact of fatigue for Class 2, 3 and 4 bellows expansion joints. Hence, this issue is considered to be closed for Bruce A.

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 December 7, 2012, 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 2014

Significant changes to ASME Section III up to the 2013 annual addenda 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 item noted in the Code Reconciliation Report, ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components of 2014 September 19 [2], Appendix 6, is a change identified in ASME Section III, introduced in the 2013 Edition, which should be reviewed further to assess the potential impact on safety margins:

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- 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.

This change may impose more conservative requirements, so should be assessed for impact on pressure boundary design governance documentation. This is identified as gap SF1-15 in Table 8.

No other changes noted in Reference [1], 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.

References:

- [1] ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components, Revision 8, Reedy Engineering, May 21, 2012.
- [2] NK21-CORR-00531-11005, Submission of Safety Basis Report, Bruce Power Letter, F. Saunders to R. Lojk, December 30, 2013.
- [3] NK21-REP-03600-00025-R001, Bruce NGS A Units 3 and 4 Global Assessment Report and Integrated Implementation Plan, May 29, 2009.
- [4] NK21-REP-03600-00021-R008, Bruce NGS A Units 1 and 2 Global Assessment Report and Integrated Implementation Plan, June 30, 2008.
- [5] NK21-CORR-00531-12046, Action Item 090734: Bruce A Legacy Registration Project, CNSC letter, K. Lafreniere to F. Saunders, April 1, 2015.
- [6] NK21-CORR-00531-12288, Integrated Implementation Plan for Bruce A, Bruce B, and Centre of Site, Bruce Power Letter, F. Saunders to K. Lafreniere, December 18, 2015.
- [7] ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components, Revision 9, Reedy Engineering, September 19, 2014.

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

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- Changes that incorporate code cases, alternative rules or calculation methods
- Changes allowing alternative test methods.

Summary of previous review findings

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. The assessment 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 committed to evaluate Class 6 safety-related systems for cyclic and dynamic reactions for steam and waterhammer loads and initiate appropriate actions if warranted.

This issue was included in the Bruce Units 3 and 4 Integrated Implementation Plan from the 2008 Integrated Safety Review as item # IIP-51, "Complete Pressure Vessel Re-certification Activities" [5] as well as the Bruce Units 1 and 2 Integrated Implementation Plan [3]. The Bruce A Legacy Registration project has been completed [6], resolving this IIP item.

Summary of SBR findings - changes to ASME VIII Division I from 2007 to 2011 [4]

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 2014

The following item noted in the Code Reconciliation Report ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Component of 2014 September 19 [2], Appendix 7, is a change identified in ASME Section VIII, since 2011, introduced in the 2013 Edition, which should be reviewed further to assess the potential impact on safety margins:

- Appendix 26 - 26-2(g)
Bellows Design

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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.

This change may impose more conservative requirements, so should be assessed for impact on pressure boundary design governance documentation. This is identified as gap SF1-16 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.

References:

- [1] ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components, Revision 8, Reedy Engineering, May 21, 2012.
- [2] ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components, Revision 9, Reedy Engineering, September 19, 2014.
- [3] NK21-REP-03600-00021-R000, Bruce NGS A Units 1 and 2 Global Assessment Report and Integrated Implementation Plan, June 30, 2008.
- [4] NK21-CORR-00531-11005, Submission of Safety Basis Report, Bruce Power Letter, F. Saunders to R. Lojk, December 30, 2013.
- [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-00531-12046, Action Item 090734: Bruce A Legacy Registration Project, CNSC letter, K. Lafreniere to F. Saunders, April 1, 2015.

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 QA provisions
- Changes allowing new or alternative materials
- Changes that incorporate code cases, 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

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Bruce A units, "Cyclic loads were not considered for Bruce NGSA Class 6 piping components as they were not specified in the Bruce NGSA 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 addressed for Units 1 and 2. The results are expected to be applicable to Units 3 and 4 [6].

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 [7]. 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 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, 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 2014

Significant changes to ASME B31.1 up to the 2013 annual addenda 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, introduced in the 2012 Edition:

- 101.7.2, 122.1.1(I)
Expansion Joints

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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.

The potential issues mentioned in the SBR and noted above have not been addressed. Consequently, this is identified as gap SF1-17 in Table 8.

References:

- [1] ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components", Revision 8, Reedy Engineering, May 21, 2012.
- [2] ANSI/ASME Code Reconciliation for Replacement Material, Parts, and Components, Revision 9, Reedy Engineering, September 19, 2014.
- [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, 2004.
- [5] NK21-REP-03600-00025-R001, Bruce NGS A Units 3 and 4 Global Assessment Report and Integrated Implementation Plan, May 2009.
- [6] NK21-CORR-00531-11567, Integrated Implementation Plan for Bruce A, Bruce B, and Centre of Site, Bruce Power Letter, F. Saunders to K. Lafreniere, October 31, 2014.
- [7] NK21-CORR-00531-11005, Submission of Safety Basis Report, Bruce Power Letter, F. Saunders to R. Lojk, December 30, 2013.

A.10. CSA N290.0-11, General Requirements for safety systems of nuclear power plants

This is a new standard that establishes the general requirements related to 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. The 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 SF2 and SF4.

CSA N290 series of standards include requirements on equipment qualification, human factors, system health monitoring, maintenance program and testing in addition to those associated with 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 SF2, SF3, SF4 and SF12.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 N290.0 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 concluded that the design of Bruce A 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 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:

- i. Shutdown System 1 (SDS1).
- ii. Shutdown System 2 (SDS2).
- iii. Negative Pressure Containment (NPC) system.
- iv. Emergency Coolant Injection (ECI) system.

These systems are independent of each other and are in poised state during plant operation.

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, 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 A Units 1, 2, 3, and 4 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 SAMG updates

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

related to multi-unit events and irradiated fuel bay events have been completed as described in [5].

The plant states as defined in clause 4.2 are not explicitly covered in the existing design documentation. As presented in [6], the basis on which Bruce A was 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). A summary of the acceptance criteria applied to Bruce Power accident analysis are provided in Section 1.5 of Part 3 of the Safety Report [7]. However, the current requirements deal only with the single process system failures (DBAs) and the dual failure limits, some of which would be considered as BDBAs. 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 addressbdba in deterministic safety analysis. This gap is being addressed by the CNSC Action Item 090739: Safety Report Improvement Plan [8] for Bruce A and Bruce B. This is already assessed as a gap SF1-1 in Table 8; therefore this gap is not repeated here.

The safety analyses documented in Part 3 of Safety Report [7] 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 S-98 is a licence condition 4.4 Fitness for Service Program in PROL 15.00/2015 [9]. Bruce A uses the reliability program described in BP-PROG-11.01 [10] 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 [10], life cycle management integrates ageing management and asset life 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 6.1.3 of Part 2 of the Safety Report [2] 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 10^{-3} year/year.

The reliability targets are specified in the design manuals. The reliability of the special safety systems is monitored and reported as required in clause 4.5.2.1. The Annual Reliability Reports demonstrate that the probability of failure on demand from all causes for some safety systems has not been consistently lower than 10^{-3} . This is already assessed as a gap SF1-5 in Table 8.

Changes in equipment performance data and relevant OPEX are incorporated in the update of Annual Reliability Reports and PRA models.

The special safety systems are independent of each other. To effectively reduce the risk presented by a postulated process system failure, special safety systems are physically and functionally independent of each other and process systems, including the reactor regulating

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

system, whose failure might require the subsequent action of the special safety system as described in section 6.1.2 of the Bruce Safety Report Part 2 [2].

As discussed in Part 2, Section 6.1.4 of the Safety Report [2] the separation requirement is addressed in the design. 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. Selected redundant equipment and their control systems/supplies are arranged in separated areas to minimize the probability of common accidents affecting all systems.

Clause 4.7 specifies the requirements related to single failure criteria. A review of similar clauses in REGDOC-2.5.2 [3] indicated that the application of the single failure criterion for the Bruce A design does not follow the newer, more restrictive, interpretations of the single failure criterion; therefore is assessed as a gap (SF1-5) against clause 7.6.2 of REGDOC-2.5.2.

To the extent practicable, the special safety system components are designed such that the most likely failure modes are in the fail-safe direction as required in clause 4.8. Since there are exceptions to this design rule (e.g., a few containment boundary valves fail open following loss of instrument air leading to possible impairment of containment on end shield cooling post steam line break) this is assessed as a gap (SF1-1) against 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 A support systems meet the intent of these requirements, except as indicated in the text.

Operational Safety Requirements for Bruce A Electrical System [11] present the safety limits, applicable analysis and surveillance requirements for Bruce A 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 of the Bruce A Safety Report Part 2 [2]).

Licence condition 6.1 *Pressure Boundary Program* requires the licensee to implement and maintain a pressure boundary program to ensure compliance with CSA N285.0 [12].

The Bruce A 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, 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 6.1.4 of Part 2 of the Safety Report [2]). The Operational Safety Requirements for special safety systems, i.e. shutdown systems [13], containment [14] and emergency coolant injection system [15] specify the testing and monitoring requirements required to verify that the system meets its performance and reliability requirements.

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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. Although the Bruce A design documentation does not explicitly reflect this requirement, the error models to capture the different sources of errors associated with the calibration of instrumentation are discussed in Part 3 of the Safety Analysis. Therefore, it is assessed as Acceptable Deviation.


As described in section 6.6 of Part 2 of Safety Report, 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 [16]. The results of this program are documented in Environmental Qualification Requirements of Safety Related Systems and Structures for Bruce A [17] which contains the detailed requirements for each of the systems subject to environmental qualifications.

Seismic Qualification Success Path is a list that identifies all of the SSCs credited with safe shutdown for a seismic event. These are contained in [18]. As discussed in Part 2, Section 2.5.1.1 of the Safety Report [2], to address Seismic Qualification for Bruce A, a Seismic Margin Assessment (SMA) was conducted [19]. The assessment was in accordance with the SMA guidelines of EPRI NP-6041SL with modifications to fit the unique characteristics of the CANDU reactor system. The SMA is based on the evaluation of all structures, systems and components that make up the “success path”, including the reactors and their auxiliary systems, control systems, electrical systems, as well as the civil structures. The electrical and mechanical components are captured on the Safe Shutdown Equipment List (SSEL). Seismic qualification priority list is provided in Table 2-3 of Part 2 of the Safety Report [2]. In the EPRI approach to SMA, it is necessary to demonstrate operation and survival of components and structures to bring the plant to a safe shutdown and maintain it there for 72 hours. The set of components selected to demonstrate this ability is called the success path. The path selected for the Bruce A SMA is shown in Table 2-2, Part 2 of the Safety Report.

Bruce A design meets the aging requirement, as documented in the Equipment Reliability Program [10]. 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 [10], 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 DEC, this is assessed as a gap against clause 7.4.1 of REGDOC-2.5.2 (**Gap**). This gap is included under SF1-1 in Table 8.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

The Bruce A design includes protection against common mode events as described in Section 2.5 of Part 2 of the Safety Report [2]. This includes:

1. Seismic Qualification
2. Missile Protection
3. Protection Against Dynamic Effects Associated with the Rupture of Piping
4. Environmental Qualification of Safety-Related Equipment.

Bruce A complies with the human factors related requirements. Bruce Power has a Human Factors Engineering Program Plan, DPT-PDE-00013 [20], 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 [21].

Sections 4.16 to 4.20 cover the requirements related to System Health Monitoring, operability, maintainability, maintenance program and testing.

Bruce A has extensive testing programs to demonstrate that the special safety systems meet their ongoing reliability requirements. Section 03.5 of the Bruce Operating Policies & Principles (OP&Ps) [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.

The process for development of Life Cycle Management Plans for Systems, Structures, or 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 will then be 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 [27]. Life Cycle Management is one of the key elements of BP-PROG-11.01, Equipment Reliability Program [10]. System health monitoring, reporting and management are extensively discussed in Safety Factor 2.

Bruce A 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 of Safety Report [2], the instrumentation and control systems are designed to a large variety of detailed requirements, depending on their

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

function, importance and physical environment. However, all the systems are designed to the following general criteria:

1. 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.
2. 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.
3. Equipment is designed for a minimum of regular maintenance. Any necessary maintenance operations are kept as simple and speedy as possible.
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.
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.
6. Where possible, the control systems are designed to prevent or minimize damage to equipment.

Bruce A meets the intent of the operability requirements as described in the 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. In addition, the 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 systems' design allow for maintenance to ensure compliance with their design basis and performance requirements. Section 03.5 of the Bruce Operating Policies & Principles (OP&Ps) 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. 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.

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Design provisions are also 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. 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 (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, BP-PROG-11.04 Plant Maintenance and BP-PROG-00.04 Pressure Boundary Quality Assurance Program and their supporting procedures. These programs are addressed extensively under SF2.

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 A design meets the requirement for periodic testing of the entire channel of instrumentation logic. The channelized logic at Bruce A 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 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 [6].

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&Ps Section 63.1 Shutdown System Availability [22].

With respect to commissioning requirements in clause 4.20, Bruce A Safety Report, Bruce Power DMs, and OSR do not explicitly state tests should be done prior to first criticality of the reactor. Commissioning tests were carried out to demonstrate that all parts and functions of the system meet their design requirements under normal conditions during initial start-up of the plant, after a long-term lay-up of Units 3 and 4 and following refurbishment of Units 1 and 2. With regards to systems modifications, the requirements for commissioning planning, commissioning specification, execution and reporting are defined in Commissioning Modifications and Projects [28].

Sections 4.21 and 4.22 presents the requirements related to sharing within a unit and between units. Bruce A meets the intent of these requirements.

The requirements related to sharing between safety and process systems within a unit are not applicable to CANDU reactors' design. Special safety systems are physically separated from process systems and there is no instrumentation sharing between safety and process systems.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Special safety systems are independent of the process systems and perform no process functions. As described in Section 6.1.4 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, usually 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 A design does not fully meet the requirements as documented in [32]. 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 Emergency Cooling Injection 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. This sharing of systems was factored into the reliability requirements of these systems and each has redundant components to ensure adequate reliability. 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 A design meets the intent of this requirement.

Section 4.23 presents the requirements for design documentation, SOE documents, operational documents, history docket and operational history.

A general design description of the plant is provided in Parts 1 and 2 of the Bruce A Safety Report. 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 [29].

The design documentation follows well established processes and procedures as described in Design Management [30]. 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 [31] to ensure nuclear safety requirements are incorporated into the design. Under the Equipment Reliability Program [10], 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 plant and site, including environmental conditions. Plant components and systems are described in Part 2 of the Safety Report. 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 A Probabilistic Risk Assessment (PRA) includes Level 1 and Level 2 analyses. The Bruce A PRA model, abbreviated as BAPRA, is the result of a continuing process of updates and improvements that began in 2003 with the development of the original BAPRA model version BAPRA16B C6798/TR/005 Ver0. A full summary of the changes made to the

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

BAPRA model since its inception is provided in Appendix F of the year 2014 version of the Level 1 At-Power Internal Events NK21-03611.1 P NSAS Ver00. The list of current Bruce PRA analyses and corresponding guides is presented in Safety Factor 6.

The Bruce A design documentation does include Hazard Analysis. The detailed hazard analysis of protection against fire is generated as per DPT-PDE-00027 [33], DPT-PDE-00028 [34] and DPT-PDE-00029 [35], and is documented in NK21-REP-71400-00003 [36], NK21-REP-71400-00004 [37] and NK21-REP-71400-00005 [38]. Seismic margin in the event of earthquake is generated as per DPT-PDE-00017, and is assessed in NK21-REP-20091-00001. Other internal and external hazards are assessed in RABA-0601 (Enclosure 5 to NK21-CORR-00531-04059). Detailed assessments related to hazards analysis are documented in Safety Factor 7.

Bruce Power is implementing 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. 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.

Issues relevant to the adequacy of design documentation are identified as SF1-8, SF1-10 and SF1-11 and are considered gaps. These gaps relate to the adequacy of design documentation pertaining to the guaranteed shutdown state, seismic qualification and design, lifting and handling of large loads, design extension conditions. The sources of these issues are micro-gaps against CNSC REGDOC-2.5.2 and CSA N290.1 requirements, 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 OLCs. These limits are based upon the up to date safety analysis and also incorporated in OP&Ps and operating manuals.


As described in Safety Factor 5, Bruce A has recently 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. Bruce Power is moving from Operating Policies and Principles (OP&Ps) 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.

References:

- [1] CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants, May 2014.
- [2] NK21-SR-01320-00002-R005, Bruce A 2012 Safety Report – Part 2: Plant Components and Systems, Bruce Power, February 2013.
- [3] BP-PROG-10.01-R009, Plant Design Basis Management, Bruce Power, December 4, 2014.
- [4] BP-PROG-00.04-R020, Pressure Boundary Quality Assurance Program, March 21, 2014.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- [5] NK21-CORR-00531-12209, 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] RABA 0804 Review of Bruce NGSA Against Modern Safety Standards Draft Regulatory Document RD-337, Design of New Nuclear Power Plants, October 16, 2008.
- [7] NK21-SR-01320-00003-R004, Bruce A 2012 Safety Report, Part 3: Accident Analysis, Bruce Power, January 3, 2012.
- [8] NK21-CORR-00531-10774, Safety Report Improvement Plan for Bruce A and B, Bruce Power, November 20, 2013.
- [9] NK21-CORR-00531-11391, Bruce Nuclear Generating Station A Nuclear Power Reactor Operating Licence: Licence Conditions Handbook (LCH-BNGSA-R8), June 4, 2014.
- [10] BP-PROG-11.01-R004, Equipment Reliability, Bruce Power, October 8, 2013.
- [11] NK21-OSR-53000/55000-00001-R000, Operational Safety Requirements for Bruce A Electrical System, August 2009.
- [12] CAN/CSA N285.0-12, General Requirements for Pressure-Retaining Systems and Components in CANDU Nuclear Power Plants, 2012 (Update 1, 2013).
- [13] NK21-OSR-63720-63730-00001-R000, Operational Safety Requirements for Bruce A Shutdown Systems, January 18, 2008.
- [14] NK21-OSR-34200-00004-R001, Operational Safety Requirements for Bruce A Containment System, December 21, 2007.
- [15] NK21-OSR-34340-00003-R002, Operational Safety Requirements for Bruce A Emergency Coolant Injection System, May 2013.
- [16] NK21-MAN-03651-00001-R003, Bruce A Environmental Qualification Room Conditions Manual, March 2012.
- [17] NK21-EQR-03651-00001-R003, Environmental Qualification Requirements of Safety Related Systems and Structures for the Bruce A Nuclear Generating Station, June 2006.
- [18] NK21-CALC-20091-00002-R06, Bruce NGS A Seismic Assessment Seismic Success Path and Equipment List, Bruce Power, March 18, 2011.
- [19] NK21-REP-03611-00005-R000, Bruce A Units 1 and 2 Seismic Margin Assessment Report, December 8, 2006.
- [20] DPT-PDE-00013-R008, Human Factors Engineering Program Plan, June 16, 2014.
- [21] B-REP-00701-29NOV2013-059, Assessment of Fire Protection at Bruce Power, November 29, 2013.
- [22] BP-OPP-00002-R013, Operating Policies and Principles-Bruce A, Bruce Power, March 31, 2014.
- [23] BP-PROC-00400-R002, Life Cycle Management for Critical SSCs, Bruce Power, July 5, 2013.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- [24] DPT-PE-00008-R007, System and Component Performance Monitoring Plans, February 18, 2016.
- [25] DPT-PE-00009-R000, System and Component Performance Monitoring Walkdowns, September 24, 2007.
- [26] DPT-PE-00010-R006, System Health Reporting, August 27, 2013.
- [27] BP-PROC-00666, Component Categorization, Bruce Power, June 13, 2013.
- [28] BP-PROC-00615-R001, Commissioning Modifications and Projects, Bruce Power, September 20, 2013.
- [29] BP-PROG-10.02-R009, Engineering Change Control, Bruce Power, December 13, 2013.
- [30] BP-PROC-00335-R006, Design Management, Bruce Power, May 24, 2013.
- [31] BP-PROC-00363-R003, Nuclear Safety Assessment, Bruce Power, January 24, 2013.
- [32] NK21-CORR-00531-11005/NK29-CORR-00531-11397, Submission of Safety Basis Report, Bruce Power Letter, F. Saunders to R. Lojk, December 30, 2013.
- [33] DPT-PDE-00027-R003, Fire Hazard Assessment Preparation and Maintenance, October 29, 2013
- [34] DPT-PDE-0028-R004, Fire Safe Shutdown Analysis Maintenance, October 28, 2013.
- [35] DPT-PDE-0029-R003, Fire Protection Code Compliance Review Maintenance, November 20, 2013.
- [36] NK21-REP-71400-00003-R005, Fire Hazards Assessment, August 22, 2012.
- [37] NK21-REP-71400-00004-R006, Bruce-A Nuclear Generating Station, August 20, 2012.
- [38] NK21-REP-71400-00005-R005, Fire Protection Code Compliance Review, August 14, 2012.

A.11. CSA N290.2-11, Requirements for emergency core cooling systems of nuclear plants

This is a new standard that 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 Bruce Power design against the requirements in this standard is performed. This high level review is focused on the applicable requirements for Emergency Coolant Injection System, which performs the emergency core cooling function for Bruce A reactors. The assessment concluded that the design of the 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.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Section 4 lists the functional requirements for emergency cooling systems. The Emergency Coolant Injection (ECI) System is a special safety system, designed to operate under the conditions existing after a Loss of Coolant Accident (LOCA) and subsequent shutdown.

The system meets the functional and design requirements as defined in the system design manual [1]. The ECI system design requirements are summarized in Section 6.3.2 of Part 2 of the Safety Report [2]. The overall emergency core cooling design target is to support maintaining the fuel to remain in a coolable geometry for all LOCA break sizes up to and including a guillotine break of the largest header and to prevent major fuel and pressure tube damage for break sizes up to and including the size of the largest feeder [1]. The ECI is designed to initiate automatically for all postulated breaks down to a size when the make-up from the D₂O 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. There are no cases in the Part 3 of Safety Report [3] where manual initiation of the ECI is required. The safety analysis documented in Part 3 of the Safety Report [3] has confirmed that the system meets the design requirements.

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:

- 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. In the event of a loss of coolant accident the availability of the valves associated with Emergency Coolant Injection at the Heat Transport System pressure boundary is assured by periodic testing of the valves to ensure a sufficiently high degree of reliability; those valves which must open are duplicated in parallel and meeting the requirements for Class 1 components in Section III of the ASME Code.

The systems that supply electrical power and cooling water to equipment used in the operation of the ECI system are classified as safety support systems and the process is documented in Safety Related System List procedure [4]. The initial high-pressure injection system does not require electrical power for its operation. A set of accumulators is the injection source for the initial high pressure injection phase. Use of stored energy (in the form of pressurized gas) makes the injection independent of external energy supplies. The low-pressure pumps used to inject water from the grade level tank and from the recovery system require Class III power. The normal Class III supply is backed up by the standby generators that are automatically started by the HPECI initiation logic. The accident analysis has shown that even with the interruption of the Class IV power, the allowable release limits are not exceeded [3].

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.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Section 5.1 General

The ECI system is a special safety system and meets the general requirements as described in the high level review of CSA N290.0.

Section 5.2 Systems Operation

As described in section 6.3 of Part 2 of 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 NGSA 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 (SDS1). Section 3.2.3 of Part 3 of Safety Report [3] indicates that the shutdown action by the least effective SDS is credited in the safety analysis of LOCA.

The ECI system design takes into account the potential sources of gas intrusion. An assessment (section 6.1.7 of [5]) investigated the possibility of air becoming entrained in the flow from the common recirculation line, as it connects to the Grade Level Water Storage Tank (GLWST) discharge piping in a horizontal section, which could be drained if the GLWST fails to isolate. The assessment showed that even a conservative estimate of the amount of entrained air would be insufficient to damage the recovery pumps, and noted that the process is self-limiting, since any resulting degradation in pump performance would reduce the recirculation flow, thereby reducing the amount of entrained air at the pump suction. The design details and associated safety limits are provided in the Design Manual and ECI OSRs.

The Safety Related System Impairments Manual (ECI Impairments) [6] lists the ECI three normal (unimpaired) states during normal station operation as follows:

- Poised – system will act automatically and manually
- Blocked – system will not act automatically but can be initiated by Control Room action
- Shutdown – system will not act automatically and operation cannot be initiated from Control Room.

As described in the ECI OSRs [5], the high pressure ECIS must be operable to any unit whenever Heat Transport System temperature is greater than 90°C. However, the ECIS can be blocked for HTS temperature greater than 90°C if certain conditions are in place. Section 34 and Appendix A of Bruce A OP&P [7] present the conditions for ECI manual blocking. The Emergency Coolant Injection System shall only be isolated for maintenance if the associated heat transport systems are cooled to below 90°C. It shall be possible to return the system to service in the event that heat transport system coolant inventory cannot be maintained. Section 34.4 Emergency Coolant Injection System Maintenance [7] provides further details.

The ECI system short- and long-term operation is described in ECI OSR [5] and Part 2 of Safety Report [1]. The ECI automatic initiation meets the requirements for response to ECI initiation signal. The safety analysis limits, surveillance requirements and operability conditions for the ECI system are documented in ECI OSRs [5]. As for all special safety systems, all actions of the ECI system can be manually initiated from the Main Control Room. It is noted that there are only limited controls and only the HPECI portion of the ECI (including the operation of the boiler SRVs) can be controlled from the SCA. The instrumentation and controls related to low

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

pressure injection and long-term recovery are described in the Emergency Coolant Injection System Instrumentation and Control Design Manual [8].

The system is provided with a recovery pump strainers at the recovery sump intake to prevent obstruction of the flow. Periodic inspection of the recovery sump ensures there is no debris which could restrict flow to the recovery pumps and that the strainers have not deteriorated and would still perform their function of preventing large debris generated during an accident from reaching the pumps.

Clause 5.2.6.4 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 following 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 1×10^{-3}). The control logic makes use of sealed mercury-wetted contact relays assembled into plug-in modules for easy replacement if required. The alarms and signal isolators are front-accessible units. The ECI system uses channelized distribution frames in each instrument room to allow easy access to system signals from a single location. As a design requirement, components requiring maintenance are located outside containment if practicable. In addition, components shall be capable of being isolated for maintenance during normal reactor operation. Every component required for automatic response to a LOCA is tested including the initiating logic. The test frequency is established based on the components' known failure rate and their redundancy [8].

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 [8]. The system is designed so that component failure or partial power failure will not cause a spurious injection to be initiated. In Bruce A, each bank of four boilers (steam generators) is connected to a long horizontal steam drum where primary moisture separation (by cyclone separators) takes place. There are 12 steam Safety Relief Valves (SRVs) per drum (24 SRVs per Unit) which are to be opened on a LOCA signal, concurrently with ECI initiation. The SRVs during normal plant operation are closed and are used to protect the steam system from overpressure (self-actuating). Addition of power operated actuators is provided to open the SRVs for boiler steam crash cooldown. Descriptions of boiler steam crash cooldown instrument loops and make up water supply controls are provided in the Design Manual [8].

The unit portion of the system consists of the equipment which is unique to each reactor unit. The system parameters indicative of a LOCA are monitored in each unit. The control logic which initiates the injection is also repeated in each unit. The appropriate valve actions that will connect the common supply header to the HT system for that unit are initiated and the common supply portion of the system is then requested to act. Controls on the Main Control Room operator's panel are described in the ECI Design Manual [8].

The ECI system must initiate on the detection of low pressure in the Heat Transport System in combination with one of the conditioning signals, which are reactor vault high pressure or temperature, moderator high level, or heat transport sustained low pressure. The ECI design

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

meets the intent of the requirements by providing automatic instrumentation to monitor and initiate system actuation when required. There are eight categories of automatic instrumentation functions as described in ECI OSRs:

ECIS Initiation - This function detects sustained Heat Transport System (HTS) low pressure condition in one of the units and, provided one of the ECIS conditioning signals has been registered, initiates emergency injection by activating unit and common devices. It also implements delays, which minimize water hammer.

LOCA Conditioning Signals - In order to reduce the probability of injection when it is not required, one of the LOCA conditioning signals must be registered along with HTS low pressure to initiate injection. The limits on the conditioning parameters ensure that ECIS will be effective for the range of accidents for which it is credited.

Accumulator Water Tank (AWT) Isolation - This function isolates the AWTs once their inventory has been injected into the Heat Transport System of the accident unit.

Recovery Initiation - This function starts the recovery phase of emergency injection when water discharged into containment is drawn from the recovery sump and recirculated through the broken Heat Transport System.

Grade Level Water Storage Tank Isolation - This function isolates the GLWST when it is depleted.

Boiler Safety Relief Valves (Crash Cooldown) Logic - This function actuates the crash cooldown of boilers in accident unit to lower the Heat Transport System pressure and thus to enhance the emergency coolant injection rate.

ECI Pump Logic - This function detects injection pump failure and starts one of the other pumps. It also implements the delays necessary to ensure that ECIS piping is refilled before pumped injection is resumed to prevent excessive water hammer.

ECI Room Sump Pump Logic - This function starts and stops the sump pumps in the Leakage Mitigation Subsystem.

Section 5.4 Usability Requirements Specific to Manual Operation

As with all safety systems, once their automatic functions are initiated, no single operator action can stop the ECI system operation. It is noted in [9] that once an initiation signal comes in to the 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 an 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. The Safety System Monitoring Computers (SSMC) will serve the ECI system as well as

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

the shutdown systems. The unit portions of the system will be monitored by the respective unit monitoring computer; the common portion will be monitored by the Unit 0 monitor computer. Each monitor computer receives information from the field mounted devices by communication with three channelized multiplexers over fibre optic links. For a computer description refer to DM-21-66460/66560. As a design requirement, instrumentation is provided such that the operator can monitor the status of the system in all modes of operation. Indications and alarms for all essential ECI parameters are provided such that impairment or unavailability is discovered as soon as possible. In addition, a handswitch off normal alarm is provided in the Main Control Room to alert the operator that an essential handswitch is in the improper position for auto injection [8].


Section 5.5 Service Loads and Water Hammer Loads

Implementation and maintaining a pressure boundary program is a licence condition 6.1 (Pressure Boundaries) of the current Bruce Power licence [10]. As part of the licence renewal application process, a transition plan is detailed in Licence Condition 6.1 of the LCH for Bruce A [11] to comply with the version of CSA N285.0 listed in the Document Version Control table within the LCH. A transition to the 2012 version of the standard (with update 1 and 2) is currently under development and is being managed as part of Bruce Power's transition program. The LCH for Bruce A and B [10] requires pressure boundary program compliant with the 2012 version of CSA N285.0. A transition plan to the 2012 version of N285.0 standard (with update 1 and 2) is currently being managed as part of Bruce Power's transition program.

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 [5] 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 valves (PRV) manifold (section 2.0 of Containment OSRs [12]). 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-issued signal to 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 (section 4.0 of Containment OSRs [12]). During operation following a LOCA, the equipment and piping upstream of the AWT isolating valves (0-34340-MV323, MV324) will not contain potentially radioactive fluid. Leakage in this part of the subsystem will not lead to radiological consequences and it will not affect the ability of the ECIS to provide water to the HIS (provided that system parameters are maintained within limits). The piping downstream of the AWT isolating valves 0-34340-MV323, MV324 to the penetration

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

through containment to each unit becomes an extension of containment during recovery following a LOCA. The fluid being recirculated may contain radioactive fission products and for this reason, leakage must be controlled (section 4.1.6 of ECI OSRs [5]). As described in section 6.1.11 of [5], during recovery operation following a LOCA the ECI recovery system becomes an extension of containment (see also Section 4.1.6 of [5]). The fluid being recirculated could be radioactive and for these reasons, 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 valve, or some other boundary perforation. In general, small leakage does not impact on the 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.

As presented in section 6.2.5.4 of Part 2 of Safety Report [2] the ECI recovery pumps are located outside containment in an area that is considered an extension of the containment envelope. The pumps and heat exchangers associated with the ECI system are located in the ECI recovery room, which is designed as a confinement area. The high pressure ECI recovery room area is common to all four units. 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. Piping outside the containment structure has isolation valves as close as practicable to the containment. The emergency coolant injection pressure boundary is continuously checked by maintaining a positive internal pressure and detecting any leaks. Leakage from any valves is generally returned to active drainage rather than into the loop itself.

Section 5.7 Chemistry, Water Quality, and Inventory Management

Bruce A 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. As specified in the ECI Operating Manual [7], hydrazine is added to Common Supply Header and LPECI Header as required to minimize the corrosion of the carbon steel components. The addition of hydrazine maintains a low oxygen environment, maintains an alkaline system pH and protects against microbiologically influenced corrosion and inhibits zebra mussel growth. LiOH can be added to the ECI loops if pH cannot be maintained using hydrazine alone. (LiOH is not added to the LPECI loop or the ESS.) For aluminum components (i.e., the Grade Level Storage Tank) out of specification chloride and pH levels can be returned to normal by using a temporary ion exchange facility. The chemistry limits applicable to the Emergency Coolant Injection and the Emergency Storage System as well as chemistry control action procedures are specified in the Chemistry Control Procedure [13]. The chemistry control specifications are based on the difference of system construction material. The control parameters, minimum sampling

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

frequency, specification and action levels are presented in the Chemistry Specification Emergency Coolant Injection System [14]. The normal operating specifications are independent of Unit status and always apply. The only time those specification are not applicable is when the systems are drained or as specified (e.g., vacuum building outage to allow safe entry of personnel into the building and ESS tank). The objective of chemistry control for the aluminum Grade Level Water Storage Tank (GLWST) in the ECI system is to inhibit corrosion of the tank. In addition the chemistry of the GLWST is controlled to minimize the potential for aluminum hydroxide production and potential plugging of ECI strainers during post-LOCA recirculation.

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. Individual 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 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 twice yearly, during the spawning season, when the presence of zebra mussels has been 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 Safety Report, water for all purposes is drawn from Lake Huron through a tunnel and open intake channel that is common to all four units and through individual pump houses to each unit. Screens are provided at pump intakes to remove debris.

Section 5.8 Reactor Coolant System Depressurization

Once the ECI system has been initiated, the automatic instrumentation opens the Boiler Safety Relief Valves (BSRVs), which are part of the Main Steam Supply System (MSSS), to rapidly cool the boilers in the accident unit. The only credited automatic instrumentation function associated with the MSSS is the initiation of boiler crash cooling by opening the BSRVs, which facilitates emergency coolant injection (ECI) following a LOCA. Since the crash cool signal is generated by ECIS instrumentation, the associated design requirements are addressed in the ECIS OSR. The BSRVs facilitate ECI system injection, both by ensuring the initiation signal is registered, and by depressurizing the HTS to increase the injection rate [15]. Automatic crash cooling of boilers using ten out of twenty-four instrumented safety relief valves with 80% designed capacity is credited in the reference analyses in Part 3 of Safety Report. The manual crash cooldown is a part of manual initiation of the emergency injection, which is credited for very small breaks. Following reactor trip, the safety relief valves are opened manually for small breaks in order to provide timely injection and a long-term heat sink as described in the ECI OSR.

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

It is a design requirement that annunciation be provided to indicate when the ECI system has been blocked to allow depressurization of the primary heat transport system or for any other purpose [1].

Section 5.9 Heat Sink for Small Breaks

The analyses presented in Appendix 4 of Part 3 [3] of Safety Report demonstrate that, for all small LOCAs the ECI system, in conjunction with other operating process systems, is capable of refilling the HT system without a large transient reduction of coolant inventory. This, along with the availability of forced or effective natural circulation, prevents failure of the fuel, the fuel sheath or the pressure tubes (PTs), with the possible exception of individual channels directly affected by single channel events. Following a postulated small LOCA, the HT system depressurizes at a rate determined by the extent to which the coolant discharge rate exceeds the rate of D₂O makeup. In response to the decreasing pressurizer level, coolant makeup is provided automatically by the D₂O feed system. Breaks occurring at the top of the pressurizer lead to a level increase and are addressed in Appendix 4, Section 4.3. For very small breaks (with a discharge rate of less than about 40 kg/s) the coolant makeup is sufficient to prevent a decrease in the inventory of the HT system. In this event, fuel cooling is not impaired and the reactor can be shut down in an orderly fashion without requiring automatic intervention of the special safety systems.

For larger LOCAs the automatic reduction in power is provided by the reactor shutdown systems. The reactor power reduction results in a rapid decrease in the rate of heat addition to the coolant, which acts to accelerate the depressurization of the HT system. Further depressurization is assisted by the boiler crash cooldown function, which is initiated when the HT pressure falls below 5.6 MPa(a), and at least one of the LOCA conditioning signals (e.g., reactor vault high pressure, MHL or sustained HTLP) is received. At the same time, ECI is automatically initiated.

Other ECI system impairment scenarios considered in Appendix 4 of Part 3 of the Safety Report include a range of small LOCAs coincident with one of the following events: loss of unit Class IV power, loss of ECI, loss of ECI recovery, failure of boiler crash cooldown and loss of the ECI conditioning signal resulting in simultaneous loss of injection and boiler crash cooldown. The analysis demonstrates that fuel channel integrity is maintained for all of these cases and that the radiation dose to the public remains below the relevant limits.

Section 5.10 Loop Isolation

The Bruce A 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 6-3 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 A 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

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

purity). The injection of light water emergency coolant acts as a strong absorber and adds sufficient negative reactivity that shutdown system depth is not an issue.

Detailed assessments are performed to demonstrate sufficient subcriticality margin following a PT/CT failure (Section 4.5.4.3 of Part 3 of Safety Report [3]). The assessments are performed for the maximum size in-core break of 225 kg/s only. This represents the limiting case for subcriticality as it has the largest rate and magnitude of mass and energy discharge into the moderator. In cases where ECI is available following a reactor trip, the injection of light water will ensure sufficient subcriticality margin is maintained throughout the entire transient and therefore such cases are of no safety concern.

Section 5.12 Venting and Draining

In general, Bruce A 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 requirement 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 a gap (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. 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 test. Furthermore, conditioning logic is provided for opening the emergency storage tank isolation valves (3434-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

During recovery operation following a LOCA the ECI recovery system becomes an extension of containment. The fluid being recirculated could be radioactive and for these reasons, leakage from the system is controlled. Leakage may be due to a valve being left open or passing, from packing or seals of pumps and valve, or some other boundary perforation. In general, small leakage does not impact on the 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 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 operability of this subsystem is defined by mechanical hardware characteristics only (e.g., valve positions). Leakage from portions of the system not serviced by the Leakage Mitigation Subsystem (i.e., outside the ECIS recovery equipment room) is addressed in the ECI OSR [5]. The Leakage Mitigation Subsystem interfaces with Containment, whose operability requirements are addressed in the Containment

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

System OSRs [12]. The Leakage Mitigation Subsystem is part of the active drainage and interfaces with the Active Liquid Waste Handling System during normal operation.

Triplicated recovery sump level measurements are described in the ECI Instrumentation and Control Design Manual [8].

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 [16]. The ECI components located within containment are LOCA qualified in accordance with DG-29-03650-3 [8]. The components of the recovery circuit located outside containment are also qualified to withstand the radiation dose expected after a LOCA. The components outside of containment that are required to be functional following a Main Steam Line Break (MSLB) are qualified for the MSLB environment. The power supply to these components is backed-up by the Qualified Power Supply (QPS) [8]. As discussed in the ECI OSR, the ECI was not originally designed to mitigate seismic events at Bruce A; however it has been credited in the seismic margin assessment performed as part of Unit 3 and 4 restart.

Section 5.14 Debris Interceptors

Section 5.14 presents the specific design requirements for debris interception, which are applicable to new build reactors. For existing reactors the debris interceptors should meet the minimum allowable performance requirements.

Modifications have been made to the sump strainers to ensure that there is no potential blockage that could affect the ECIS recovery function. In particular, improvements to the effectiveness of the ECIS strainers were added as a condition to the Bruce NGSA PROL 15.00/2004 for Units 3&4 restart. The work consisted of: (1) installing an improved strainer to capture debris that might be generated as a result of a LOCA; (2) replacing the calcium silicate insulation in the vaults with fibreglass; and (3) revising the strainer and sump area to increase the surface area and reduce pressure drop to the ECI pumps for debris generated after a LOCA. The completion of this work is documented in [17].

References:

- [1] NK21-DM-34330/34340-R002, Emergency Coolant Injection System Process Design and Operation, November 1995.
- [2] NK21-SR-01320-00002-R005, Bruce A 2012 Safety Report – Part 2: Plant Components and Systems, Bruce Power, February 2013.
- [3] NK21-SR-01320-00003-R004, Bruce A 2012 Safety Report, Part 3: Accident Analysis, Bruce Power, January 3, 2012.
- [4] BP-PROC-00169-R002, Safety Related System List, Bruce Power, September 28, 2007.
- [5] NK21-OSR-34340-00003-R002, Operational Safety Requirements for Bruce A Emergency Coolant Injection System, May 2013
- [6] NK21-OM-03672, Safety Related System Impairments Manual.
- [7] BP-OPP-00001-R015, Operating Policies and Principles-Bruce B, Bruce Power, October 8, 2013.


 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- [8] NK21-DM-63433/63434-R006, Emergency Coolant Injection System Instrumentation and Control, Units 1-4, April 21, 2005.
- [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-00531-11391, Bruce Nuclear Generating Station A Nuclear Power Reactor Operating Licence: Licence Conditions Handbook (LCH-BNGSA-R8), June 4, 2014.
- [11] NK21-CORR-00531-11272, Nuclear Power Reactor Operating Licence, Bruce Nuclear Generating Station A (PROL 15.00/2015), May 1, 2014.
- [12] NK21-OSR-34200-00004-R001, Operational Safety Requirements for Bruce A Containment System, December 21, 2007.
- [13] NK21-CCP-34340-00001, Emergency Coolant Injection, July 14, 2014.
- [14] B-CYS-34340-00001-R005, Chemistry Specification Emergency Coolant Injection System, November 2, 2010.
- [15] NK21-OSR-36100-00001-R000, Operational Safety Requirements for Bruce A Main Steam Supply System, September 12, 2008.
- [16] NK21-EQR-03651-00001-R003, EQ Requirements of Safety Related Systems and Structures for the Bruce A Nuclear Generating Station, June 2006.
- [17] NK21-CORR-00531-02391, Completion of CNSC Prerequisites for Return to Service for Bruce Unit 3, Bruce Power Letter, F. Saunders to M.P. Burton, December 4, 2003.
- [18] NK21-OM-34340, Emergency Coolant Injection Supply, Operating Manual.

A.12. CSA N290.3-11, Requirements for the containment system of nuclear plants

This is a new standard that presents the requirements for the design, qualification, installation, operation, maintenance, inspection, and documentation of a containment system. A high level of Bruce A 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 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 A, 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.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 6.2 of Part 2 of Safety Report [1], containment is a special safety system that 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 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.

The station containment envelope includes the four reactor vaults, the central fuelling area in the service building, the fuelling duct (which runs beneath and interconnects these areas), the east service area, the two pressure relief ducts, the pressure relief valve manifold, and the vacuum building. Cooling and service water are supplied from Lake Huron through an intake tunnel which extends into the lake. The details of water intake and discharge arrangements are described in section 3.7.1 of Part 2 of Safety Report [1].

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 Safety Report [3].

With regard to severe accidents, it is recognized that originally Bruce A was not designed to cope with these, other than the dual failure LOCA plus 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 [5].

Section 5 presents the general requirements and containment design features. Containment design features meet the requirements in this clause as described in the General Requirements and Overview Design Manual [10]. Specific design details are presented in the Negative Pressure Containment Design Manual Package; i.e., parts 2 to 12.

Operation of the containment pressure suppression system is automatic. The pressure relief valves are actuated by a rise in pressure in the pressure relief duct, and the dousing spray

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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.

Containment isolation is initiated upon the detection of high activity or high pressure in containment. There are four pressure measurements in the pressure relief valves (PRV) manifold, and sixteen activity measurements distributed throughout containment. There are two activity measurements in each Vault Vapour Recovery System (VVRS), two in each half (north and south) of the central fuelling area, 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. Containment is a two-channel (Channel N and P) special safety system, so there are two pressure measurements and eight activity measurements per channel. One of the high pressure or activity signals in either channel will initiate containment isolation [2].

Two separate systems are provided for mitigation of hydrogen following the design basis event combinations. Hydrogen Ignition System [6] is for mitigation of short term hydrogen generation and Passive Autolytic Recombiners (PARs) is provided for slower longer term hydrogen generation such as from radiolysis of water.

As stated in section 1.5.3 of Part 3 of Safety Analysis [3], timely activation of containment isolation is demonstrated by comparing conservatively calculated doses to Siting Guide dose limits. A derived acceptance criterion is not applied, since showing that the dose limits are met is the primary objective of the accident analyses. The Bruce A Safety Report Part 3 [3] states that “containment structural integrity for design basis accidents is assessed (Section 5.6.4.1) for peak overpressure due to ... pressure loading due to hydrogen deflagration. ... Since the containment structure (with the exception of the vacuum building) is pressure tested to a higher level, it is concluded that the containment structural integrity is maintained...”

The 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 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. The Bruce A 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. 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.

Although not specifically part of the containment system, the Emergency Coolant Injection System (ECIS) forms an extension of the containment boundary once activated. The operation of the ECIS can also have a direct bearing on containment integrity during a BDDBA. Early injection of water to the Heat Transport System or to the moderator systems provides several hours of heat removal capacity allowing alternate actions to be taken to prevent containment

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

failure. Establishing ECI recovery provides heat removal from containment which can be used to control containment pressure and water level [7].

Bruce A 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 [7]. Additional evaluations of alternative CFVS are targeted for completion by Q4 2016. It is noted that the consequences of severe accidents are mitigated by SAMG; however the current design documentation does not explicitly consider the load conditions during severe accidents. This is already assessed as a gap under SF1-11 in Table 8.

Section 6 describes the general design principles of a containment system. The containment system at Bruce A was originally designed for single unit design basis accidents which also included serious process failures that would be classified as BDBAs today. The original design was not intended to provide protection for all BDBAs, particularly those involving multi-unit events. Nevertheless, when supplemented by additional safety features, the existing containment envelope and systems will provide substantial benefit in mitigating the consequences of such events [7].

Loads and loading combinations, considered for the design of the containment structures are summarized in section 2.3.2 of Part 2 of the Safety Report [1]. The design weather data selected for Bruce A site are presented in Table 2-1, Part 2 of the Safety Report. The protection against common mode incidents is summarized in section 2.5, Part 2 of Safety Report. A detailed assessment of the probability and consequences of an aircraft crash at Bruce A concluded that there is not significant risk to the public due to potential aircraft crashes [8]. The containment performance assessment is presented in Appendix 5.6 of Part 3 of Safety Report [3].

The selection of materials used inside containment considers post-accident conditions. As part of the 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 concern that post LOCA fibres from calcium silicate insulation covering on many systems (pressurizer, bleed condenser, etc.) plug the ECI recovery strainer was addressed on Bruce A restart by replacing the strainer with a larger area device. The calcium silicate insulation was removed on Units 3&4 and on Units 1&2 prior to restart.

The carbon steel liner of the Bruce A containment is coated with inorganic zinc primer. This type of paint can remove 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

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

based paints were shown in integral tests to adsorb a large fraction (70 percent or more) of the total iodine [8].

Section 7 discusses the leakage criteria applicable to containment boundary. As described in section 6.2 of Part 2 of 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. Leakages which occur within the containment structure initially increase the humidity of the atmosphere within the building and this result in an increased rate of collection of condensate by the vapour recovery system. Such leakage also increases the local concentrations of tritium. If these leakages are sufficiently large to create liquid water, its presence is indicated by moisture detecting elements (beetles) installed in the containment structure.

The design target leakage rate for the containment boundary, except for the vacuum building, was set at 1% of the total contained mass per hour at 68.9 kPa(g) (10 psig) for the reactor vaults and fuelling duct/fuelling machine rooms; and, 62 kPa(g) (9 psig) for the pressure relief duct and pressure relief manifolds. However, safety analysis is performed assuming a higher limit in order to assure margins. The operational target leak rate for the main volume of the vacuum building is 47 L/s (100 scfm) at 7 kPa(a) (1 psia) and for the upper chamber it is 1.4 L/s (3 scfm).

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 [9]. Design details and are provided in the Design Manual Containment Leakage Rate Measurement System [9].

The maximum allowable leakage rate is based on the analyses documented in Part 3 of Safety Report [3] (section 5.6.4). The safety limits related to leakage are presented in Containment OSRs [2]. The design leakage rates are presented in the Design Manual Negative Pressure Containment System Part 1 [10].

The licence limits for Negative Pressure Containment System are presented in Appendix A, A21 of Bruce A OP&P [11]. The containment leak rate must be $\leq 2\%$ of the total contained mass per hour at the design pressure of 68.9 kPa(g).

Bruce Power Nuclear Emergency Response Plan (NERP) [12] 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 of 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 assistance. Since beyond design basis event response is not addressed in BP-PLAN-00001 [12], for those events where accident consequences indicate that the design basis response has not been effective, the ERO will activate Severe Accident Management Procedure [13]. The Severe Accident Management Procedure [13] is implemented by station specific SAMG

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

documentation. The Bruce A specific Severe Accident Guides applicable to containment are listed in section 5.3 of [13].

Section 8 describes the requirements related to identification and location of containment penetrations and the associated extensions of the containment boundary. Bruce NGSA Penetrations and Extensions of the Containment Envelope, Report No. 90232 contains a list of penetrations and extensions of the containment envelope at Bruce A. The information on the list identifies systems and lines passing through containment penetrations and is intended to provide the appropriate information on the containment penetrations for purposes of periodic inspection of the containment envelope with the exception of the concrete containment boundary. The list is developed to satisfy the operational requirement that all valves and dampers which are part of the containment envelope carry identification relative to their containment function and operational conditions. In addition, all containment penetrations and associated extensions should be clearly marked on all flowsheets.

The list provides the following information for each system penetrating the containment structure:

- Line designation (including diameter) of each line penetrating the containment structure
- Normal containment boundary provided for each extension of the containment envelope (including dampers, valves and line designations forming the extension)
- For the portion of the system forming the normal containment boundary
 - Code Classification
 - Operational State
- First point of isolation if the normal containment boundary is lost
- Normal operating and design pressures and temperatures for each line as provided on the design flowsheets

Section 9 describes the design requirements for containment subsystems such as containment structure, barrier 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.

Under licence conditions 6.1 and 6.2 [14][15], Bruce Power is required to implement and maintain a pressure boundary program and have in place a formal agreement with an Authorized Inspection Agency. The 2008 edition of this standard is referred to in section 2 of N290.3 standard, whereas 2012 edition including Update No. 1 (September 2013) and Update No. 2 (November 2014) are listed in the PROL [16]. As part of the licence renewal application process, a transition plan is detailed in Licence Condition 6.1 of the LCH for Bruce A to comply with the version of CSA N285.0 listed in the Document Version Control table within the LCH. N287 series (287.1 to 287.6) cover concrete containment structures requirements and are referred to for additional recommendations and guidance under licence condition 5.1 Design Program. N287.7 edition 2008, describes the requirements for in-service examination and testing requirements for concrete containment structures. The standard is included in LCH for recommendations and guidance for licence condition 6.1 Fitness for Service Program.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Section 9.2 Barriers for Containment Penetrations: Bruce A design meets the intent of the requirements in this clause. The containment penetrations are described in section 6.2.2.7 of Part 2 of the Safety Report [1]. Allowable leakage through penetrations is specified in the Design Manual [10].

Bruce A was not designed for leak testing capability of resilient seals at the containment design pressure. 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 items to be checked [8].

As documented in Appendix L (Safety Factor on Plant Design) of Enclosure 1 of [17] the Bruce A vacuum type containment 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 6.2.4 of the Safety Report [1] as well as periodic inspections performed in accordance with CSA N285.5 and N287.7. 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.

The design requirements for the airlocks and transfer chambers are specified in the Part 7 of the Containment Design Manual [18]. The airlocks and transfer chambers are designed with a door at each end and it is possible to open one door only when the other door is closed.

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 (OSR) for the Bruce A Containment System [2] describes the containment envelope and presents the safety limits and surveillance requirements for the systems and its components. Airlocks and Transfer Chambers can be tested individually in accordance with the OSR for the Bruce A Containment System [2] Table 3.3-1. It is impractical to measure the leakage through the individual doors, so the approach taken is to pressurize the inter-space and measure the pressure decay. The result is the sum of the leakage past both doors, which bounds the leakage past either door. Assigning all of the leakage to one door and assuming the other is open at the time of the accident is conservative and consistent with the reliability requirement that either door is able to provide a sufficiently leak tight barrier (section 3.3.3 of [2]). 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 6.2.2.7 of the Safety Report [1] 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.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Bruce NGS A CSA N287.7-08 Periodic Inspection Program for Bruce NGS A Concrete Containment Structures and Appurtenances (Excluding Vacuum Building) [19] 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 Frequency.

As documented in [17] Bruce A has piping systems penetrating containment that do not have redundant isolation valves. In the 1990s, a report was prepared on containment extensions at Bruce A [20]. 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.

The benefit of double isolation valves for the MCS was assessed for Bruce 1&2 [21] . The assessment concluded that it is not practicable to make the change.

Many of the systems that connect to the PHT and penetrate containment have two isolation valves, but not all of them. One area where Bruce A does not comply with this requirement is for reactor cooling systems that penetrate containment. The maintenance cooling system has four isolation valves, one in each line, penetrating containment, inside the containment wall. The ECI system contains dual isolation valves (inside containment) in the unit portion of the system that penetrates the reactor vault.

Piping and valves that form part of extensions of the containment boundary and associated penetrations including airlocks and transfer chambers are inspected in accordance with CSA N285.5 as required in the PROL to assure their continued structural integrity.

As presented in [8] in 1990 a report was prepared on containment extensions at Bruce A. This review covers all types of containment extensions, be they attached to the PHT or just to the containment atmosphere. Thus, while all of the systems at Bruce A were not specifically designed with this requirement in mind, the report has clearly identified where the second isolation point is for each extension, and thus the intent of the requirement for dual isolation has been met. This issue is discussed more fully in the comparison of Bruce A against the Darlington Design Guides, which was issued for the Bruce A Units 1&2 restart.

Section 9.3 Energy Management Systems: (i.e. 12 main pressure relief valves, four auxiliary and four instrumented pressure relief valves, vacuum building dousing system, vacuum system, vault coolers) are described in Part 2 of Safety Report and the Design Manuals and section 5.0 of Containment OSRs. The associated safety analyses are summarized in the OSRs. Containment atmosphere pressure and temperature is continuously monitored in the MCR. 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 initiates this containment isolation.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Heat removal from containment is provided by an air-to-water cooling system. 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.

In order to minimize potential damage to the containment boundary two separate systems are provided for mitigation of hydrogen following the low probability design basis event combinations.

- (a) Hydrogen Ignition System for mitigation of short term hydrogen generation, and
- (b) Passive Autocatalytic Recombiner (PAR) for slower longer term hydrogen generation such as from radiolysis of water.

See 9.5 below for further details.

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 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 [22] provides additional details.

Section 9.5 Combustible gas management: As described in section 6.2.2.10 of Part 2 of Safety Report, 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. The system is inactive during normal operation and the igniters are energized by the containment isolation signal. The igniters are powered from the Class II distribution system while the instrumentation and control for the igniters is powered from Class I. At Bruce B, the igniters and instrumentation are backed up by EPS. There is no qualified power supply to the igniters at Bruce A [7].

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. PAR is a completely passive device and does not require any services or supplies. A PAR unit will automatically activate on presence of hydrogen above the lower threshold concentration and initiate recombination to produce steam. In addition PAR will also provide short term hydrogen mitigation while the hydrogen ignition system is active.

Based on the conclusion that the hydrogen ignition function is only required for low probability dual failure events, an agreement was reached with the CNSC that it should be considered a safety support system rather than an integral part of containment (e.g., not included in the containment unavailability model). The most current analysis of hydrogen behaviour in containment demonstrates that the combination of hydrogen igniters in the short term, and passive auto-catalytic recombiners and venting via EFADS in the longer term are effective in mitigating any concerns related to potential hydrogen ignition post-LOCA [2].

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

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

implementation of Severe Accident Management Guidelines where computational aid will be used to determine hydrogen concentration based on an estimated percentage of core Zirconium oxidation [23].

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 [7]. 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 performed assessment of site-specific external hazards. The assessment of Review Level Condition (RLC) 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 (**Gap**) in SF1-3.

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-10017 [24].

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. As described in the EFADS Design Manual, the filter system is installed in shielded rooms. All instruments, with the exception of the primary elements, are located outside shielded rooms. All valves associated with the filters are located outside the shielded filter rooms where possible. There are still locations within the plant which have high fields associated with the LOCA, for example in the vicinity of the VVRS, where post LOCA actions may have to be completed in a short period. These areas have been identified in the AIM for the operators. At the time of the original design all systems considered to have significant radiological implications for station personnel during maintenance or operation were reviewed in the design phase. The review process included a series of Man Rem Audit meetings on a system-by-system basis, and AECL design, operations, health physics, and physics and analysis groups were represented. Each system design was examined with respect to reliability, maintainability, simplicity, 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. Proposals to reduce radiation exposure by improving system design were analyzed and, wherever feasible, implemented.

The EFADS filter units are provided with shielding suitable for the activity levels present as per Design Manual Emergency Filtered Air Discharge System [22].

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

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

system and other sources. As described in the Containment OSRs, this "compressed gas ingress" is removed by venting a portion of the containment atmosphere through the 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 analysis assumes a compressed air ingress rate in the long term (once unnecessary sources of instrument air have been isolated) of 400 kg/hr (Appendix 5, section 5.6.3.1.4, Part 3 of Safety Report). Sensitivity analysis of the re-pressurization time is available for gas in-flows up to 600 kg/hr.

The accident consequences are affected by the post-accident air-ingress rate. Following a LOCA, operators will isolate all unnecessary sources of compressed air into containment (e.g., Section 4.3.4.1, Abnormal Incidents Manual, [25]), so the rate during normal operation is irrelevant as specified in the Containment OSRs [2]. Furthermore, the only impact is on re-pressurization time, for which there is no specific limit (Section 1.4.3). As such, no Safety Analysis Limit for compressed gas ingress is specified [2]. According to [17] 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) [25] 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.

Isolation of unnecessary instrument air is dealt with procedurally. The Abnormal Incidents Manual [25] 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.

Section 13 Operational requirements: discusses the operational requirements related to containment atmosphere. Bruce A meets the operational requirements to maintain the containment atmosphere at sub-atmospheric pressure in normal operation to minimize uncontrolled leakages to the environment. The design and test pressures for the containment envelope are specified in the section 6.2.2.1 of Part 2 of Safety Report [1].

Section 21.1 of Bruce Power A OP&P [11] presents the operating conditions or restrictions related to the operation and maintenance of the Negative Pressure Containment System containment system.

Section 14 Maintenance of isolation barriers: describes the requirements applicable to maintenance of isolation barriers. Clause 14.1 requires that when maintenance is performed on a penetration, a single closed isolation barrier shall be demonstrated to be available. The requirement that this barrier should not rely on air or power to maintain its position is not considered in the design documentation. Therefore, it is assessed as a gap (**Gap**) in SF1-5.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Bruce A OP&P, section 21.4 [11] specifies the maintenance requirements as follows: “When performing maintenance on any component or channel of the Negative Pressure Containment System, the component or channel shall be put in a safe state, where such a state exists, repaired, tested, and returned to service. Where redundant components or channels exist, this method shall be used on one component or channel prior to working on another. Senior Operations Authority approval is required for any alternative method.

“All work performed on the Negative Pressure Containment System shall have the prior authorization of the Control Room Shift Supervisor.”

As documented in [17] Bruce A has piping systems penetrating containment that do not have redundant isolation valves. In the 1990s, a report was prepared on containment extensions at Bruce A [20]. 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.

References:

- [1] NK21-SR-01320-00002-R005, Bruce A 2012 Safety Report – Part 2: Plant Components and Systems, Bruce Power, February 2013.
- [2] NK21-OSR-34200-00004-R001, Operational Safety Requirements for Bruce A Containment System, December 21, 2007.
- [3] NK21-SR-01320-00003-R004, Bruce A 2012 Safety Report, Part 3: Accident Analysis, Bruce Power, January 3, 2012.
- [4] NK21-CORR-00531-12209, 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] NK21-CORR-00531-12209, 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] NK21-62111-R000, Hydrogen Ignition System Design Manual.
- [7] NK21-CORR-00531-11801, Bruce Power Progress Report No. 6 on CNSC Action Plan – Fukushima Action Items, Bruce Power Letter, F. Sanders to K. Lafrenière, January 30, 2015.
- [8] RABA 0804 Review of Bruce NGSA Against Modern Safety Standards Draft Regulatory Document RD-337 Design of New Nuclear Power Plants, October 16, 2008.
- [9] NK21-DM-34270, Containment Leakage Rate Measurement System Design Manual, November 1990
- [10] NK21-DM-34200.1, Negative Pressure Containment System, Part 1, General Requirements and Overview, February 1976.
- [11] BP-OPP-00002-R013, Operating Policies and Principles-Bruce A, Bruce Power, March 31, 2014.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


- [12] BP-PLAN-00001-R004, Bruce Power Nuclear Emergency Plan, April 24, 2014.
- [13] BP-PROC-00659-R002, Severe Accident Management, February 3, 2014.
- [14] NK21-CORR-00531-11272, Nuclear Power Reactor Operating Licence, Bruce Nuclear Generating Station A (PROL 15.00/2015), May 1, 2014.
- [15] NK21-CORR-00531-11391, Bruce Nuclear Generating Station A Nuclear Power Reactor Operating Licence: Licence Conditions Handbook (LCH-BNGSA-R8), June 4, 2014.
- [16] NK21-CORR-00531-12136, Nuclear Power Reactor Operating Licence, Bruce Nuclear Generating Station A and B (PROL 1.00/2020), May 1, 2015.
- [17] NK21-CORR-00531-11005/NK29-CORR-00531-11397, Submission of Safety Basis Report, Bruce Power Letter, F. Saunders to R. Lojk, December 30, 2013.
- [18] NK21-DM-34200.7, Negative Pressure Containment System Part 7: Airlocks, Transfer Chambers and Confinement Bulkheads (including monitoring), October 1974
- [19] NK21-PIP-21100-00001-R003, CSA N287.7-08 Periodic Inspection Program for Bruce NGS A Concrete Containment Structures and Appurtenances (Excluding Vacuum Building), October 2014
- [20] Bruce NGS A Penetrations and Extensions of the Containment Envelope, Report No. 90232.
- [21] NK21-CORR-00531-04342, Bruce A Units 1 and 2 Return to Service – Single Failure Review and Cost-Benefit Analyses, Bruce Power Letter, F. Saunders to P. Webster, July 31, 2006.
- [22] NK21-DM-34310-R002, Emergency Filtered Air Discharge Systems (EFADS), June 1987.
- [23] BP-SAM-00001-R000, Technical Support Group User's Guide, October 15, 2009
- [24] BP-SAM-10017-R001, Bruce A – SAM Parameters and Setpoints, April 14, 2010.
- [25] NK21-OM-09034-R113 Bruce Nuclear Generating Station A Abnormal Incidents Manual, April 15, 2014.

A.13. CSA N290.11-13, Requirements for reactor heat removal capability during outage of nuclear power plants

This is a new standard 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.

As described in section 5.1.1.3 of Part 2 [1] of Safety Report, decay heat is removed in a staged manner during a reactor outage.

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

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 is designed to cool the HT system from 177°C (350°F) to 54°C (130°F) and to hold it at the latter temperature for an indefinite time. The system utilizes the preheaters and main HT pumps to transfer heat from the HT system coolant to a demineralized water recirculation loop.

Maintenance of some components (steam generators, pumps, valves) requires that the HT system be depressurized and drained to the header level. Cooling during this mode of operation is provided by the maintenance cooling system, which is connected to the inlet and outlet headers. The maintenance cooling system is normally used for completion of cooldown to less than 35°C after the shutdown cooling system has reduced the HT system temperature to 54°C (130°F) and could be used to cool down the HT system from 160°C (326°F) in the event the shutdown cooling system is unavailable.

A general requirement is to have at least two heat sinks available that are capable of removing the decay heat under a range of shutdown conditions. For failures involving electrical supply failure, backup cooling systems and pumps are provided that are powered by on-site emergency power sources. Two systems are provided by design for removing the decay heat after reactor shutdown, i.e., the Shutdown Cooling System and the Maintenance Cooling System. The Maintenance Cooling System (MCS) is considered a directly cooled system (the heat transport (HT) D₂O is cooled directly by service water), whereas the initial heat exchange is from the HT D₂O to boiler feedwater for the Shutdown Cooling System (SDCS) [2]. The design requirements, systems descriptions, system failures and reliability considerations are provided in the design manuals for Shutdown Cooling System [3] and Maintenance Cooling System [4].

The Shutdown and Maintenance Cooling Systems Operational Safety Requirements document [5] specifies the operability of the mechanical hardware and instrumentation required to perform the safety-related functions and manual operation of both systems. There is no automatic instrumentation required for either system. Both systems are classified as a group D safety-related systems; however since the Maintenance Cooling System protects and supports other safety-related system (i.e., maintains HTS integrity and maintains containment boundary) it also has group E classification as per Safety Related System List [6]. Procedure BP-PROC-00169 [6] 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.

The safety-related functions performed by the Shutdown Cooling System (SDCS) are to:


- Serve as a normal shutdown heat sink over a HTS temperature range of 170°C to 55°C;
- Serve as an emergency shutdown heat sink for HTS temperature up to 256°C;
- Maintain a pressure boundary between the Feedwater System and the SDCS when not in service;

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

- Provide emergency isolation of the Feedwater System following a break in the SDCS when in service.

The Shutdown Cooling System (SDC) requires the Heat Transport System and at least the Auxiliary Condensate and Feedwater Systems to be in service to operate. It reduces Heat Transport temperature to below the level that the Main Steam/Reject Systems are required. The Shutdown Cooling System is designed to withstand full boiler feedwater pressure. During normal operation, the SDC System is poised and isolated from the boiler feedwater system. It is normally placed in service after the heat transport system is cooled from zero power hot to 165°C. This system is also capable to be used as an emergency cool down system to lower the HT temperature from 256°C in the event when ASDVs/CSDVs are not available. The Shutdown Cooling System is not a nuclear system. Since all components and instrumentation of this system are outside containment, it is classified as a non-nuclear system and designed according to the requirements of the power piping code USAS B31.1. The Shutdown Cooling System is not credited for any design basis accidents when it is exposed to harsh environment. None of the Shutdown Cooling System components/equipment is on the EQ List and there is no issued EQ Dossier for this system. The shutdown cooling exchangers (3-4-34710-HX1, HX2) and steam drum isolation valves (3-4-34710-MV26, MV27) are listed on the Safe Shutdown Equipment List (SSEL) and are seismically qualified per [2]. The SDC System can be used to act as an alternate heat sink to cool the HTS from an elevated temperature (up to Zero Power Hot 256°C if CSDVs are unavailable) to 65°C in the event of a preheater or boiler tube rupture, as directed via the Abnormal Incidents Manual [7], Section 4.3.6.1. Excessive thermal stressing in the SDC System components would require Station Engineering to evaluate the need for subsequent inspection following such an incident [8]. The Shutdown Cooling System is designed and constructed to the same non-nuclear standards as the Boiler Feedwater System. The system is subject to periodic inspections to address the risk of degradation/failure pressure boundary for the tubes of heat exchangers of shutdown cooling system. This potential pressure boundary failure could result in forced shut down for up to two weeks. This can be mitigated by conducting periodic inspections of Heat Exchangers and Vessels to confirm equipment status (inspections must be done during outages). A preventive maintenance for inspection of HX internals and perform Eddy current test has been defined and assigned to heat exchangers with a frequency of once per six years [8].

If it is required to shut down all the Main Heat Transport pumps and depressurize the main circuit, the Maintenance Cooling System (connected between the reactor outlet headers and the corresponding inlet headers of the HT system) can then be placed in service and the HTS depressurized. The major portion of the system is located outside of containment and valves inside containment provide isolation between the maintenance cooling system and the HT system during normal plant operation. As described in Section 5.1.1.3.3 of Part 2 of Safety Report [1], the Maintenance Cooling System is designed to withstand HT system temperature and pressure, and is classified as a Class I system in accordance with Section III of the ASME Code 1971 Edition with Winter Addenda. The tube side of the heat exchanger is designed and constructed to meet the requirements for Class I components in Section III of the ASME Code. The shell side is designed and constructed to meet the Tubular Exchangers Manufacturers Association (TEMA) Class C requirements. Cooling water to the heat exchanger is taken from the same low pressure service water supply which goes to the Shutdown Cooling System heat exchangers. As described in section 11.5 of Part 2 of Safety Report, the Fire Protection (Water)

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

System is connected and could be made available as a backup to the Maintenance Cooling System. The Maintenance Cooling System has no equipment on the EQ requirements list [9]. The Environmental Qualification Safety Related Component List (EQSRCL) is a list of all EQ safety-related equipment and components, including their harsh/mild indicators and evaluation for degradable materials. This list is developed and maintained by procedure SEC-EQD-00031 [10]. As a result of Bruce A Units 3 and 4 Restart Seismic Margin Assessment, the system equipment is listed on the Safe Shutdown Equipment List as per Appendix A of [2]. The MCS is subject to periodic inspection in accordance with CSA-N285.4

The MCS is a safety-related system which performs the following functions [5]:

- Serve as a normal shutdown heat sink over the full range of HTS pressures with ROH temperatures $\leq 90^{\circ}\text{C}$;
- Serve as an emergency shutdown heat sink when the HTS is pressurized, SDC is unavailable, and ROH temperatures $\leq 160^{\circ}\text{C}$;
- Maintain a leak tight boundary of the containment extension formed by the MCS when in service;
- Provide capability to restore the pressure boundary of the HTS should a MCS failure occurs while in service.

The systems associated with outage heat sinks are identified and listed in Bruce A Outage Heat Sinks Operating Manual [1]. 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 Check List is prepared and used as a reference on a loss of heat sink. As indicated in the Operating Manual, the check list is to be reviewed prior to, and then completed whenever there is a change in heat sinks or following a significant change to the heat sink line-up (e.g., during flow defueling activities at the start of an outage since outage heat sink line-up could be changing, prior to the shutdown of all four main Heat Transport (HT) pumps, prior to opening/closing boiler manways). The heat sink check sheet is surrendered when the main HT pumps are started as part of the full heatup with all heat sink-related systems in their normal OM-09110 startup state.

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 is not explicitly reflected in the operating documentation; therefore it is assessed as a gap (**Gap**) in SF1-7.

Maintenance activities are carried out according to the specific procedures. The Outage Work Management Program [11] 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 [12] 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 [11] 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

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

outage work. The Program is implemented by BP-PROC-00342 Planned Outage Management [13] and BP-PROC-00343 Forced Outage Management [14].

As presented in Shutdown and Maintenance Cooling Systems OSRs [5], following design basis accidents for which SDCS is credited, but is not available; MCS can be credited as an acceptable alternative. For this reason, the SDCS heat sink function can be considered to be a defense-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 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 call 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; 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. Since this is identified as a gap SF1-3 against clause 6.1.1 of REGDOC-2.5.2, the gap is not repeated in Table 8.

Specific changes to the Operating Manual have been introduced based on new analysis results documented in Bruce A Containment Outage Heat Sink Analysis for 4 Unit Operation at 92.5% FP [15]. The new analysis was performed to account for four units returning to operation.

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 [16]. Further series of analyses have been carried out and historical operating data analysed to refine the methodology for deriving operating restrictions during outage [17][18][19].

The MCS recall times for Bruce A for the current configuration where all four units are operating are determined and documented in [15]. The MCS restoration times are reflected in the Bruce A Heat Sink Operating Manual [20].

Fuel cooling assessment for using Mini-SLAR and MARK-III SLAR tool in conjunction with a fuelling machine has been performed to derive updated wait times for Bruce A specifically for maintenance activities on fuel channels following shutdown [21].

The Bruce A OP&P [22] requires a method of transporting heat from the fuel to a heat sink to be always in service. In addition, “there shall always be available an alternative method of cooling the core unless the reactor unit is in the defueled guaranteed shutdown state”. Backup and emergency heat sinks fulfill this requirement. As summarized in [23] during outage, HT pumps on Low Speed Drive (LSD) and Intermittent Buoyancy Induced Flow (IBIF) are credited as

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

backup heat sink with or without SDC in service. During transition, MCS is credited as backup sink. The credited heat sinks as identified in [16] are listed below:

Transition to Outage:

Primary: PHT pump full speed to Boilers

Backup: MCS

Emergency: Thermosyphoning

During Outage:

Primary: MCS

HT closed and full:	Backup: Low Speed Drive (LSD)
Boilers	Emergency: Intermittent Buoyancy Induced Flow (IBIF) to

HT closed and drained:	Backup: LSD
	Emergency: IBIF to Boilers

HT open and drained:	Backup: IBIF to Vault + D2O Inventory
	Emergency: IBIF to Vault + ECI/EWS


Part 3 of Safety Report, sections 3.3.4 and 3.3.5 present a summary of Shutdown Cooling System failures and Maintenance Cooling System 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 Shutdown Cooling and Maintenance Cooling System Failures [24].

References:

- [1] NK21-SR-01320-00002-R005, Bruce A 2012 Safety Report, Part 2: Plant Components and Systems, February 2013.
- [2] NK21-CALC-20091-00002-R06, Bruce NGS A Seismic Assessment Seismic Success Path and Equipment List, Bruce Power, March 18, 2011.
- [3] NK21-DM-34710, Bruce Generating Station, Shutdown Cooling System Design Manual, January 1975.
- [4] NK21-DM-34720, Bruce A Units 1-4, Maintenance Cooling System Design Manual, May 1991.
- [5] NK21-OSR-34700-00001-R001, Operational Safety Requirements for Bruce A Shutdown and Maintenance Cooling Systems, September 2008.
- [6] BP-PROC-00169-R002, Safety Related System List, September 28, 2007.

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


- [7] NK21-OM-09034-R113, Bruce Nuclear Generating Station A Abnormal Accident Manual, R113, April 15, 2014.
- [8] NK21-CAR-34710-00001-R001, Condition Assessment Report Shutdown Cooling System, March 24, 2011.
- [9] NK21-CAR-34720-00001-R001, Condition Assessment Report, Maintenance Cooling System, March 29, 2011.
- [10] SEC-EQD-00031-R002, Preparation of Environmental Qualification Dossiers (EQD), Bruce Power Procedure, June 27, 2011.
- [11] BP-PROG-11.03-R005, Outage Work Management, July 26, 2011.
- [12] BP-PROG-11.02-R006, On-Line Work Management Program, October 23, 2012.
- [13] BP-PROC-00342-R005, Planned Outage Management, June 28, 2013.
- [14] BP-PROC-00343-R005, Forced Outage Management, July 26, 2010.
- [15] NK21-REP-03674 P NSAS, Bruce A Containment Outage Heat Sink Analysis for 4 Unit Operation with the Outage Unit at 92.5% FP, May 11, 2015.
- [16] 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.
- [17] NK29-REP-03500-00007-R000, Corporate Review of Outage Heat Sinks Decay Heat Curve Documentation and Confirmatory Analysis, June 30, 2004.
- [18] NK21-REP-03503-00001-R000, Bruce A Unit 4 Outage Heat Sink Analysis, March 24, 2005.
- [19] NK21-CALC-09320-00001-R000, Bruce A Outage Heat Sink Analysis (92.5% FP), December 15, 2005.
- [20] NK21-OM-03674, Bruce Nuclear Generating Station A Operating Manual, Outage Heat Sinks, Units 01234.
- [21] NK21-CORR-00531-08964/NK29-CORR-00531-09660, Bruce A and B: Updated Wait Times to be Adopted in Undertaking Inspection and Maintenance Activities on Fuel Channels Following Shutdown, Bruce Power Letter, F. Saunders to R. Lojk, May 22, 2012.
- [22] BP-OPP-00002-R013, Operating Policies and Principles-Bruce A, Bruce Power, March 31, 2014.
- [23] NK29-03500 LOF NSAS, Memorandum J. Stoklosa to M. Kwee, AR# 28261866: Clarification of SDC Role as Outage Heat Sink, January 13, 2012.
- [24] NK21-SR-01320-00003-R004, Bruce A 2012 Safety Report, Part 3: Accident Analysis, January 3, 2012.

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 ISR 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 ISR 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 ISR Basis Document defines RNA as "the particular clause provides requirements that are less strenuous than clauses of another standard that has already been assessed". The definition has been broadened to include 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: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

B.1. CSA N290.1-13, Requirements for the Shutdown Systems of CANDU 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 CANDU Nuclear Power Plants


Article No.	Clause Requirement	Assessment	Compliance Category
4	Requirements	This is not a requirement/guidance clause (this is a title only).	NA
4.1	Functional requirements	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 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev.5].</p>	C
4.1.2	Functional requirement to shut down the reactor	This is not a requirement/guidance clause (this is a title only).	NA

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


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> <p>1)Termination of the chain fission reaction is generally accomplished by inserting rods or liquids that absorb neutrons.</p> <p>2)In CANDU reactors, SDS is credited for overpressure protection.</p>	<p>Bruce A reactor incorporates these common CANDU design features.</p> <p>SDS1 and SDS2 can both be used to terminate reactor operation when parameters reach an unacceptable range. Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 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> <p>1)"Independence" and "diversity" are defined in CSA N290.0, Clause 3.1.</p> <p>2)For CANDU reactors, two separate, independent, and diverse shutdown systems are generally provided.</p>	<p>SDS1 and SDS2 are functionally and physically independent and employ two diverse shutdown principles. SDS1 is the primary shutdown system which releases 30-spring-assisted gravity drop shutoff rods. SDS2 uses rapid injection of concentrated gadolinium nitrate solution into the bulk moderator through seven horizontally distributed nozzles. Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 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 adequate margin on the assumption of a single failure.</p>	<p>Although AOOs are not explicitly assessed, they are covered within the single failure events where shutdown system effectiveness in rendering the reactor subcritical is demonstrated in Part 3 of the Bruce A Safety Report [NK21-SR-01320-00003 Rev.4].</p>	IC
4.1.2.2.3	<p>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>	<p>The two shutdown systems are physically separated and independent of each other. Independence is achieved by employing diverse shutdown principles (SDS1 uses solid shutoff rods, and SDS2 directly injects poison into the moderator). It permits the assumption that at least one will operate following any single process failure.</p> <p>Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev.5].</p>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


4.1.2.3	<p>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.</p> <p>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.</p>	<p>Bruce A design incorporates two shutdown systems, which are functionally and physically independent of each other and functionally independent of the reactor regulating system. In addition, credit is not taken for both shutdown systems acting together. Since the shutdown systems are independent at least one will operate following any single process system failure. Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev.5] presents more details.</p>	C
4.1.3	<p>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.</p> <p>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.</p>	<p>In the special safety systems, every essential process and nuclear measurement loop, is redundantly designed, usually triplicated so that a single loop component or power failure will not incapacitate or spuriously invoke operation of the system. Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev.5].</p>	C
4.1.4			NA
4.1.4.1	<p>Diverse methods or concepts of the MSD (e.g., rods and poison) shall be used to avoid common-cause failures and cross-link effects.</p>	<p>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 A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].</p>	C
4.1.4.2	<p>When more than one SDS is used, the system components involved in trip initiation shall not be shared between SDS.</p>	<p>Each of the shutdown systems employs a triplicated independent logic system and actuation for sensing the requirement for shutdown. Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].</p>	C
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>Different design teams were used for the two shutdown systems to avoid common design faults. Section 4 of Bruce Nuclear Generating Station 'A' Design Manual for Shutdown System Number Two [NK21-DM-63730-001, Rev. 5]</p> <p>There is a comprehensive system of monitoring, inspection, and testing to ensure the integrity of mechanical components and reliability of equipment. Section 1 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 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>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


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 supply. Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 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 A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].</p>	C
4.1.5	Independence between an SDS and process systems	This is not a requirement/guidance clause (this is a title only).	NA
4.1.5.1	SDS and process system sharing	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>Safety systems are physically separated from, process systems. Redundant components are used when possible to ensure that a failure of a single component does not cause a system failure. Section 1 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].</p>	C
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>Special safety systems are independent of the process systems. Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].</p>	NA

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


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> <ul style="list-style-type: none"> i)The process functions and the SDS functions shall not be credited at the same time. 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. iii)The process function shall be designed to the same standard as the SDS. 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>b)Equipment sharing:</p> <ul style="list-style-type: none"> 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. 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. iii)Isolation devices or interlocks between SDS and process systems shall be classified and qualified as SDS devices. 	Special safety systems are independent of the process systems and perform no process functions. Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].	NA
4.1.6	Independence between SDS and other safety systems	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.	The four special safety systems are independent of each other and the reactor regulating system. Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


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> <p>a) Sharing of components:</p> <p>Sharing shall be restricted to passive components in a specific system. Where such sharing is used, 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 those sources (e.g., decreasing or increasing potential levels, superimposed noise, dirty fluid, changing fluid characteristics).</p>	<p>SDS1 and SDS2 are functionally and physically independent of each other and from containment system and ECI system, along with functionally independent of the reactor regulating system. Independence is achieved by employing diverse shutdown principles. SDS1 uses solid shutoff rods, and SDS2 directly injects poison into the moderator.</p> <p>Separation of the instrumentation channels of the two systems is achieved by channelization. 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. Such channels are referred to as associated channels. Adequate separation is maintained with three different routes for three sets of associated channels. Separation is also achieved between channels following a common route by routing the channels in separate cable pans.</p> <p>Section 6.1.6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].</p>	C
---------	---	--	---

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


4.1.7	A failure in support power (electrical or compressed air) shall not prevent the SDS from performing its function.	<p>In the special safety system, every essential process and nuclear measurement loop is redundantly designed, usually triplicated so that a single loop component or power failure will not incapacitate or spuriously invoke operation of the system.</p> <p>For SDS1, the logic is designed such that any loss of either 120 V (AC) or 48 V (DC) to a channel results in a channel trip. Group A and B Shutoff Rod Clutches each have dual Class II supplied 90 V DC power supplies, one in service and the other in hot standby. For SDS2, the logic and instrumentation have been designed so that a channel trip occurs on loss of power. Emergency power from Qualified Power Supply (QPS) can be manually switched in from the main control room for SDS2 operation and status monitoring for common mode events such as large secondary side failures.</p> <p>Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].</p>	C
4.1.8	Manual trip	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.	Actuation of SDS1 can be done manually by operators using trip buttons in the control room. Actuation of SDS2 can be done manually by operators using trip buttons available both in the control room and in the respective SCA. Section 7 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].	C
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>	The main control room has a manual trip pushbutton for both SDS1 and SDS2. The SCA has a secondary manual trip button for SDS2. Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].	C
4.2	Performance requirements	This is not a requirement/guidance clause (this is a title only).	NA
4.2.1	Reliability	This is not a requirement/guidance clause (this is a title only).	NA

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


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> <p>1)General requirements on reliability and reliability analysis for safety systems can be found in CSA N290.0, Clause 4.5.</p> <p>2)The probability of an SDS failure on demand for existing CANDU plants is typically lower than 10E-3.</p> <p>3)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.</p>	<p>Implementing and maintaining a reliability program in accordance with S-98 [Reliability Programs for Nuclear Power Plants] is a licence condition as specified in PROL 15.00/2015. The reliability requirements for shutdown systems are to have an unavailability of less than 10E-3. As presented in Section 6.1.3 of Part 2 of the Safety Report [NK21-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 10E-3year/year.</p> <p>The reliability targets are specified in the design manuals. The annual reliability reports show that the probability of failure on demand from all causes for some safety systems has not been consistently lower than 10E-3. The current PRA results indicate that the contribution of all sequences, involving failure to shut down, to the large release frequency is about 2.3x10E-7, which is higher than the CNSC REGDOC-2.5.2 proposed target of 10E-7 (Gap). See Safety Factor 6 for more details. This however is not a gap against the PROL.</p>	Gap
4.2.1.2	<p>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.</p> <p>Notes:</p> <p>1)The SDS demonstrated unavailability requirement for existing CANDU plants has been 10E-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>	<p>The reliability of the Shutdown System is monitored and regularly reported. It usually has been substantially better than the 10E-3 y/y unavailability requirement. Section 1 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].</p>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


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>The AECB Siting Guide has specified the maximum permissible failure frequencies for two classes of reactor equipment failure. These two failure limits are:</p> <ol style="list-style-type: none"> 1. process failures (those failures of operating equipment which require the intervention of protective equipment or operator action) shall not occur more frequently than once every three years. 2. "Dual failures", that is, the coincidental failure of a process system and a special safety system, shall not occur more frequently than once every 1000 years. <p>The interpretation of these criteria is essentially the same as the unavailability target of $10E-3$ as discussed below.</p> <p>Process and nuclear measurement loops that are essential to the operation of the special safety systems are redundantly designed and usually triplicated so that a single loop component or power supply failure will not incapacitate or spuriously invoke operation of the special safety system. As presented in Section 6.1.3 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5] to provide a high degree of assurance that a special safety system will perform as designed, the unavailability target of SDS is limited to less than $10E-3$ yr/yr.</p>	C
4.2.3	<p>The SDS design should be simple, conceptually and physically, to facilitate achievement of high performance reliability.</p>	<p>Shutdown systems are designed to be simple and highly reliable. Section 1 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].</p>	C
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> <ol style="list-style-type: none"> a) the use of gravity to move shutoff rods into the core; b) the acceleration of shutoff rod insertion by release of compressed springs (CANDU); and c) the injection of neutron-absorbing liquids by release of compressed gas or hydraulic fluid into the injection system. 	<p>Both shutdown systems employ stored energy to achieve their action: SDS1 uses gravity (for dropping the shutoff rods into the core), as well as stored energy in springs for the assist in initial acceleration; SDS2 uses compressed helium (for injection of a neutron-absorbing solution into the moderator). Section 4 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].</p>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


4.2.5	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 excursion following a PIE is minimized.	Acting alone, both SDS1 and SDS2 have sufficient reactivity depth and act with sufficient speed so that the reactor siting criteria is met. Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].	C
4.2.6	The design should aim for fail-safe operation of its SSCs where such an option exists, while maintaining a balance with simplicity. Note: The requirement for fail-safe operation appears in CSA N290.0, Clause 4.8.	The shutdown systems are designed to be in the failsafe direction for the most likely failure modes. Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].	C
4.3	Detailed SDS design requirements	This is not a requirement/guidance clause (this is a title only).	NA
4.3.1	Trip parameters (variables)	This is not a requirement/guidance clause (this is a title only).	NA
4.3.1.1	SDS trip parameters shall be selected to sense the plant conditions of concern that result from the PIEs considered in the plant design. Notes: 1) Examples of SDS trip parameters for a 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. 2) Annex B provides a list of postulated failures for CANDU reactors.	Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5] summarizes the various trip parameters applicable to the various events. Trip coverage assessments for the various events are included in the Bruce A Safety Report Part 3 [NK21-SR-01320-00003 Rev. 4]. Except for a few cases where limited windows of single trip coverage exist, a minimum of two diverse trips are demonstrated to be effective for each analyzed event. The limited windows of single trip coverage are justified by the impracticality to close them and/or assessed to result is a low risk associated with them.	C
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. A summary of trip parameters is provided in Part 2 of the Safety Report and the SDS Design Manual.	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


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>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 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>	C
---------	---	--	---

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


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>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>	<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 [NK21-OM-09034, Rev.113].</p> <p>The SDS control room panel contains a separate alarm window system which will indicate the state of the trip parameters and trip channels. These windows seal-in when a parameter reached the trip level and will not clear until the operator resets.</p> <p>The design requirements for Secondary Control Area function are presented in the Bruce A Secondary Control Area Design Manual [NK21-DM-63760-001, Rev. 00]. The SCA and associated field panel areas provide control and monitoring capability remote from the MCR Complex to ensure that:</p> <ol style="list-style-type: none"> 1. Reactor units are shut down. 2. Reactor units are cooled down. 3. Common containment is maintained. <p>The above functions shall be accomplished by monitoring and controlling Unit 0, 1- 4, (and in particular the applicable Critical Safety Parameters (CSP)):</p> <ol style="list-style-type: none"> 1. From the SCA and associated field panels, and 2. By local field control actions. <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. A summary of the operator actions credited in the safety analysis is documented of the Safety Report 1.3 of Part 3 of the Safety Report. Operator actions considered in Bruce A safety analysis are consistent with the requirements for existing CANDU plants as per section 4.4.4.5 Guidance for Operator Action of CNSC REGDOC-2.4.1.</p>	C
4.3.2	Trip sensors	This is not a requirement/guidance clause (this is a title only).	NA

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


4.3.2.1	<p>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>	<p>As described in Part 2, Section 6.1.4 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 or power supply failure will not incapacitate or spuriously invoke operation of the special safety system.</p> <p>There are two neutronic parameters that will initiate a reactor shutdown through SDS1. The parameters are high neutron power, derived from vertical in-core flux detectors, and high neutron log rate derived from vertical ion chambers. In addition to these neutronic trip parameters, an absolute log of neutron power trip (referred to as absolute Log N) is available for operation at low power. All components used to generate trip functions are designed as part of the SDS and meet the same requirements.</p> <p>SDS1 has 7 process trip parameters that initiates a reactor shutdown: Heat Transport High Pressure, Heat Transport Low Pressure, Heat Transport Low Flow, Steam Generator Low Level, Pressurizer Low Level and Pressurizer Very Low Level, Moderator High Temperature, and startup instrumentation trip below range limits.</p> <p>There are two neutronic parameters that will initiate a reactor shutdown through SDS2, high neutron power, derived from horizontal in-core flux detectors and, in Units 1 and 2 only, vertical in-core flux detectors, and high neutron log rate, derived from horizontal ion chambers. In addition, an absolute log of neutron power trip is available for operation at low power.</p> <p>SDS2 has 4 process trip parameters that will initiate a reactor shutdown:</p> <p>Heat Transport High Pressure, Heat Transport Low Pressure, Steam Generator Low Level, and Pressurizer low Level.</p> <p>Table 6-1 in the Bruce A Safety Report shows the trip variables, setpoints and conditioning parameters [NK21-SR-01320-00002 Rev. 5, Section 6].</p>	C
---------	--	---	---

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


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 to a large variety of detailed requirements. All the systems are designed for very high reliability and availability, tolerant to expected and unexpected transients, and designed for a minimum of regular maintenance. Section 7 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].</p>	C
4.3.2.3	<p>The sensors and their associated instruments shall have provisions for calibrating their signals to the required accuracy.</p>	<p>Surveillance requirements cover all Safety Analysis Limits on process parameters, plus additional checks and tests to ensure that the credited components are able to perform their credited safety function. Surveillance frequencies are determined principally by the unavailability requirements for the system as confirmed by unavailability assessments. This means that test frequencies could be changed provided the impact on system unavailability and instrument loop uncertainty is determined to be acceptable. In other cases, test frequencies are based on standard industry practice or specified by the regulator. Any change to existing surveillance frequencies must be assessed for impact on both system unavailability and instrument loop uncertainty. Loop calibration is a complete check of the instrument loop, including the sensor. Where a loop calibration is specified for a setpoint, this refers specifically to calibration of the associated alarm unit. The surveillance verifies that the instrument loop responds to the measured parameter within the necessary range and accuracy. Loop calibration leaves the instrument loop adjusted to account for instrument drift between successive calibrations consistent with the plant specific setpoint methodology as per Operational Safety Requirements for Bruce A Shutdown Systems [NK21-OSR-63720-63730-00001].</p> <p>Bruce Power maintains station calibration records, which reflect existing scheduled calibration frequencies for instruments. As such, the requirement of the clause is deemed in compliance</p>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


4.3.2.4	<p>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>	<p>In-core detectors are used for power measurements because the ion chambers do not provide the necessary spatial flux information. These detectors are characterized by a sensitivity to both neutron and gamma fluxes, where the sensitivity of different types of detectors vary with irradiation. They are used to give a measurement of reactor power from source level to 150% of full power. Various detectors are distributed in the core to provide accurate information on power levels and its spatial distribution as per Bruce A Safety Report – Part 2 [NK21-SR-01320-00002].</p> <p>The reason for the various detectors used is due to the detectors having mixed responses, being sensitive to both neutron and gamma rays. Also, not all detectors are sensitive to the same operating range. If a type of detector is not sensitive within the operating range then a different type of detector is used. As such, the requirement of the clause is deemed in compliance</p>	C
4.3.3	Trip set points	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>Each automatic instrumentation function listed in the Instrumentation Summary Tables (Table 4.3-1, Table 4.3-2) shall be operable. This is the desired steady state condition for which shutdown system reliability has been demonstrated as per Operational Safety Requirements for Bruce A Shutdown Systems [NK21-OSR-63720-63730-00001].</p> <p>“Shutdown system trip set points shall be adjusted to maintain trip coverage claimed in the Safety Report. Manual adjustment of the trip set points shall only be made following procedures that are approved by the Senior Operations Authority” as per section 63.5 of the Operating Policies and Principles - Bruce A [BP-OPP-00002 R012].</p> <p>Bruce Power has defined nominal trip set points in the indicated tables of the OSR. Any necessary deviation to these values requiring a manual adjustment must follow approved procedures by the Senior Operations. As such, this the requirement of the clause is deemed in compliance</p>	C

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


4.3.3.2	Where automatically adjusted set points are incorporated, the design of the set point adjusting 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.	The Bruce A design does not include automatically adjusted set points. Detailed requirements for the adjustment of the trip set points are stated in the design manuals for the shutdown systems [NK21-DM-63720-001 and NK21-DM-63730-001].	NA
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 63.5 in Operating Policies and Principles - Bruce A [BP-OPP-00002 R012], manual adjustment of the trip setpoints shall only be made following procedures approved by the Senior Operation Authority.	C
4.3.3.4	<p>Trip set points shall be selected to provide sufficient allowance between the set points and corresponding safety analysis limits to account for uncertainties. The uncertainties include but are not limited to</p> <ul style="list-style-type: none"> a)instrument calibration uncertainties; b)instrument uncertainties during normal operation; c)instrument drift; d)instrument uncertainties caused by design basis events; e)process-dependent effects; f)calculation effects; g)dynamic effects; and h)calibration and installation bias accounting. <p>Notes:</p> <ul style="list-style-type: none"> 1)Based on ANSI/ISA-67.04.01. 2)Set point margins should accommodate normal operational transients to minimize spurious trips without compromising the safety margin. 	<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 Safety Report.</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>	IC
4.3.4	Trip logic	This is not a requirement/guidance clause (this is a title only).	NA

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


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>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>	<p>SDS1 uses 2 out of 3 local coincidence logic, whereas SDS2 uses 2 out of 3 general coincidence logic. SDS1 has three independent channels from the sensor location to the output tripping relay. The logic and equipment is arranged in a manner that ensures no single fault will disable the system. Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].</p>	C
---------	--	---	---

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


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.	<p>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".</p> <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. Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].</p>	C
---------	--	---	---

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


4.3.4.3	<p>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>	<p>For SDS1, the ion chamber and in-core detector amplifier units are located in the reactor auxiliary bay rooms. There is a separate enclosed cubicle for each channel of SDS1 located in the control equipment room. These channel trip cubicles contain all the relay equipment for each of the channels. All of the reactor measuring devices on SDS1 are field mounted in a manner which minimizes the possibility of common mode failures with devices used for SDS2 and for the regulating system. Their connecting cables are separately routed back to the three SDS1 channel cubicles in the control equipment room. For SDS2, the ion chambers and in-core detectors for SDS2 are horizontally mounted and their cables are routed in conduit through the side of the containment to ensure complete separation from SDS1. The cubicles and panels containing the logic for each channel are located in three channelized instrument rooms. General coincidence is used, so there are no cross connections between the trip logic from the sensor to the valves as per Bruce A Safety Report – Part 2 [NK21-SR-01320-00002].</p> <p>As described in Part 2 of the Safety Report, there is one manual trip pushbutton and one test trip pushbutton. The manual trip can be actuated from the SDS2 main control room panel. There is a local test trip button for each channel, mounted on each SDS2 channel cubicle, which can operate only one channel at a time. A valve reset pushbutton on the SDS2 main control room panel is used to minimize the number of times the poison injection valves open and close during testing. There is a second manual trip pushbutton located in the secondary control area (SCA). The manual trip pushbutton in the SCA is connected directly to the channel trip logic. The manual trip from the main control room is connected to the channel trip logic via buffer relays.</p> <p>Bruce Power has demonstrated through the equipment layout of SDS's of equipment separation between SDS's, along with no cross connections between trip logics. As such, the requirement of the clause is deemed in compliance.</p>	C
---------	--	--	---

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


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>All shutdown system actions that are required in the short term are automatic for all accidents considered at Bruce A. 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 1-24 through 1-33 of Section 1 of Part 3 of the Safety Report. It can be seen that for the shutdown actions required by the operator there is substantial time for such actions, usually 15 minutes or more.</p> <p>Instrumentation and control systems are designed with the maximum practical amount of automatic control incorporated in the design to allow the station to be operated with minimum staff to leave operators free for higher level monitoring the overall unit status. The operator can readily intervene in the operation of the automatic control systems if necessary. Section 7 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].</p>	C
4.3.5	Completion of trip action	This is not a requirement/guidance clause (this is a title only).	NA
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>A computer system is used to monitor the state of the shutdown and ECI systems. In SDS1, it is kept in shutdown state by automatic insertion of the shutoff rods, whenever certain parameters exceed specified bounds. In SDS2, it is kept in the shutdown state by automatic injection of a gadolinium nitrate solution into the moderator in the calandria, whenever certain parameters exceed specified bounds as per Bruce A Safety Report [NK21-SR-01320-010002].</p> <p>By design, Bruce Power has shown during shutdown actions that all actions of associated equipment are driven automatically. As such, the requirement of the clause is deemed in compliance.</p>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


4.3.5.2	<p>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>	<p>SDS trips are typically subject to a seal-in delay. Shutdown system action is initiated the moment the trip setpoint is exceeded but is sealed in only if the parameter remains beyond the setpoint for the duration of the delay time. The maximum duration for the delay is established such that SDS response does not affect the parameter initiating the trip as per Bruce Power training manual [CMT-60544-00003].</p> <p>The trip seal-in time delay is intended to minimize the frequency of spurious trips. It ensures that a trip signal must be sustained for a specific period in order for the reactor trip logic to seal-in. As indicated in the Design Manual, the nominal SDS1 trip seal-in time delay is 0.15 seconds. After this time, the reactor trip logic will not re-set without operator intervention even if the trip condition clears. The maximum Safety Analysis Limit of 0.30 seconds is acceptable based upon ensuring that there is no potential for inadvertent clearing of the trip due to shutoff rod movement. There is no minimum Safety Analysis Limit, as a lower seal-in time reduces the likelihood that a trip will clear due to shutoff rod movement during an accident. Unlike Bruce B, the Bruce A SDS2 trip logic does not incorporate a seal-in delay.</p> <p>As such, this meets the requirements of the clause and is deemed in compliance.</p>	C
---------	---	--	---

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


4.3.5.3	Resetting of the trip logic and repositing of the reactivity components subsequent to the trip action shall be initiated only manually and shall not interrupt the completion of the shutdown action.	<p>Although the Bruce A Safety Report, Bruce Power DMs, and OSR do not explicitly state manual resetting of the trip logic and repositing of reactivity components, Section 63.9 of the OP&P states:</p> <p>“a) Shift Manager authorization is required prior to resetting all reactor trips. Prior to giving this authorization, the Shift Manager shall confirm that:</p> <ul style="list-style-type: none"> i) The cause of the trip is clearly understood. ii) Unit and station conditions are appropriate to allow resetting of the trip. <p>b) Senior Operations Authority approval is required prior to resetting the following completed reactor trips:</p> <ul style="list-style-type: none"> • Any neutronic trip. • A trip preceded by a log rate stepback. • A conditioned parameter trip in indicated rising neutron power.” <p>Therefore, this clause has been assessed as Indirect Compliance.</p>	IC
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 A. 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 1-24 through 1-33 of Section 1 of Part 3 of the Safety Report [NK21-SR-01320-00003, Rev.004]. It can be seen that for the shutdown actions required by the operator there is substantial time for such actions, usually 15 minutes or more.</p> <p>In general, the safety systems are automatically initiated for all accidents and there are no permissives that require operator action or any means of inhibiting the trip initiation. Once the safety systems are initiated, the operator cannot stop the actions.</p>	C
4.3.6	Trip computers	This is not a requirement/guidance clause (this is a title only).	NA

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


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> <p>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.</p> <p>2) Software for SDSs is considered as having high safety significance. See CSA N290.14.</p> <p>3) For qualification of pre-developed software, see CSA N290.14.</p>	<p>Since Bruce A design does not incorporate digital equipment to read inputs, execute software programs and activate SDS components, this requirement is not applicable.</p> <p>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. Experience has proven that availability in excess of 99% for each computer is readily achievable. As a result, the dual computer system assures the very high reliability required for the station control system.</p> <p>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 combination of internal hardware and software self-checking. Their effects are mitigated by the independent Watchdog Timers (WDTs) 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 a fresh copy of the core image from a protected area on the solid state memory and restarts the computer, is combined with the fault detection to provide a system practically immune to transient faults as per section 7.1 of Bruce A Safety Report – Part 2 [NK21-SR-01320-00002].</p> <p>As a result, this meets the requirement of the clause and is deemed in compliance.</p>	NA
4.3.6.2	<p>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.</p>	<p>Since Bruce A design does not incorporate computerized SDS trips and safety related software; this requirement is not applicable.</p> <p>The instrumentation of the SDS is separated by channelization. Each of the three channels on a specific special safety system follows a separate route. Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].</p>	NA
4.4	Display requirements	This is not a requirement/guidance clause (this is a title only).	NA

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


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>SDS1 and SDS2 have separate display panels in the main control room that display different parameters. One SCA is located in the Construction Retube Building covers Units 1 and 2, and another SCA is located in Unit 3 that covers Units 0, 3, and 4. Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].</p> <p>The reactor units can be shut down from high power by tripping SDS2 from the SCA. The SCA has access to all three channels G, H, J. The reactor trip is provided by the operation of two of the three handswitches located on the SCA panel PL3183. The SCA intervention places two normally open contacts in each channel valve circuit clear of any wiring going to the MCR Complex in order to effectively isolate the valves.</p> <p>Reactor shutdown capability and monitoring of reactor power level is controlled and monitored from SCA. The SCA manual trip relays are downstream of all the other trip chain relays. They are normally open contacts held closed when energized by QPS, i.e., fail-safe and do not have any effect on SDS2 when under MCR control. The reactor power indication has dual signal isolation to prevent any electrical disturbance in the SCA from affecting SDS2 readings in the MCR or vice versa.</p>	C
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.	Each unit has a station safety system monitoring computer that display margin-to-trip ratio for the in-core flux detectors. Section 6 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].	C
4.5	SDS testing	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 A design has no SDS computer testing equipment in use.</p> <p>Therefore; this requirement is not applicable.</p>	NA

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


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.	Bruce A Safety Report, Bruce Power DM's, and OSR do not explicitly state SDS tests should be done prior to first criticality in the appropriate shutdown state. 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 practical to determine that the system acts in a predicted and acceptable manner for faulted conditions (e.g., transient or temporary loss of power).	NA
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 1 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002 Rev. 5].	C
4.6	<p>Consideration shall be given to cyber security for the digital SDS equipment.</p> <p>Notes:</p> <p>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.</p> <p>2)Further guidance on cyber security can be found in IEEE 7-4.3.2 and IEC 61513.</p>	Cyber security is addressed separately due to the sensitivity of the information.	RNA
4.7	Equipment qualification	This is not a requirement/guidance clause (this is a title only).	NA

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

4.7.1	<p>Equipment for the SDS should</p> <ul style="list-style-type: none"> a) be of a proven design (industrial experience); b) have a predictable failure mode; c) be designed to facilitate test, maintenance, and repair; and d) have an expected operating life that is equal to or greater than the life of the plant. 	<p>For points a) and b), all SSCs important to safety have been in place at Bruce A 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.</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 as per Section 7.14 of Draft Regulatory Document RD-337 Review [RABA 0804]. They 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&Ps Section 63.1 Shutdown System Availability [BP-OPP-00002, R012]. As such, this meets the requirements of the clause and is deemed in compliance</p>	C
4.7.2	<p>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>	<p>Bruce A 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). 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. For example, all instrument rooms (R-317, 316 and 211) at Bruce A are 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 maintenance that takes place on SDS equipment in the vault. It is common practice for Bruce Power to request EMI/RF qualification for all new I&C components, which is typically documented in the Technical Specifications.</p>	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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 63 of the Operating Policies and Principles - Bruce A [BP-OPP-00002 Rev. 12] states: "Maintenance of the shutdown system neutron power instrumentation shall be done with the reactor at a sufficiently high power so that the effect of the maintenance is immediately apparent before it is returned to service unless approval is given by the Senior Operations Authority for an alternate reactor state."	C
-----	---	--	---


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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.	<p>The safety objectives and concepts described in this section apply to an NPP during operation or during an accident.</p> <p>Four common plant states are defined: normal operation; anticipated operational occurrence (AOO); design-basis accident (DBA); and beyond-design-basis accident (BDBA). This document also introduces the plant state “design extension conditions” (DECs), as a subset of BDBAs that are considered in the plant design.</p>	<p>These are introductory remarks; hence no assessment is needed.</p> <p>Design details about the definition of plant states are provided later on in Clause 4.2.3.</p>	NA
4.1	<p>In support of the NSCA and its associated regulations, the CNSC endorses the objective established by the IAEA that NPPs be designed and operated in a manner that will protect individuals, society and the environment from harm. This objective relies on the establishment and maintenance of effective defences against radiological hazards in NPPs.</p> <p>The general nuclear safety objective is supported by three complementary safety objectives, which deal with radiation protection, the technical aspects of the design, and environmental protection. The technical safety objective is interdependent with administrative and procedural measures that are taken to ensure defence against hazards due to ionizing radiation.</p>	<p>A new safety objective, i.e., environmental protection has been introduced in CNSC REGDOC-2.5.2.</p> <p>These are introductory remarks; hence no assessment is needed. Environmental protection is discussed later on in Clause 10.</p> <p>The radiological impact of the nuclear power plant on the environment is discussed in Safety Factor 14.</p>	NA
4.1.1	The radiation protection objective is to provide that during normal operation, or during anticipated operational occurrences, radiation	The change introduced in the second paragraph is editorial in nature	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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>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 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</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</p>	C

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	of accidents with serious radiological consequences will be extremely low.	<p>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 A consists of three main parts and presents the following information:</p> <p>Part 1 provides a general description of plant and site, including environmental considerations.</p> <p>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.</p> <p>Part 3 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. 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 A.</p> <p>BP-PROC-00133 Hazardous Waste Management Requirements describes how Bruce Power complies with applicable federal, provincial, and local regulations and corporate requirements affecting the generation, handling, storage, and disposal of hazardous waste.</p> <p>The design provisions for environmental protection are discussed in detail later on under Clause 10. The radiological impact of the nuclear</p>	C

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
		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"> dose acceptance criteria safety goals <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 Safety Report describes the analysis acceptance criteria, including regulatory criteria and derived criteria. Meeting the derived criteria ensures that the regulatory criteria are met. Dose acceptance criteria for DBAs and the plant safety goals for BDBAs are met. The Safety Report presents an introduction (Part 1), a detailed description (Part 2) and the Safety Analysis (Part 3) for Bruce A. 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 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"> 0.5 millisievert (mSv) for any AOO or 	<p>The changes in this clause are provided for clarification and guidance; therefore they have no impact on the requirements. A review of the same clause in RD-337 as documented in [NK21-CORR-00531-11005] indicated that the Bruce A design does not fully meet this requirement. The Bruce A 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, 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. Bruce Power is implementing a Safety Report Improvement Program starting in 2014</p>	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2. 20 mSv for any DBA</p> <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>including annual status and progress updates to the CNSC staff. 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, File:NK21-CORR-00531-10774 & NK21-CORR-00531-11155.</p> <p>The acceptance criteria for the radiological consequences of postulated events are specified of the Safety Report 1.5, Part 3 of Bruce A Safety Report [NK21-SR-01320-00003, Rev. 004]. 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 A 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	<p>Qualitative safety goals</p> <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>In comparison to RD-337, there are no changes to the requirements in this clause. 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>A review of the same clause in RD-337 indicated that the Bruce A safety goals are less restrictive (i.e., larger) than those proposed for new plants [NK21-CORR-00531-11005]. This is identified as a gap (Gap).</p> <p>Bruce Power specified that the SCDF limit is 10E-4 per reactor year compared to the RD-337/REGDOC-2.5.2 quantitative safety goal of 10E-5 per reactor year. Bruce units meet the 10E-4 SCDF limit but the values are higher than the quantitative goal of CNSC REGDOC-2.5.2 (10E-5).</p> <p>Bruce Power specified safety goals include Large and Severe</p>	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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> <ol style="list-style-type: none"> core damage frequency small release frequency large release frequency <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 10E-5 per reactor year.</p> <p>Small release frequency</p>	<p>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 >1% fraction of Cs-137 inventory. The Bruce Power Severe Release Frequency is defined as the frequency of events with releases from containment > 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 A PRA are defined in accordance with the requirement of this clause. However, the limiting values of the safety goals adopted in the Bruce A PRA are one order of magnitude larger than the corresponding limits required in the clause, i.e., Bruce A PRA uses the safety goal limits defined in the Level 2 PRA Guide B-REP-03611-00010:</p> <ul style="list-style-type: none"> for the severe core damage frequency to be less than 10E-4 per reactor year; for the small release frequency to be less than 10E-4 per reactor year; for the large release frequency to be less than 10E-5 per reactor year. <p>The following results of the Bruce A PRAs are summarized in the letter NK21-CORR-00531-11324 submitted to the CNSC on July 31, 2014:</p> <p>Severe Core Damage Frequency (SCDF) for At-Power Internal Events:</p> <p>3.82E-6 per reactor year</p> <p>(if Emergency Mitigating Equipment (EME) installed for Fukushima-related improvements are credited) or</p> <p>2.07E-5 per reactor year</p> <p>(without crediting the Fukushima-related EME, as obtained in the Level 1 At-Power Internal Events PRA NK21-03611.1 P NSAS)</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The sum of frequencies of all event sequences that can lead to a release to the environment of more than $10E15$ becquerels of iodine-131 shall be less than $10E-5$ 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 $10E14$ becquerels of cesium-137 shall be less than $10E-6$ 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 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</p>	<p>SCDF for Outage Internal Events:</p> <p>$1.28E-5$ per reactor year</p> <p>SCDF for Internal Flood:</p> <p>$5.5E-7$ per reactor year (with the Fukushima-related EME credited)</p> <p>SCDF for Fire Hazard:</p> <p>$8.72E-6$ per reactor year (with the Fukushima-related EME credited)</p> <p>SCDF for Seismic Hazard:</p> <p>$1.7E-6$ per reactor year (crediting the Fukushima-related EME)</p> <p>SCDF for High Wind Hazard:</p> <p>$4.8E-6$ per reactor year (crediting the Fukushima-related EME)</p> <p>Aggregated SCDF by adding the above SCDFs:</p> <p>$3.24E-5$ per reactor year (with the Fukushima-related EME credited)</p> <p>Large Release Frequency (LRF) for At-Power Internal Events:</p> <p>$3.00E-7$ per reactor year</p> <p>(if Emergency Mitigating Equipment (EME) installed for Fukushima-related improvements are credited) or</p> <p>$9.9E-6$ per reactor year</p> <p>(without crediting the Fukushima-related EME, as obtained in the Level 1 At-Power Internal Events PRA NK21-03611.1 P NSAS)</p> <p>LRF for Fire Hazard:</p> <p>$7.32E-6$ per reactor year (with the Fukushima-related EME credited)</p> <p>LRF for Seismic Hazard:</p> <p>$1.7E-6$ per reactor year (with the Fukushima-related EME credited)</p> <p>LRF for High Wind Hazard:</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>(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 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, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants.</p>	<p>4.8E-6 per reactor year (crediting the Fukushima-related EME)</p> <p>Aggregated LRF by adding the above LRFs:</p> <p>2.37E-5 per reactor year (with the Fukushima-related EME credited)</p> <p>Small Release Frequency (SRF) for At-Power Internal Events:</p> <p>9.95E-6 per reactor year</p> <p>(without crediting the Fukushima-related EME, as obtained in the Level 1 At-Power Internal Events PRA NK21-03611.1 P NSAS)</p> <p>Although the above results meet the safety goal limits set up for Bruce A PRAs, they do not meet the more stringent quantitative safety goals set up in the requirement clause. Therefore, a gap is assessed against this clause.</p>	
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"> 1. normal operation 2. AOOs 3. DBAs 	<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 A, based on the range of analyses performed. It is recognized that when Bruce A 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 A does not distinguish between these four classes of events. The DEC's 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 DEC's. 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) A three-year Safety Report Improvement 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 RD-310 compliant analyses for Common</p>	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>4. BDBAs, including DECAs (DECAs could include severe accident conditions)</p> <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 in section 9.0.</p>	<p>Mode Failures will be introduced into the Safety Reports as well. The project is scheduled for completion in time for the next Safety Report update in 2017.</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 supporting documentation for NK21-CORR-00531-11567, Bruce Power is implementing a Safety Report Improvement Program starting in 2014 including annual status and progress updates to the CNSC staff. This program is expected to address both gaps.</p>	
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"> 1. consideration of inherent safety features 2. incorporation of engineered design features 3. onsite accident management procedures established by the operating organization 4. establishment of offsite intervention measures by responsible 	<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 A design incorporates engineered safety features and specific accident management procedures for AOOs, DBAs and some BDBAs as described in the Abnormal Incidents Manual [NK21-OM-09034, Rev.113].</p> <p>As a result of Fukushima event lessons learned Bruce Power is implementing Expanded Severe Accident Management Guidelines for dealing with severe accidents. The key programmatic elements of SAMG implementation for single unit events have been completed for Bruce A. Demonstration of the effectiveness of SAMG using table-top exercises and drills has already been completed by Bruce Power for single unit events. Demonstration of the effectiveness of multi-unit SAMGs will also be assessed through table-top exercises and drills.</p> <p>Bruce Power assessed the reactor's defence-in-depth for a severe accident and identified areas for potential enhancements. In cases, the evaluation indicates that there is a gap; however if enhancements of the systems, structures and components is not an option, mitigating features are provided. For example, where the existing means to protect containment integrity and prevent uncontrolled</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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"> Canadian Nuclear Safety Commission (CNSC), G-129, rev 1, Keeping Radiation Exposures and Doses “As Low as Reasonably Achievable (ALARA),” Ottawa, Canada, 2004. CNSC, REGDOC-2.3.2, Accident Management: Severe Accident Management Programs for Nuclear Reactors, Ottawa, Canada, 2013. International Atomic Energy Association (IAEA), Safety Guide NS-G-2.15, Severe Accident Management Programmes for Nuclear Power Plants, Vienna, 2009. 	<p>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 is considering 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. The bypass tees would be installed during the next scheduled containment outages at each station. The purpose of the bypass line and isolation valves is to allow containment filtered venting system to be installed at a later date without the need for an additional containment outage. Installation of the containment bypass line is tied to the Bruce A containment outage and is currently scheduled for 2015. Bruce Power is performing 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.</p> <p>An off-site emergency plan that is integrated with appropriate off-site authorities [BP-PLAN-00001, R004] is in place. The Bruce A 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 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.</p>	
4.3	Safety concepts	This is not a requirement/guidance clause (this is a title only).	NA

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
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 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 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>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 [RABA 0804]. 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 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 normally credited in Canadian 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 the control or safety systems.</p> <p>The application of defence in depth is described in more detail in later sections.</p>	C




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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>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>		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Additional information may be found in:</p> <ul style="list-style-type: none"> IAEA, INSAG-10, Defence in Depth in Nuclear Safety, Vienna, 2010. 		
4.3.2	<p>An important aspect of implementing defence in depth in the NPP design shall be the provision of 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>	<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 A meets the general principles as formulated in this clause.</p> <p>Details of physical barriers incorporated in the Bruce A design are provided in the corresponding compliance sections of this assessment.</p>	C
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> <ol style="list-style-type: none"> safety limits 	<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 LCH (LCH-BNGSA-R8) specified under Licence Condition 3.1 Maintaining Operating Policies and Principles (OP&P) that the current documentation (i.e., Bruce Power's OP&Ps) does not contain a comprehensive set of operating limits and conditions. Bruce Power is implementing 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. 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>A self-assessment and pilot CNSC inspection have identified some gaps in areas not within the scope of the baseline project. Gaps and</p>	AD

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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>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>areas for improvement in programmatic aspects identified in the self-assessment and pilot inspection are being addressed via a corrective action plan. Assessment of compliance will be part of ongoing CNSC compliance monitoring activities. Improvements to the SOE program have been identified. The completion of the actions will be according to the Bruce Power corrective action program. Addressing the gaps in the SOE program implementation and the results of the CNSC's review of the program gaps identified is captured in the Integrated Implementation Plan for Bruce A and B and Center of Site. Gaps and areas for improvement in programmatic aspects identified in the self-assessment and pilot inspection are being addressed via a corrective action plan. Assessment of compliance will be part of ongoing CNSC compliance monitoring activities. Improvements to the SOE program have been identified. The completion of the actions will be according to the Bruce Power corrective action program.</p> <p>The current practice is to define three impairment levels as described in Safety Related Systems Impairments Manual [NK21-OM-03672, Rev. 011]. 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>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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 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"> o CSA Group, N290.15, Requirements for the safe operating envelope of nuclear power plants, Toronto, Canada. o IAEA Safety Guide NS-G-2.2, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, Vienna, 2000. 	<ul style="list-style-type: none"> • The uncertainty associated with the surveillance instrumentation for instrument loops used by operator for direct surveillance and action (e.g., panel checks), • The uncertainty associated with the instruments specifically used for an automatic actuation in an instrument loop <p>As discussed above the various operating limits and 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</p>	RNA

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
		assessed.	
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>The NPP design shall:</p> <ol style="list-style-type: none"> 1. meet Canadian regulatory requirements 2. meet the design specifications 3. be confirmed by safety assessment 4. take into account current safety practices 5. fulfill the requirements of an effective management system 6. incorporate only those design changes that have been justified by technical and safety assessments <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"> 1. a clear division of responsibilities with corresponding lines of 	<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 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> <ul style="list-style-type: none"> • Demonstration that the design basis is understood and controlled, and that the current condition of systems is understood. • 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. • Demonstration that nuclear safety assessment takes into 	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>authority and communication</p> <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>account the current and expected future condition of systems and that safety criteria are and will continue to be met with confidence.</p> <ul style="list-style-type: none"> 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. A set of opportunities for improvement arising from the interim 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>Bruce Power is implementing a Safety Report Improvement Program starting in 2014 including annual status and progress updates to the CNSC staff. See 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 & NK21-CORR-00531-11155.</p> <p>Any design changes follow the requirements of the Plant Design Basis Management Program BP-PROG-10.01, which identifies processes to ensure that the design changes have been appropriately considered.</p> <p>The Bruce Power Management System Manual [BP-MSM-1, R012] 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 and Modification and in the BP-PROC-00335 Design Management. As described in Bruce Power MSM, the Management System is based on the establishment of a safety culture that assures public/nuclear, environmental and worker safety. It also provides the necessary guidance for making risk-based decisions that satisfy the desired balance between safety, commercial & 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. These are identified in Appendix A.</p> <p>To ensure that Bruce Power fosters and maintains a positive Safety</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
		<p>Culture, periodic assessments of the Safety Culture at Bruce Power are conducted. The standards associated with conducting these Safety Culture assessments are identified in BP-PROC-00302, Safety Culture Assessments. This indicator provides a measure of "perception".</p> <p>The organization, management system and safety culture are further assessed in SF10. It is noted that the CSA N286.0 standard has been adopted by Bruce Power for application to all aspects of its management system in accordance with the PROL 15.00/2015.</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 design authority has achieved the following objectives for the design:</p> <ol style="list-style-type: none"> 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 2. ensured the availability of the design information that is needed for safe plant operation and maintenance 	<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] ensures that the plant design meets safety, reliability, and regulatory requirements including pressure boundary quality assurance requirements described in BP-PROG-00.04, 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 documented in DIV-ENG-00009 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 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>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>3. established the requisite security provisions in accordance with the Nuclear Security Regulations and associated regulatory documents</p> <p>4. maintained design configuration control</p> <p>5. reviewed, verified, approved and documented design changes</p> <p>6. established and controlled the necessary interfaces with responsible designers or other suppliers engaged in design work</p> <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"> CSA Group, N286, Management system requirements for nuclear power plants, Toronto, Canada. IAEA, Safety Standards Series GS-G-3.5, The Management System for Nuclear Installations 	<ul style="list-style-type: none"> Provides a safe and reliable design for the nuclear facility. Ensures engineering activities are performed in accordance with BP-PROG-00.04, Pressure Boundary Quality Assurance Program and applicable codes, standards and regulatory requirements. 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. Ensures that design configuration control is maintained. Maintains the design expertise required for the safe design and operation of the facility. <p>The Design Management Procedure, as documented in BP-PROC-00335 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. This procedure interfaces with the implementing procedures of BP-PROG-10.02, 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, 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 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</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Safety Guide, Vienna, 2009.</p> <ul style="list-style-type: none"> IAEA, INSAG-19, Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life, Vienna, 2003. 	<p>ageing) that may affect the Design Basis or the Safety Report Basis. This 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, 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, 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 the Design Management Procedure [BP-PROC-00335, R006] 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, Design Management. 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, Nuclear Oversight Management.</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
5.2	<p>Appropriate design management shall achieve the following objectives:</p> <ol style="list-style-type: none"> SSCs important to safety meet their respective design requirements. Due account is taken of the human capabilities and limitations of personnel. Safety design information - necessary for safe operation and maintenance of the plant and for any subsequent plant modifications - is preserved. OLCs are provided for incorporation into the plant administrative and operational procedures. The plant design facilitates maintenance and ageing management throughout the life of the plant. The results of the hazard analysis, deterministic safety analysis and probabilistic safety assessment are taken into account. Due consideration is given to the prevention of accidents and mitigation of their consequences. The generation of radioactive and hazardous waste is limited to minimum practicable levels, in terms of both activity and 	<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 A design does not fully meet this requirement. BP-PROG-10.01 and the Design Management Program, [BP-PROC-00335, R006] 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.</p> <p>Ageing management is specifically described in the Equipment Reliability Program, BP-PROG-11.01, and is considered in design basis management, as per BP-PROG-10.01, "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, Human Factors Engineering Program Plan. If the classification of the human factors is determined to be "minor", DPT-PDE-00001, Human Factors Minor Change is to be followed.</p> <p>BP-PROC-00335, Design Management and BP-PROC-00363,</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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>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>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. BP-PROC-00133 Hazardous Waste Management Requirements ensures that Bruce Power is in compliance with applicable federal, provincial, and local regulations and corporate requirements affecting the generation, handling, storage, and disposal of hazardous waste.</p> <p>The Bruce Power Engineering Change Control program [BP-PROG-10.02, R009] 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 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	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	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	Gap

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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"> • design initiation, including identification of scope • work control and planning of design activities • selection of competent staff 	<p>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] 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]. This manual describes the responsibilities of the functionaries of the department. Section 4.3 of the Quality Assurance of Safety Analysis [DPT-NSAS-00001] 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 Analysis Software [DPT-NSAS-00011] 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] established the Safety Report update process and [DPT-NSAS-00003] 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 earlier. A summary of the applicable procedures is presented as follows:</p> <p>1. This procedure on Quality Assurance of Safety Analysis [DPT-</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> identification and control of design inputs establishment of design requirements evaluation of design concepts and selection of preferred concept selection of design tools and computer software conduct of conceptual safety analysis to assess preferred design concept conduct of detailed design and production of design documentation and records definition of any limiting conditions for safe operation design verification and validation configuration management identification and control of design interfaces <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 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</p>	<p>NSAS-00001] specifies the QA process for deterministic safety analysis and includes requirements for personnel under Section 4.3 on Personnel Capability.</p> <ol style="list-style-type: none"> [DPT-NSAS-00015] procedure on Execution of Safety Analysis outlines the systematic methodology for conducting safety analysis. [DPT-NSAS-00013] procedure on Guidelines for Managing Reference Data Sets ensures that only verified datasets are used for deterministic safety analysis. This practice has been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report. Not all of the existing analyses have used validated models and computer codes that would meet the current standards. This practice has been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report. This procedure on Execution of Safety Analysis [DPT-NSAS-00015] outlines the review process for safety analyses. <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-2.4.2 in Safety Factor 5.</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-2.4.2 in Safety Factor 5 (Gap).</p>	




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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>Additional information may be found in:</p> <ul style="list-style-type: none"> American Society of Mechanical Engineers (ASME), NQA-1-2008, Quality Assurance Requirements for Nuclear Facility Applications, New York, 2008. CNSC, G-149, Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors, Ottawa, Canada, 2000. CSA Group, N286, Management system requirements for nuclear power plants, Toronto, Canada. CSA Group, N286.7.1, Guideline for the application of 		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>N286.7-99, Quality assurance of analytical, scientific, and design computer programs for nuclear power plants, Toronto, Canada.</p> <ul style="list-style-type: none"> IAEA, GS-R-3, The Management System for Facilities and Activities, Vienna, 2006. Nuclear Information and Records Management Association/American National Standards Institute (ANSI), 1.0, Standard Configuration Management, Washington, D.C., 2007. 		
5.4	<p>The design authority shall identify the modern 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 qualification</p>	<p>There is no change to the requirements.</p> <p>Bruce A design meets the intent of this requirement. All of the SSCs important to safety have been in place at Bruce A for 30 years (proven design). 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>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 satisfactorily.</p>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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>The Bruce A design incorporates another feature that was new to CANDU stations, the use of the PHT pump seals as the containment boundary. The design is such that the PHT pumps are inside containment with the pump motors outside, the resulting containment boundary being the pump seals. This was done to allow changing of the pump motors with the reactor at reduced power at the same time reducing the radiation fields to workers involved in the task. Other modifications from the Pickering design were also included with the aim of reducing radiation doses during maintenance. This objective was achieved but the removal of these systems from containment has added some complexity to the safety case. However, the benefit from doing this was real radiation dose saved versus potential doses which might result from accident situations, should they arise. Bruce power continues to support the design requirements outlined in this paragraph and any significant new change (e.g., enriched fuel bundles with burnable poison) will undergo significant testing prior to any decision regarding installation. For any new design, the process to be followed is defined in Design Management procedure [BP-PROC-00335, R006] and it shows that the required objectives are achieved as discussed earlier.</p> <p>The original design requirements for the 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</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
		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 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"> • resolution of applicable safety issues from existing reactor designs • improvements in design due to advances in materials and their properties • improved methods of design and safety assessment • improved methods of construction and fabrication • improvements in reliability, operability and maintainability • improved methods to mitigate the occurrence and consequences of human error • improved methods in support of ALARA 	<p>There are no changes introduced in this clause.</p> <p>As documented in [BP-PROG-01.06], 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 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</p>	C

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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"> IAEA Safety Guide Series NS-G-2.11, A System for the Feedback of Experience from Events in Nuclear Installations, Vienna, 2006. 	<p>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]. 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 plans 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, 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>There are no changes in the requirements.</p> <p>As discussed in BP-PROC-00363, 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 Assessment process integrates safety analysis, probabilistic risk assessment and criticality safety evaluations.</p> <p>BP-PROC-00335, Design Management and BP-PROC-00363, 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,</p>	C

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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>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"> • defence in depth • safety margins • multiple barriers • safety analysis (including both deterministic and probabilistic approaches), as well as overall scope, approach, safety criteria, uncertainty and sensitivity analysis, use of computer codes, <p>and use of operating experience</p> <ul style="list-style-type: none"> • radiation risks • safety functions • site characteristics • radiation protection 	<p>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 should also be used to establish and validate operating specifications and limits, normal and off-normal operating procedures, maintenance and inspection requirements, and normal and emergency procedures. The Safety Analysis will be 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, Design Verification. Several levels of review may take place, depending upon the significance of the design change being proposed.</p> <p>Peer (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 (if required) is a verification method that is less formal and more flexible in scope, timing, conduct, review and documentation than a formal design review. A technical review is held to confirm that an activity or condition meets specified design requirements.</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> engineering aspects human factors long-term safety <p>The independent peer review should be performed by suitably qualified and experienced individuals.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> IAEA, GSR Part 4, Safety Assessment for Facilities and Activities, Vienna, 2009. 	<p>Formal Design 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 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 design 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.</p> <p>As described before, the SOE program ensures that the operation, maintenance and management that are important to safety. Bruce A PROL and LCH, "identify requirements for the establishment and maintenance of SOE. The program is established based on the guidance of COG-02-901 P&G on the definition, Implementation and maintenance of SOE consistent with CSA N290.15-10 requirements.</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, R015]. 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, Preparation and Maintenance of SOE Requirements, and DPT-RS-00015, 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	<p>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, ageing management, modification and eventual decommissioning of the NPP.</p> <p>The design documentation shall include:</p>	<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 A Safety Report. 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</p>	C


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	1. design description 2. design requirements 3. classification of SSCs 4. description of plant states 5. security system design, including a description of physical security barriers and cyber security programs 6. operational limits and conditions 7. identification and categorization of initiating events 8. acceptance criteria and derived acceptance criteria 9. deterministic safety analysis 10. probabilistic safety assessment (PSA) 11. hazard analysis	<p>for modifications are prepared according to BP-PROG-10.02. 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>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 to support safe operation and RD-310 implementation. A report "Derived Acceptance Criteria for Deterministic Safety Analysis" (COG-13-9035) documenting the derived acceptance criteria to be applied to deterministic safety analysis of postulated accidents is drafted and currently under industry review. The report will be submitted to CNSC upon completion. Further details are given in Safety Factor 5.</p> <p>Section 2.1, Identification of Initiating Events, of Part 3 of the 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. 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>The design documentation follows well established processes and procedures as described in Design Documentation [BP-PROC-00335, R006]. 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</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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</p> <p>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"> • CNSC, RD/GD-369, Licence Application Guide: Licence to Construct a Nuclear Power Plant, Ottawa, Canada, 2011. • CNSC, REGDOC-2.4.1, Deterministic Safety Analysis, Ottawa, Canada, 2014. 	<p>into the design. Under the Equipment Reliability Program, BP-PROG-11.01, 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 BP-PROC-00400 "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>A general description of the plant design is provided in Part 1 of the Safety Report. Plant components and systems are described in Part 2 of the Safety Report. 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 A Probabilistic Risk Assessment (PRA) includes Level 1 and Level 2 analyses. The Bruce A PRA model, abbreviated as BAPRA, is the result of a continuing process of updates and improvements that began in 2003 with the development of the original BAPRA model version BAPRA16B C6798/TR/005 Ver0. A full summary of the changes made to the BAPRA model since its inception is provided in Appendix F of the year 2014 version of the Level 1 At-Power Internal Events NK21-03611.1 P NSAS Ver00. The list of current Bruce PRA analyses and corresponding guides is presented in Safety Factor 6.</p> <p>The Bruce A design documentation does include Hazard Analysis. The detailed hazard analysis of protection against fire is generated as per DPT-PDE-00027, DPT-PDE-00028 and DPT-PDE-00029, and is documented in NK21-REP-71400-00003, NK21-REP-71400-00004 and NK21-REP-71400-00005. Seismic margin in the event of earthquake is generated as per DPT-PDE-00017, and is assessed in NK21-REP-20091-00001.</p> <p>Other internal and external hazards are assessed in RABA-0601 (Enclosure 5 to NK21-CORR-00531-04059). Additional information is provided in Section 9.3 Hazard Analysis. Detailed assessments related to hazards analysis are documented in Safety Factor 7.</p> <p>The assessment of CNSC REGDOC-2.4.1 is documented in Safety</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
		Factor 5.	
6.	Safety requirements	This is not a requirement/guidance clause (this is a title only).	NA
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 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</p>	<p>The introductory paragraph to this clause is new and requires independence of the levels of defence in depth.</p> <p>As presented of the Safety Report 6.1.2 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002] 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 A provides the layers of defence against the release of fission products to the environment as described in Section 2 above. These include:</p> <ul style="list-style-type: none"> • The uranium dioxide (UO₂) fuel, which contains almost all the radioactivity, is a ceramic with high melting point sealed in a corrosion resistant metallic cladding; • The zirconium alloy fuel element sheath which has been demonstrated over thirty years to have a very low failure rate • The Heat transport system designed to high quality; • The sub-atmospheric Containment System designed to retain a large fraction of any fission products released from the heat transport system following an accident; • The Filtered Air Discharge System to remove particulates and 	Gap

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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>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. 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</p>	<p>iodine from controlled release following repressurization of containment;</p> <ul style="list-style-type: none"> 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. <p>The Bruce A 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. In regard to item (3), the ECI or moderator systems are capable of maintaining the integrity of the Heat Transport system (barrier 3) for all design basis accidents.</p> <p>As indicated in the compliance assessment against CNSC 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>facilities, and plans for onsite and offsite emergency response.</p> <p>Guidance</p> <p>IAEA INSAG-10, Defence in Depth in Nuclear 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"> • 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. • 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). • 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 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. 		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> The design (e.g., in safety design guides, management system programs) should provide: <ul style="list-style-type: none"> levels of defence in depth that are addressed by individual SSCs supporting analysis and calculation evaluation of operating procedures The safety analysis should demonstrate that the challenges to the physical barriers do not exceed their physical capacity. The structure for defence in depth provisions at each level of defence should be established 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 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. Special attention should be given to the feasibility of a given provision and the existence of supporting safety analyses. Deficiencies in the completeness of the supporting safety analyses should be documented and flagged as issues to be queried. <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</p>		




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	DECs ensures the independence of the fourth defence level.		
6.1.1	<p>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> <p>To the extent practicable, the design shall prevent:</p> <ol style="list-style-type: none"> challenges to the integrity of physical barriers failure of a barrier when challenged failure of a barrier as a consequence of failure of another barrier the possibility of failure of engineered barriers from errors in operation and maintenance that could result in harmful consequences <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>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 minimum acceptable states for those components or subsystems as credited in the safety analyses. Therefore, the minimum allowable performance standards shall be defined for each system and shall be listed or referenced in the Safety Report and in the Operating Policies and Principles for the plant.)</p> <p>The Bruce A OP&Ps state the following in regard to safety related systems: A safety related system, or portion thereof, shall be available whenever the reactor units are in a state where the system is required to provide its safety related function as credited in the Safety Report and subsequent analyses, unless one of the following conditions exists:</p> <ol style="list-style-type: none"> Alternatives, as noted below, ensure that no significant increase in public risk results from removing the system from service: <ol style="list-style-type: none"> An alternate system for the safety related system, as specified within the Operating Policies & Principles, is available while the safety related system is unavailable. Alternate conditions, as specified within the Operating Policies and Principles, make it acceptable for the safety related system to be unavailable. Compensating measures, established in procedures approved by the Vice President, Bruce A Operations Division ensure that the unavailability of the system does not result in a significant increase in the assessed public 	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
		<p>risk as stated in current licensing submissions.</p> <p>2. Vice President, Bruce A Operations Division approval and CNSC concurrence shall be obtained prior to removing a safety related system from service if its removal from service could result in a significant increase in the assessed public risk as stated in current licensing submissions.</p> <p>Regulating System Availability: No portion of the regulating system shall be removed from service unless the ability to control bulk reactor power is not affected or the reactor has been placed in a guaranteed shutdown state. If the regulating system is impaired, such that it cannot control bulk reactor power, the reactor shall promptly be placed in a guaranteed shutdown state. If the stepback or setback functions of the regulating system are impaired, and repairs cannot be made promptly, specific approval of the Vice President, Bruce A Operations Division shall be obtained for continued reactor operation.</p> <p>The rules for removing safety related systems for non-power operation are given in the OP&Ps.</p> <p>Human Factors Engineering Program Plan [DPT-PDE-00013, R008] provides direction in implementing Human Factor processes into changes performed under the Design Change Package procedures (BP-PROC-00539). 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 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. 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</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
		<p>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. As per BP-PROC-00539, all design change packages (DCPs) require at least a cursory level of HF involvement.</p> <p>The list of internal initiating events is presented in Table 2-1 of Part 3 of the 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).</p>	
6.2	<p>The NPP design shall provide adequate means to:</p> <ol style="list-style-type: none"> maintain the plant in a normal operational state ensure the proper short-term response immediately following a PIE facilitate the management of the plant in and following DBAs and DEC's 	<p>New requirements for DEC's and shielding considerations are added to this clause.</p> <p>The Bruce A design incorporates control systems and special safety systems that meet the requirements as documented in [RABA 0804].</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 [NK21-SR-01320-00002 Rev. 005]). Under certain transient conditions, if the reactivity range of the liquid zone controllers is exceeded, then further control via the regulating system is 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</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The following fundamental safety functions shall be available in operational states, DBAs and DECAs, except where the postulated accident involves a loss of that function:</p> <ol style="list-style-type: none"> 1. control of reactivity 2. removal of heat from the fuel 3. confinement of radioactive material 4. shielding against radiation 5. control of operational discharges and hazardous substances, as well as limitation of accidental releases 6. monitoring of safety-critical parameters to guide operator actions <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>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 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 A. At the time Bruce A was constructed these systems were identified based on experience in the design and</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>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 A are listed in the Safety Related Systems list [BP-PROC-0169, R0002].</p> <p>An Assessment of Systems Important to Safety for the Safety & 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 & Licensing portion of the Nuclear Asset Management Program.</p> <p>Systems Important to Safety (SIS) Decision Methodology [DPT-RS-00012, R001] describes the methodology and process involved in determining which station systems are Systems Important to Safety.</p>	
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"> 1. inherent safety features 2. passive safety features 3. specified procedural actions 4. action of control systems 	<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 1.3.1 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 spent fuel bay 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. 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 fuelling results in a reactor with very</p>	IC


 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>5. action of safety systems</p> <p>6. action of complementary design features</p>	<p>low reactivity control requirements and very low excess reactivity capacity, i.e., the capacity to add additional reactivity is physically limited.</p> <p>As described in Part 2, Section 1.3 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"> 1. The UO₂ fuel pellets, which bind the majority of radioactive fission products within the solid matrix. 2. The fuel sheath, which contains fission products not retained in the fuel matrix. 3. The heat transport system boundary, which contains any leakage from the fuel sheath. 4. The containment building, which contains any release from the heat transport system. 5. The exclusion zone surrounding the facility, which provides for dilution of any release from containment. <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 utilize gravity and pressure for activation) at Bruce A 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 A Abnormal Incidents Manual [NK21-OM-09034, Rev.113].</p> <p>It is recognized that there are no complementary design features at Bruce A original design to respond to management of severe accidents. In preparing the SAMGs, all systems that are available will be used for the recovery, some of them under conditions not normally envisaged for those systems. Thus, there are no systems specifically classified as "complementary design features"; therefore this is a</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
		design gap. Bruce Power is addressing the need for additional complementary design features through evaluations and potential design improvements as part of Fukushima Action Items. 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.	
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 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</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. DEC's 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). 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. 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</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>DBAs, and potential releases into the environment for DECs.</p> <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"> • CNSC, G-129, rev. 1, Keeping Radiation Exposures and Doses "As Low as Reasonably Achievable (ALARA)", Ottawa, Canada, 2004. • 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. 	<p>improved station design that contributed significantly to the reduction of both collective and individual dose expenditures.</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 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 Bruce A Units 1, 2, 3, and 4 to provide additional hydrogen mitigation capability.</p> <p>Bruce A PARs project is required 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>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
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"> 1. evacuation needs 2. land usage needs 3. security requirements 4. environmental factors <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 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>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 [NK21-SR-01320-00001, Rev. 005], the Bruce A Section includes part of a 914 m (3,000 ft) exclusion zone surrounding the Bruce A powerhouse structure. 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 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>	C



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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 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</p>		




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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, 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"> the site selection and threat assessment report facility robustness against natural and human induced external hazards (including malevolent acts) the capability of the onsite security program, along with any offsite security resources that will supplement the onsite security program <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> <p>Environmental factors</p>		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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"> • CNSC, RD-346, Site Evaluation for New 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"> 1. access routes for normal operational actions and maintenance 2. access control to minimize radiation exposures 	<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 A design includes some considerations of hazards; however as discussed later on of Clause 9.3 it is recognized that the list is not complete. As presented in Section 3 of Part 2 of the Safety Report [NK21-SR-01320-00002, Rev. 005] 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</p>	IC

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>3. actions taken in response to internal or external events</p> <p>4. egress routes</p> <p>5. movement of hazardous substances, nuclear materials, and radioactive materials</p> <p>6. movement of authorized and unauthorized personnel</p> <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>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. 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 has the station close to the lake with the nuclear portion of the station and the vacuum building facing north. 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 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 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</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 is expanding 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"> 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 	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	resources (personnel, equipment and consumable resources) would need to be shared among several units. These challenges should be identified and the available resources and mitigation strategies shown to be adequate.	<p>completed.</p> <p>2. Secondly, 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 are targeted for completion by December 2015.</p> <p>A model for severe accidents with multi units is to be considered within SAMG program. 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>Options for enhancing the ability of containment to accommodate severe accidents in multiple units are investigated. The ongoing analysis involves numerous multi-unit event combinations with various credits for mitigating actions and systems. The analysis includes an evaluation of the benefits and practicality of installing passive filtered venting, including a RIDM-based assessment. Bruce Power is considering 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. The bypass tees would be installed during the next scheduled containment outages at each station. The purpose of the bypass line and isolation valves is to allow containment filtered venting system to be installed at a later date without the need for an additional containment outage. A decision regarding the installation of a passive filter will be provided to the CNSC by December 16, 2015.</p> <p>Bruce Power Nuclear Emergency Response Plan [BP-PLAN-00001, R004] 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.</p> <p>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</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
		emergency response and mitigation techniques.	
7.	General Design Requirements	This is not a requirement/guidance clause (this is a title only).	NA
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"> 1. safety function(s) to be performed 2. consequence(s) of failure 3. probability that the SSC will be called upon to perform the safety function 4. the time following a PIE at which the SSC will be called upon to operate, and the expected duration of that operation <p>SSCs important to safety shall include:</p> <ol style="list-style-type: none"> 1. safety systems 	<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] 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]. 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>As discussed in [RABA 0804] the Bruce A 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</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2. complementary design features</p> <p>3. safety support systems</p> <p>4. other SSCs whose failure may lead to safety concerns (e.g., process and control systems)</p> <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 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"> • review and definition of PIEs • grouping and identification of bounding PIEs • identification of plant-specific safety functions to prevent or mitigate the PIEs 	<p>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 the control or safety systems.</p> <p>Bruce Power performed an Assessment of Systems Important to Safety for the Safety & 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 & Licensing portion of the Nuclear Asset Management Program.</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> • safety categorization of the safety functions, in accordance with their safety significance and role in achieving fundamental safety functions • identification of SSCs that provide the safety functions • assignment of SSCs to a safety class corresponding to the safety category • verification of SSC classification • identification of engineering design rules for classified SSCs <p>This approach should be used for all SSCs including pressure retaining components, electrical, instrumentation and control (I&C) and 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</p>		


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>that the safety functions belonging to the subsequent level of defence in depth remain functional.</p> <p>Some specific SSCs classification guidelines are given below:</p> <ul style="list-style-type: none"> SSCs whose failure cannot be accepted because the failure will result in unacceptable consequences with certainty should be allocated to the highest safety class. 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. 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. 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. 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 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>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</p>		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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	The design authority shall establish the plant design envelope, which comprises all plant states considered in the design: normal operation, AOOs, DBAs and DEC's, as shown in figure 1.	<p>The requirement is changed to include DEC's.</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</p>	IC

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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>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>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;</p>	<p>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] 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 [BP-PROG-00.04]</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 are being investigated. The analysis involves numerous multi-unit event combinations with various credits for mitigating actions and systems. The analysis includes an evaluation of the benefits and practicality of installing passive filtered venting, including a RIDM-based assessment. Bruce Power is considering the installation of containment bypass tees and containment boundary valves into the existing EFADs piping where it exits the Vacuum</p> <p>Building and Pressure Relief Valve (PRV) manifold at Bruce A and B. The bypass tee would be installed during the next scheduled containment outages at each station. The purpose of the bypass line and isolation valves is to allow containment filtered venting system to be installed at a later date without the need for an additional containment outage. A decision regarding the installation of a passive filter is expected by December, 2015.</p> <p>Bruce Power is implementing design changes to improve severe accident response. For example Passive Autocatalytic Recombiners</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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's.</p> <p>The design principles for complementary design features to deal with DEC's 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>(PARs) have been installed in Bruce A Units 1, 2, 3, and 4 to provide additional hydrogen mitigation capability. Bruce A PARs project is required 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 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 [NK21-CORR-00531-10963] 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>As part of the Station Improvement Plan (Letter, F. Saunders to M. Leblanc, "Application for the Renewal of the Power Reactor Operating Licence for Bruce Nuclear Generating Station A", October 31, 2013, NK21-CORR-00531-10873), procurement of 400 kW generators was completed in 2012. Installation of electrical receptacles to provide power to U1/2/3/4 reactors, Unit 0 and EFADS has also been completed, including commissioning.</p>	
7.3	<p>Plant states considered in the design shall be grouped into the following four categories:</p> <ol style="list-style-type: none"> 1. Normal operation is an operation within specified OLCs, including start-up, power operation, shutting down, shutdown, maintenance, testing, and refuelling. 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 	<p>The requirements in this clause are modified with the introduction of the DEC's are defined in item 4.</p> <p>As presented in [RABA 0804], the basis on which Bruce A was 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</p>	Gap

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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 DECs. 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 DECs.</p>	<p>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. A complete listing of both the setback and stepback parameters is given in Table 3-2 and Table 3-3 of Appendix 3 Control Failures of Part 3 of the Safety Report. These transients generally have a frequency higher than 10E-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 & NK21-CORR-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 A. 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>Bruce Power is implementing a Safety Report Improvement Program starting in 2014 including annual status and progress updates to the</p>	


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design should include the following:</p> <ul style="list-style-type: none"> 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) key parameters and characteristics for operational states, including nominal values and deviations due to uncertainties and settings of instruments, controls, trips, equipment action time, or due to process fluctuations 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 methods of transferring the plant between different operating configurations final safe configurations after AOOs, DBAs, and DECAs 	<p>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, dated November 20, 2013, File: NK21-CORR-00531-10774 & NK21-CORR-00531-11155.</p> <p>A summary of the acceptance criteria applied to Bruce Power accident analysis are provided in Section 1.5 of Part 3 of the Safety Report [NK21-SR-01320-00003, Rev. 004]. 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/DECAs in CNSC REGDOC-2.5.2.</p>	
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</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 Abnormal Incidents Manual [NK21-OM-09034, Rev.113]. 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</p>	C


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>safe normal operation, including:</p> <ol style="list-style-type: none"> limits important to safety constraints on control systems and procedures plant maintenance, testing, and inspection requirements to ensure that SSCs function as intended, taking the ALARA principle into consideration 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 <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>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</p>	<p>align with the modern requirements.</p> <p>Operating limits, including those for Normal Operation, are specified in the OP&P. Further discussion regarding Safe Operating Envelope is presented in Clause 4.3.3.</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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"> • normal reactor start-up (from shutdown, through criticality, to full power) • power operation, including full-power and low-power operation • changes in reactor power, including load-follow modes (if applicable) and return to full- power after an extended period at low-power • operation during transition between configurations such as reactor shutdown from power operation (hot shutdown, cool-down) • refuelling during normal operation, where applicable • shutdown in a refuelling mode or other maintenance condition that opens the reactor coolant or containment boundary • handling of fresh and irradiated fuel <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	The design shall include provisions such that releases to the public following an AOO do not exceed the dose acceptance	<p>There are no changes to the requirement</p> <p>A review of the same clause in RD-337 [NK21-CORR-00531-11005]</p>	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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>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</p>	<p>indicated that the Bruce A design does not fully meet this requirement. The licensing basis does not specify separate acceptance criteria for AOOs. The deterministic safety analysis provided in the Bruce A Safety Report [NK29-SR-01320-00001] 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 A, this would be the case, e.g., loss of control system functions. For some of the other scenarios, e.g., PHT pump seal failure, the public doses arise from incipient iodine in the HT system and from tritium in the D2O. Thus, repair of the seal would enable the reactor to continue operation. The doses from this event, as calculated in the Bruce A 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 2.11 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</p>	


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>deviations from normal operation can be detected, and that the control systems can be expected to return the plant to a safe state, 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"> • reactor power and its distribution • core component temperatures • fuel cladding oxidation, and deformation • pressures in the primary and secondary systems • containment parameters • temperatures and flows • reactivity coefficients • reactor kinetics parameters • reactivity worth of reactivity devices <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</p>	<p>Class IV power failure and pump seizure scenarios. Overpressure protection provided by each shutdown system acting alone has also 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 9.55 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>At Bruce A, as at all other CANDU stations 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 addressed as part of the Safety Report Improvement activities, as identified in previous sections.</p>	


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>requirements of the systems.</p> <p>Additional information</p> <p>Examples of AOOs may be found in:</p> <ul style="list-style-type: none"> CNSC, REGDOC-2.4.1, Deterministic Safety Analysis, Ottawa, Canada, 2014. 		
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 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</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 [NK21-SR-01320-00003, Rev. 004].</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 A reference dose limit documented in Part 3 of the Safety Report and Operating Policies and Principles – Bruce A [BP-OPP-00002, R012]. Bruce A meets this 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 A licence.</p> <p>As discussed in [RABA 0804] 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>	C

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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>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"> CNSC, REGDOC-2.4.1, Deterministic Safety Analysis, Ottawa, Canada, 2014. 	<ul style="list-style-type: none"> 15 minutes for actions in the main control room, and 30 minutes for actions outside the main control room. <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.</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 [NK21-OM-09034, Rev.113].</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</p>	<p>The first two paragraphs are substantially revised to include DECs.</p> <p>The original design of Bruce A lacks a systematic provision for severe accident mitigation. The source term as defined by the requirement was not used for the Bruce A design. As well, the original design has not provided for complementary design features to mitigate the</p>	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>additional failures.</p> <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 DECs. 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 DECs. This source term is referred to as the reference source term and shall be based on a set of representative core damage accidents 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 DECs.</p> <p>In the case of plants with multiple units at a site, the use of</p>	<p>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 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 DECs 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 will be 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 & NK21-CORR-00531-11155.</p> <p>Historically, DECs leading to severe accidents as defined in this clause have not been considered in the design. 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> <p>Bruce Power recognised the need for SAMGs to address multi-unit events including a station blackout. Update of SAMG and its implementation to address multi-unit events is ongoing. For example, options for enhancing the ability of containment to accommodate severe accidents in multiple units as follows:</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 DECs, consideration should be given to:</p> <ul style="list-style-type: none"> • factors of the accident progression (i.e., physical conditions, processes and phenomena) • BDBA (including severe accident) scenarios resulting from initiating events, human actions, and SSC operability (success or failure) • selection of bounding events that are considered in design and determination of limiting values and ranges of the parameters of these events <p>The design should identify the features that are designed for use in, or that are capable of preventing or mitigating events considered in DECs. These features include complementary design features and other SSCs that may be credited for DECs. These features should:</p> <ol style="list-style-type: none"> 1. be independent, to the extent practicable, of those used in more frequent accidents 	<ul style="list-style-type: none"> • The ongoing analysis involves numerous multi-unit event combinations with various credits for mitigating actions and systems. The analysis includes an evaluation of the benefits and practicality of installing passive filtered venting, including a RIDM-based assessment. • Bruce Power is considering the 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. The bypass tees would be installed during the next scheduled containment outages at each station. The purpose of the bypass line and isolation valves is to allow containment filtered venting system to be installed at a later date without the need for an additional containment outage. • A decision regarding the installation of a passive filter is expected by December 2015. <p>The implementation of SAMG for multi-unit events is being 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 IFB events in station operating documentation, is being assessed under the COG Severe Accident Joint Project JP-4426 and a plan and schedule for implementation into station-specific documentation is monitored. It is noted that demonstration of the effectiveness of SAMG using table-top exercises and drills has already been completed by Bruce Power for single unit events. Demonstration of the effectiveness of multi-unit SAMGs will also be assessed through table-top exercises and drills. The use of a simulation environment capable of training and testing procedures is also being considered for deployment at Bruce Power.</p>	



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2. have a reliability commensurate with the function that they are required to fulfill</p> <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 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"> • use best-estimate models and assumptions • take credit for realistic system action and performance beyond original intended functions, including the potential use of safety, non-safety and temporary systems • take credit for realistic operator actions <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 considered. The</p>		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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">• if it is physically impossible for the condition to occur, or• if the condition can be considered with a high degree of confidence to be extremely unlikely to arise <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">• The degree of substantiation provided for the demonstration of practical elimination should take account of the assessed frequency of the situation to be eliminated and of the degree of confidence in the assessed frequency.• 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.• 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;		




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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.</p> <ul style="list-style-type: none"> The necessary high confidence in low likelihood should, wherever possible, be supported by means such as: <ul style="list-style-type: none"> multiple layers of protection application of the safety principles of independence, diversity, separation, redundancy use of passive safety features use of multiple independent controls It should be ensured that the practical elimination provisions remain in place and valid throughout the plant lifetime; for example, through in-service and periodic inspections. <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</p>		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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> <p>Additional information</p> <p>Examples of BDBAs may be found in:</p> <ul style="list-style-type: none"> • CNSC, REGDOC-2.4.1, Deterministic Safety Analysis, Ottawa, Canada, 2014. 		
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</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> <ul style="list-style-type: none"> • Enhancement of SAMG to include multi-unit events and IFB events. • Assessment of instrument and equipment survivability under severe accident and identification of equipment upgrades required. • Assessment of plant habitability under severe accident conditions and identification of modifications required. • Improvement to understanding of severe accident phenomena including containment integrity, hydrogen production, aerosol behavior, and in vessel retention. <p>As discussed in [B-REP-00701-09DEC2013-060] Bruce Power is implementing short-term and long-term provisions to provide make up</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>severe accident 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>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</p>	<p>to critical systems. The short-term provisions are as follows:</p> <ol style="list-style-type: none"> (1) Modifications to allow emergency water to be added to the SGs via Emergency Boiler Cooling (EBC) system at Bruce A and the Emergency Water System (EWS) at Bruce B have been completed in all units. (2) The design of an alternate method of providing makeup water to the SGs using the Inter Unit Feedwater Ties (IUFT) is complete. (3) 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>As documented in Bruce Power Progress Report No. 4 on CNSC Action Plan - Fukushima Action Items, [NK21-CORR-00531-10963] 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. For example as per the Station Improvement Plan (Letter, F. Saunders to M. Leblanc, "Application for the Renewal of the Power Reactor Operating Licence for Bruce Nuclear Generating Station A", October 31, 2013, NK21-CORR-00531-10873), procurement of 400 kW generators was completed in 2012. Installation of electrical receptacles to provide power to U1/2/3/4 reactors, Unit 0 and EFADS has also been completed, including commissioning [as documented in supporting documentation for NK21-CORR-00531-11567]. These electrical modifications allow for a quick connection of portable generators to back feed into the Qualified Power Supply (QPS) at Bruce A. This modification allows key instrumentation and control equipment to remain operable for an indefinite period of time.</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</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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>In addition, evaluations should be carried out on the capability of complementary design features to cope with DECs. 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>accident, options for enhancing the ability of containment to cope with severe accidents have been explored. The ongoing analysis involves numerous multi-unit event combinations with various credits for mitigating actions and systems. The analysis includes an evaluation of the benefits and practicality of installing passive filtered venting, including a RIDM-based assessment.</p> <p>As discussed in Part 2, Section 6.4 of the Safety Report, Passive Autocatalytic Recombiners (PARs) have been installed in Bruce A Units 1, 2, 3, and 4 to provide additional hydrogen mitigation capability. Bruce A PARs project is required 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>	




Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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> <ul style="list-style-type: none">• corium stratification• thermal-chemical interaction between corium, steel components and vessel• heat transfer from corium to vessel or end-shield• hydrogen burn• steam explosion due to molten fuel-coolant interaction• corium-concrete interaction <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> <p>Additional information</p>		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Additional information may be found in:</p> <ul style="list-style-type: none"> CNSC, RD-327, Nuclear Criticality Safety, section 16 - Nuclear Criticality Accident <p>Emergency Planning and Response, Ottawa, Canada, 2010.</p>		
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>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>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.</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 recognised the need for SAMGs to address multi-unit events including a station blackout. Update of SAMG and its implementation to address multi-unit events is ongoing.</p>	Gap




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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> <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>		

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> CNSC, REGDOC-2.4.1, Deterministic Safety Analysis, Ottawa, Canada, 2014. 		
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, 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> <ul style="list-style-type: none"> leaks and breaks in pressure-retaining components flooding by water from neighbouring buildings spurious actuation of the fire-fighting system overfilling of tanks failures of isolating devices 	<p>A new requirement for internal events to be identified and AOOs, DBAs and DECAs to be determined from these events is 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 7.4.1 (Gap).</p> <p>A systematic identification of internal hazards in accordance with current expectations has not been performed for the Bruce A 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 A 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 CNSC has accepted the results of the Pipe Whip and Jet Impingement Assessment of Piping Inside the Reactor Vault. The results of the assessment concluded that no design changes are required in the Units 1 and 2 vaults as a result of pipe-whip or jet impingement.</p> <p>The original design of Bruce A 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 as part of an on-going project to implement the CNSC Regulatory Standard S-294 in support of the operating licence renewal in 2014 [NK21-CORR-00531-11005].</p> <p>A Fire Safe Shutdown Analysis has been performed for Bruce A [NK21-REP-71400-00004], to ensure safe design in case of fire events. In addition, a Fire Hazard Analysis and Fire Code Compliance Reviews [NK21-REP-71400-00005] have also been prepared. Bruce Power has already completed a PRA Guide - "Phase 1 Fire PRA Guide" [B-REP-03611-00008].</p> <p>Section 2.5.2 of Part 2 of the Safety Report [NK21-SR-01320-00002]</p>	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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"> • a realistic assessment is made of the postulated missile size and energy, and its potential trajectories • potentially impacted components associated with systems required to achieve and maintain a safe shutdown state are identified • a loss of these potentially impacted components is evaluated to determine if sufficient redundancy remains to achieve and maintain a safe shutdown state <p>The civil design takes into account loads generated by internal hazards in the environmental loading category consistent with section 7.15.</p>	<p>indicates that a feature incorporated into the Bruce A design provides an adequate level of protection against any credible turbine generator missile is the separation of the 600 V Class II switchgear, such that a single missile cannot disable both halves of the system.</p>	
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</p>	<p>There are no changes to the requirement</p> <p>The change introduced in CNSC REGDOC-2.5.2 is minor, i.e., 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, 1965. The design weather data selected for Bruce A site are presented in Table 2.1-l. Chapter 2 of the Safety Report [NK21-01320-00002, Rev.005].</p> <p>Loads and loading combinations, considered for the design of the containment structures are summarized in Chapter 2 of Part 2 of the Safety Report,</p> <p>A Seismic Margin Assessment [NK21-REP-20091-00001, Rev.2] has been completed for Bruce A in support of restarting Units 3 and 4. The Review Level Earthquake (RLE) for the assessment was characterized by a Uniform Hazard Spectrum (UHS) with a</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>evaluation, such as potential aircraft crashes, ship collisions, and terrorist activities.</p> <p>Guidance</p> <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"> • site-specific hazard evaluation for external hazards (of human or natural origin) • design assumptions or values, in terms of recurrence probability of external hazards • definition of the design basis for external hazards • collection of site reference data for the plant design (geotechnical, seismological, hydrological, hydrogeological and meteorological) • evaluation of the impact of the site-related issues to be considered in the application, concerning emergency preparedness and accident management • arrangements for the monitoring of site-related parameters throughout the life of the plant <p>Natural external hazards other than earthquakes may be categorized as:</p> <ul style="list-style-type: none"> • hazards that have potential to damage SSCs important to safety 	<p>recurrence period of 10,000 years. The Bruce A RLE is characterized as the 84th percentile per annum probability of exceedance (10,000 year recurrence) UHS. The Bruce A RLE accommodates various interpretations of regional geology and seismicity in terms of representing historical data and known or potentially seismogenic features, and uses various interpretations of ground-motion estimation in eastern North America. The report describes the seismic margin assessment performed in order to demonstrate the successful operation and survival of the components and structures necessary to bring the plant to a safe hot or cold shutdown and maintain that condition for 72 hours. The principal systems in the success path and the method used to identify these systems are described as well as a success path equipment list was compiled to identify the specific mechanical and electrical equipment required to maintain seismic integrity of the success path.</p> <p>As summarized in [B-REP-00701-09DEC2013-060] review of the basis for external events against modern state-of-the-art practices for evaluating external events magnitudes and relevant design capacity for these events was recommended in order to strengthen reactor defence-in-depth. The Bruce Power Probabilistic Risk Assessment (PRA) external hazards analysis involved a screening analysis that was completed in September 2012. As a result of the screening, seven hazards were determined to require further assessment</p> <ul style="list-style-type: none"> • High/Low Ambient Air Temperature • Lightning • Toxic/Chemical/Radiological Release • Turbine Generated Missiles • Transportation Accidents • External Flooding • Tornadoes/High Winds <p>Analysis to assess the impacts of these unscreened events is underway. Bruce Power is implementing a Safety Report Improvement Program starting in 2014 including annual status and progress updates to the CNSC staff. The activities related to upgrade of the Safety Report, the schedule and program organization and interfaces are presented in Planning Basis for Safety Report</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> hazards that are evaluated and screened out <p>Natural external hazards considered in the design process should include:</p> <ul style="list-style-type: none"> earthquakes extreme meteorological conditions of temperature, snow, freezing rain, hail, frost, subsurface freezing and drought 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 cyclones (e.g., hurricanes, tornadoes) and straight winds abrasive dust and sand storms lightning volcanoes (site is sufficiently remote from volcanoes) biological phenomena collision of floating debris (e.g., ice, logs) with accessible safety-related structures, such as water intakes and ultimate heat sink components geomagnetic storm (solar flare and electromagnetic pulses) combinations of extreme weather conditions that could reasonably be assumed to occur at the same time <p>Natural external hazards that are evaluated and screened out may be based on the following criteria:</p>	<p>Improvement at Bruce A and B [NK21-CORR-00531-10774/NK29-CORR-00531-11155]. The implementation of these activities is tracked under Action Item 090739 [NK21-CORR-00531-07548/NK29-CORR-00531-08524].</p> <p>The requirements related to plane crash and terrorist activities are not addressed in this assessment due to the sensitivity of information.</p>	



Rev Date: July 8, 2016


Status: Issued

Subject: Safety Factor 1 - Plant Design


File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> a phenomenon that occurs slowly or with adequate warning with respect to the time required to take appropriate protective action a phenomenon which in itself has no significant impact on the operation of an NPP and its design basis an individual phenomenon which has an extremely low probability of occurrence the NPP is located sufficiently distant from or above the postulated phenomenon (e.g., fire, flooding) 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) <p>Human induced hazards considered in the design process should include:</p> <ul style="list-style-type: none"> aircraft crashes (general aviation) 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 release of hazardous gases (asphyxiant, toxic) from offsite and onsite storage release of corrosive gases and liquids from offsite and onsite storage release of radioactive material from offsite sources 		

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> • fire generated from offsite sources (mainly for its potential for generating smoke and toxic gases) • collision of ships or floating debris with accessible safety-related structures, such as water intakes and ultimate heat sink components • collision of vehicles at the site with SSCs • electromagnetic interference from off the site (e.g., from communication centres and portable phone antennas) and on the site (e.g., from the activation of high voltage electrical switchgear and from unshielded cables) • 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) <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 DECs.</p> <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> • American Nuclear Society (ANS), 2.3, Estimating Tornado, Hurricane, and Extreme Straight Line Wind Characteristics at Nuclear Facility Sites, La Grange Park, Illinois, 		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2011.</p> <ul style="list-style-type: none"> CNSC, RD-346, Site Evaluation for New Nuclear Power Plants, Ottawa, Canada, 2008. IAEA, NS-G-3.1, External Human Induced Events in Site Evaluation for Nuclear Power Plants, Vienna, 2002. National Research Council (NRC), National Building Code of Canada, Ottawa, Canada, 2010. 		
7.4.3	<p>Combinations of randomly occurring individual events that could credibly lead to AOOs, DBAs, or DEC's 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 DEC's, depending on their likelihood of occurrence.</p>	<p>The change in this clause is minor and does not affect the requirement, i.e., "DEC's" replaces "BDBAs".</p> <p>As documented in [RABA 0804], when Bruce A was 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 A 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 & NK21-CORR-00531-11155</p>	IC
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</p>	<p>A new requirement for design limits related to DEC's is introduced.</p> <p>As discussed in [RABA 0804], all of the SSCs important to safety have been in place at Bruce A 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>	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>states, DBAs and DEC.</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 DEC.</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"> identified codes and standards conservative safety margins reliability and availability: material selection single-failure criterion redundancy separation diversity independence fail-safe design equipment qualification: environmental qualification 	<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 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; hence this is identified as a gap (Gap).</p>	




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> • seismic qualification • qualification against electromagnetic interference • operational considerations: • testability • inspectability • maintainability • aging management • management system <p>The design of complementary design features 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	Bruce A uses the reliability program described in BP-PROG-11.01 and in the hierarchy of its implementing procedures (listed in	AD

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>analysis shall be performed for each of these SSCs.</p> <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 10E-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>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</p>	<p>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 a probabilistic unavailability models of SIS. The ongoing record of reliability of SIS is documented in Annual Reliability Reports. The 2013 Annual Reliability Report NK21-REP-09051.1-00011 contains detailed results on the Bruce A systems that comprise the SIS list. Quantitative unavailability models exist for eight 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 A Annual Reliability Report NK21-REP-09051.1-00011, out of the eight 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 three SIS are higher. Namely, the target for the Standby Class 3 Power System is 60E-03, the target for the Qualified Power System is 10E-03, and that for the Heating, Ventilation and Air Conditioning System is also 10E-03. Except for the Standby Class 3 Power System, the calculated unavailabilities for all systems meet their respective Bruce Power targets.</p> <p>Corrective actions to bring the predicted future unavailability of the Class 3 Power System back to within target are being managed through the Bruce Power Corrective Action Program. As stated in the 2013 Annual Reliability Report NK21-REP-09051.1-00011, Station Condition Record (SCR) #28290623 was initiated with corrective actions to address the over target predicted future unavailability for the standby Class 3 power system. The corrective actions include</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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"> the plant is designed, constructed, and operated in a manner that is consistent with the assumptions and risk importance of these SSCs these SSCs do not degrade to an unacceptable level during plant operations the frequency of transients posing challenges to SSCs is minimized these SSCs function reliably when challenged <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 evaluate the reliability of SSCs.</p>	<p>validating the modelling assumptions, updating the Class 3 unavailability model if required and optimizing the testing program to reduce the unavailability.</p> <p>The calculated unavailabilities of three SIS are above the value 1E-03 value required in this Clause. These are: 85.3E-03 for the Standby Class 3 Power System, 7.54E-03 for the Qualified Power System, and 1.47E-03 for the Heating, Ventilation and Air Conditioning System. 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 the Clause.</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
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 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"> 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. 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, 	<p>There are no changes that affect the requirements in this clause.</p> <p>A review of the same clause in a draft version of RD-337 indicated that the Bruce A design meets this requirement, as documented in [RABA 0804]. For example, the design considerations leading to full independence between the two shutdown systems as discussed in Part 2, Section 6.1.6 of the Safety Report [NK21-SR-01320-00002, Rev. 005] 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 SDS2 system does not provide trip coverage across the full spectrum of potential failures equal to that provided by SDS1. However, most accident cases are provided with dual parameter coverage on SDS2 as well as SDS1.</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 A 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. Channelization ensures that the three cable routes are separated, that the equipment associated with the three sets of channels is located in three different</p>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Washington, D.C., 2007.</p> <ul style="list-style-type: none"> U.S. NRC, NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, Washington, D.C., 1994. 	<p>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.</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"> redundant divisions of a safety system redundant divisions of a safety support system a safety support system and a process system 	<p>There are no changes in this clause that might impact the intent of the requirement.</p> <p>As discussed in Part 2, Section 6.1.4 of the Safety Report [NK21-SR-01320-00002] 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 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.</p> <p>Selected redundant equipment and their control systems/supplies are arranged in separated areas to minimize the probability of common</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>This shall apply to equipment and to the routing of items, including:</p> <ol style="list-style-type: none"> 1. electrical cables for power and control of equipment 2. piping for service water for the cooling of fuel and process equipment 3. tubing and piping for compressed air or hydraulic drives for control equipment <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> <ol style="list-style-type: none"> 1. A safety system designed to act as backup shall not be located in the same space as the primary safety system. 	<p>accidents affecting all systems.</p> <p>A review of the same clauses in RD-337 indicated that the Bruce A design does not fully meet this requirement, as documented in [NK21-CORR-00531-11005]. Bruce A original design has not systematically applied grouping and separation, as the philosophy was not developed at the time. Some retrofitting was undertaken after Bruce B was built, such as environmental qualification of essential equipment. The principle will be applied to future design changes, where practicable, as discussed in Section 7.6.1.</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 2.5.4 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 [NK21-MAN-03651-00001, Bruce A Environmental Qualification Room Conditions Manual]. The results of this program are documented in Environmental Qualification Requirements of Safety Related Systems and Structures for Bruce A [NK21-EQR-03651-00001].</p> <p>The Bruce A design includes protection against common mode events as described in Section 2.5 of Part 2 of the Safety Report. This includes:</p> <ol style="list-style-type: none"> 5. Seismic Qualification 6. Missile Protection 7. Protection Against Dynamic Effects Associated with the Rupture of Piping 8. Environmental Qualification of Safety-Related Equipment. <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. 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>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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>		
7.6.1.2	<p>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 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</p>	<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 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.</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,</p>	IC




Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>be a 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"> • design diversity • equipment diversity • functional diversity • human factor engineering diversity <p>The design for I&C systems should also consider:</p> <ul style="list-style-type: none"> • signal diversity • software diversity <p>For I&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>	<p>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 inspection 1.3.2.4 of Part 2 of the Safety Report). Similarly, backup independent air is supplied for pneumatic equipment when necessary.</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> different technologies different approaches within the same technology different architectures within the same technology <p>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.</p>		
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 systems.</p>	<p>This is a new requirement.</p> <p>As presented in Section 6.1.2 of the Bruce A Safety Report Part 2 [NK21-SR-01320-00002] 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



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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> <p>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.</p>		
7.6.2	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>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</p>	Gap




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>1. all failures caused by that single failure</p> <p>2. all identifiable but non-detectable failures, including those in the non-tested components</p> <p>3. all failures and spurious system actions that cause (or are caused by) the PIE</p> <p>Each safety group shall be able to perform the required safety functions under the worst permissible systems configuration, taking into 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>design does not fully meet this requirement, as documented in [NK21-CORR-00531-11005]. The application of the single failure criterion for the Bruce A 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).</p> <p>As part of the Bruce 1&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&2 ECI, QPS and the bleed condenser relief valves.</p> <p>The application of the 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.</p> <p>Bruce Power has identified and completed two corrective actions to address this gap:</p> <ol style="list-style-type: none"> 1. Connect QPS bus to Unit 2 Class III Power. 2. Disconnect motive power from 0-71310-MV1. <p>Bruce Power has confirmed that both of these actions have been completed for the Bruce 3&4 and Bruce 1&2 restart program.</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 that these components are available. 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>	


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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 maintained in service, and that remain unaffected by the PIE. Design documentation shall include justification 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 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 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"> • preferred action: the system or the test scheme should 	<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 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 A.</p> <p>As discussed in Part 2, Section 1.3 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</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>be redesigned to make the failure detectable</p> <ul style="list-style-type: none"> 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 <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 SFC, the following should be considered in order to demonstrate a high degree of performance assurance:</p> <ul style="list-style-type: none"> adequate testing during the manufacturing stage sample testing from those components received from the manufacturer adequate testing during construction and commissioning stages necessary testing to verify their reliability after the components have been removed from service during the operation stage <p>Any consideration for an exception to the SFC during testing and maintenance should fall into one of the following permissible categories:</p>	<p>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>Standby safety support systems, such as the standby emergency generators, are also tested regularly so that the system reliability can be tracked. 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
	<ul style="list-style-type: none"> the safety function is provided by two redundant, independent systems (e.g., two redundant, fully effective, independent cooling means) 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) 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) the loss of system redundancy has minor safety significance (e.g., control room air filtering) the loss of system redundancy may slightly increase PIE frequency, but does not impact accident progression (e.g., leak detection) <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> <ul style="list-style-type: none"> IAEA, Safety Series No. 50-P-1, Application of the 		


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Single Failure Criterion, Vienna, 1990.</p> <ul style="list-style-type: none"> 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. 		
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 alarms or another reliable indication.</p>	<p>There are no changes to this requirement.</p> <p>A review of the same clause in draft version of RD-337 indicated that the Bruce A design meets this requirement, as documented in [RABA 0804].</p> <p>As presented in Section 6.1.3 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 10E-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., a few containment boundary valves fail open following loss of instrument air leading to possible impairment of containment on end shield cooling post steam line break) 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 components such as air-operated valves are designed to be fail-safe to the extent possible. Self-actuating devices are employed where possible.</p>	Gap
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</p>	<p>There is no change in the requirements.</p> <p>A review of the same clause in a draft version of RD-337 indicated that the Bruce A design meets the intent of the requirements, as</p>	IC


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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>documented in [RABA 0804]. 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 10E-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. Numerous Safety System Tests (SSTs) have been devised to ensure that the systems meet these requirements. As established in Section 1.3 of Part 2 of the Safety Report the unavailability target of special safety systems is limited to less than 10E-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 formal regulatory reliability requirements, and the same principles for testing and maintenance are employed. These systems must be similarly reliable (typically 10E-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</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
		factored into their reliability calculations. The intent of the requirement is therefore met.	
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"> 1. the process and safety functions are not required or credited at the same time 2. 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 are required to mitigate the PIE are unaffected 3. the system is designed to the standards of the function of higher importance with respect to safety 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 5. the requirements for instrumentation sharing are met 	<p>There are no changes in the requirements.</p> <p>A review of the same clause in a draft version of RD-337 indicated that the Bruce A design meets the intent of this requirement, as documented in [RABA 0804].</p> <p>There is no sharing of safety and process systems. There is no instrumentation sharing between safety and process systems.</p>	IC
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</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 6.1.4 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>	IC

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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"> 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 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 3. an isolation device shall always be associated with the safety system and shall be classified and qualified accordingly 	<p>Neither of the two shutdown systems shares equipment with process systems. None of the safety systems shares equipment. Bruce A does not share any instrumentation between safety and process systems so this part of the requirement does not apply. The channelized logic at Bruce A 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 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	<p>SSCs important to safety shall typically not be shared between two or more reactors.</p> <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>The change introduced in item 1 relates to the safety requirements during DEC's.</p> <p>As review of the same clause in RD-337 indicated that the Bruce A design does not fully meet this requirement, as documented in [NK21-CORR-00531-11005]. 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</p>	IC

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>If sharing of SSCs between reactors is arranged, then the following requirements shall apply:</p> <ol style="list-style-type: none"> 1. safety requirements shall be met for all reactors during operational states, DBAs and DEC's 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) <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>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.</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>	
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</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>A review of the same clause in RD-337 indicated that the Bruce A design does fully meet this requirement, as documented in [NK21-CORR-00531-11005]. The Safety Report for Bruce A (NK21-SR-01320-00003, Rev. 004) 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 A. The effects of pipe whip and jet impingement are being addressed for Bruce A primarily by showing that any pipe leak</p>	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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 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-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-</p>	<p>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, the CNSC has accepted the results of the Pipe Whip and Jet Impingement Assessment of Piping Inside the Reactor Vault. The results of the assessment concluded that no design changes are required in the Units 1 and 2 vaults as a result of pipe-whip or jet impingement. 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 pressure HPECI system (H₂O injection valves outside containment, D₂O 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 A 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 A EQ Program [BP-PROC-00261] 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 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</p>	


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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>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</p>	<p>systems to detect incipient failures before they occur, 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>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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> <ul style="list-style-type: none"> o components in the means of shutdown o main coolant pumps o headers o emergency core cooling system components o steam generators o steam lines o turbine <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"> 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 of the proposed design and in-service inspection requirements. o No uncontrolled active degradation mechanism should 		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>exist in the piping system to be qualified for LBB.</p> <ul style="list-style-type: none"> 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. 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. 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. o The LBB evaluation should use design basis loads and, after construction, be updated to use the as-built piping configuration, as opposed to the design configuration. o The methodology should take account of potential for degradation by erosion, corrosion, and erosion-cavitation due to unfavourable flow conditions and water chemistry. 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>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>		


Article No.	Clause Requirement	Assessment	Compliance Category
	<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> <ul style="list-style-type: none"> o finite element modelling and analysis assumptions are checked to make sure they are justified and conservative o finite element mesh is properly refined to account for geometric structural discontinuities with proper element shapes and aspect ratios o loads and boundary conditions are correct and properly applied in the finite element models o load combinations and scale factors applied to unit load cases conform to design or load specifications o linearized stress results, obtained from load combinations, are compared with ASME code (or equivalent) allowable limits 		
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"> 1. the reactor can be safely shut down and kept in a safe shutdown state during and following AOOs and DBAs 	<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 2.5.4 of the Safety Report [NK21-SR-01320- 00002], 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</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2. residual heat can be removed from the reactor after shutdown, and also during and following 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 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 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,</p>	<p>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 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. 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 (NK21-EQR-03651-00001) and Safety Requirements Matrix (NK21-SRM-03651-00001) documents.</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</p>	

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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&C and certain post 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"> systems and equipment required to perform safety functions in a harsh environment, including their safety functions and applicable DBAs 	<p>general steps of the EQ process are described in Part 2, Section 2.5.4.2 of the Safety Report.</p> <p>A review of the same clause in RD-337 [NK21-CORR-00531-11005] 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 [B-REP-00701-09DEC2013-060]. 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>This effort has resulted in developing a COG generic methodology for evaluating instrumentation and equipment survivability for severe accident conditions ["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&E) survivability assessment has been completed and documented in "Bruce Power Severe Accident Management Guidance Instrument and Equipment Survivability - Summary Report" [Enclosure 2, NK21 - CORR-00531-11801 - Bruce Power Progress Report No. 6 on CNSC Action Plan - Fukushima Action Items]. This assessment provides a reasonable level of confidence that the I&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).</p> <p>The instrument and equipment survivability report includes various</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> non-safety-related equipment whose failure due to harsh post-accident environment could prevent safety-related equipment from accomplishing its safety function accident monitoring equipment <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"> a distinction between mild and harsh environments (e.g., specific criteria to define plant environments as either mild or harsh) a list of bounding harsh DBAs for qualification of equipment 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 temperature, pressure and radiation profiles for harsh environment qualification typical equipment mission time during DBAs mild environmental conditions (e.g., temperature, pressure, humidity, radiation) for operational states, including the assumed duration of the AOOs to which equipment is exposed in 	<p>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 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 is requesting closure as per [NK21 -CORR-00531-11801].</p>	



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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">• 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.• Equipment should be reviewed in terms of design, function, materials and environment, to identify significant aging mechanisms caused by 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.• The qualification should systematically address the sequence of age conditioning, including sequential, simultaneous, synergistic effects, and the method for accelerating radiation degradation effects.• Appropriate margins, as given in EQ-related standards, should be applied to the specified environmental conditions.• For certain equipment (e.g., digital I&C equipment, and		



Rev Date: July 8, 2016


Status: Issued

Subject: Safety Factor 1 - Plant Design


File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>new advanced analog electronics) additional environmental conditions – such as electromagnetic interference, radio frequency interference, and power surges – should be addressed.</p> <p>For mild environment qualification, equipment may be considered qualified, provided that:</p> <ul style="list-style-type: none">the environmental conditions are specified in a design specificationthe manufacturer provides certification that the equipment meets the specification <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">the accident timeframes for each functionthe equipment type and location used to perform necessary functions in each timeframethe functions credited in the accident timeframes that need to be performed to achieve a safe shutdown state for DEC'sthe postulated harsh environment of DEC's within each timeframea reasonable assurance that the equipment will survive to perform its function in the accident timeframes, in the DEC environment		


Article No.	Clause Requirement	Assessment	Compliance Category
	<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 should be addressed in a qualification program. Examples of protective barriers include:</p> <ul style="list-style-type: none"> • steam-protected rooms and enclosures • steam doors • water-protected rooms (for flooding) <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> • ASME, QME-1, Qualification of Active Mechanical Equipment Used in Nuclear Power Plants, New York, 2002. • CSA Group, N290.13, Environmental qualification of equipment for CANDU nuclear power plants, Toronto, Canada. • Electric Power Research Institute (EPRI), Technical Report rev. 1, Nuclear Power Plant Equipment Qualification Reference Manual, Palto Alto, California, 2010. • IAEA, Safety Reports Series No. 3, Equipment Qualification in Operational Nuclear Power Plants: Upgrading, 		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Preserving and Reviewing, Vienna, 1998.</p> <ul style="list-style-type: none"> International Electrotechnical Commission (IEC), 60780 ed 2.0, Nuclear Power Plants - Electrical Equipment of the Safety System – Qualification, Geneva, 1998. IEEE, Standard 323, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, Piscataway, New Jersey, 2003. IEEE, Standard 627, Qualification of Equipment Used in Nuclear Facilities, Piscataway, New Jersey, 2010. 		
7.9			NA
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 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</p>	<p>The Bruce A 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"> 1. 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. 2. 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. 3. Equipment is designed for a minimum of regular maintenance. Any necessary maintenance operations are kept as simple and speedy as possible. 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 5. The control systems are designed to make the unit as tolerant 	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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>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>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 A design meets the requirement for periodic testing of the entire channel of instrumentation logic. The channelized logic at Bruce A 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 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 [RABA 0804].</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 and steam generator pressure. 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</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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 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 electrical or mechanical components) or the provision for deliberate operator interventions</p>	<p>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 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 a fresh copy of the core image from a protected area on the solid state memory and restarts the computer, is combined with the fault detection to provide a system practically immune to transient faults. Each computer is connected to an independent 120 V (AC), Class II bus.</p> <p>Further details of computer fault protection are provided in Section 7.1.1.2 and the design basis in Section 7.1.6 of Part 2 of the Safety Report.</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 6.1.4 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 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</p>	



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>(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&C function, the interfaces should 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>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 QPS diesels start automatically but system-supplied loads must be manually activated. 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 (Table 1-20 in Part 3 of the Safety Report) the design of the system in no way impedes the required actions.</p>	



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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"> initiation of safety tasks after completion of automatic sequences initiation of safety actions that are not required until a considerable time after the PIE control actions to bring the plant to a safe state in the long term, after an accident <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"> CSA Group, N290.14, Qualification of Pre-developed Software for Use in Safety Related Instrumentation and Control Applications in Nuclear Power Plants, Toronto, Canada. 		




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> • CSA Group, N290.6, Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of an Accident, Toronto, Canada. • IAEA, NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Plants, Vienna, 2002. • IEC, 61226, Nuclear Power Plants - Instrumentation and Control Important to Safety - Classification of Instrumentation and Control Functions, Geneva, 2009. • IEC, 61513, Nuclear Power Plants – Instrumentation and Control Important to Safety, General Requirements for Systems, Geneva, 2011. • IEC, 60987, Nuclear Power Plants – Instrumentation and Control Important to Safety – Hardware Design Requirements for Computer-Based Systems, Geneva, 2007. • IEC, 62385, Nuclear Power Plants – Instrumentation and Control Important to Safety – Methods for Assessing the Performance of Safety System Instrument Channels, Geneva, 2007. • IEC, 60880, Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems Performing Category A Functions, Geneva, 2006. • IEC, 60671, Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Surveillance Testing, Geneva, 2007. • IEEE, 7-4.3.2, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, Piscataway, New Jersey, 2010. • IEEE, 603, Standard Criteria for Safety Systems for Nuclear Power Generating Stations, Piscataway, New Jersey, 2009. 		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
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 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"> 1. Functions not essential to safety are separate from and shown not to impact the safety function. 2. The safety function is normally executed in processors 	<p>A review of the same clause in a draft version of RD-337 indicated that the Bruce A safety system uses 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. The Safety System Monitoring Computer also provides only information to the operator. Neither system provides direct safety functions. The only place where computer based equipment is used is in the Pump Trip logic which has Programmable Controllers. The Pump Trip programmable controllers are used to calculate margin to saturation based on pump discharge temperatures and pump suction pressure; and alarm and initiate trip of main pumps conditioned on reactor power being under 30%. The programming is burned onto a ROM, so the programming cannot be altered once installed (without changing the ROM). They are a Fischer Porter Chameleon type.</p> <p>At this time the safety systems at Bruce A 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 [BP-PROC-00050 R001] notes that software is classified as follows:</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</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>separate from software that implements other functions, such as control, monitoring, and display.</p> <p>3. The requirements associated with diversity apply to computer-based systems that perform similar safety functions – the choice of diversity type shall be justified.</p> <p>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.</p> <p>Guidance</p> <p>The standards and practices used for computer-based systems or equipment are identified prior to the design. The I&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&C development.</p> <p>The I&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</p>	<p>Nuclear Power Plant Safety, Control, Monitoring, and Testing Systems, COG-95-264.1, Revision 1",</p> <p>As noted in [RABA 0804] Bruce A has no safety related software in use at this time. These features may be applicable to any future code development should Bruce A introduce safety-related software into the system.</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>qualification activities of pre-developed software.</p> <p>When the pre-developed software was not 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"> consistency applies to uniform notations, terminology, comments, symbology, and implementation techniques modularity ensures that any change to one component has minimal impact on the others 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 traceability provides a thread to antecedent and subsequent documents, and refers to the ability to trace the design decision history and reasons for changes understandability means that the development processes and outputs should be clear to a third party verifiability refers to the extent to which the development processes and outputs have been created to facilitate verification using both static methods and testing <p>The complete software development documentation should provide all information throughout the software development</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>lifecycle.</p> <p>Additional information:</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> IAEA, NS-G-1.1, Software for Computer Based Systems Important to Safety in Nuclear Plants, Vienna, 2000. 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. 		
7.9.3	<p>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> <ol style="list-style-type: none"> indicating plant status identifying the locations of radioactive material supporting estimation of quantities of radioactive material recording vital plant parameters facilitating decisions in accident management 	<p>There are no changes to this clause.</p> <p>A review of the same clause in a draft version of RD-337 indicated that the Bruce A design meets the intent of this requirement, as documented in [RABA 0804].</p> <p>As discussed in Part 2, Section 6.2.2.12 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. Several upgrades to the system are underway to meet the performance requirement in terms of providing data for all single or dual failures accidents.</p> <p>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</p>	IC



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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 for recording vital plant parameters and variables, such as:</p> <ul style="list-style-type: none"> • temperature at various locations • pressure of containment, and primary coolant system • level of radioactivity at various locations • reactor vessel water level for a light water reactor (LWR), or heat transport system water level and moderator level for a CANDU reactor • containment water level • hydrogen concentration <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</p>	<p>withstanding the 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.</p> <p>The classification of equipment as complementary design features is a new classification and has not been used at Bruce A 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>	




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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>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"> • incorporate testing capability, to verify operability requirements on a periodic basis • facilitate maintenance, repair and calibration • permit administrative access control for instrument channel calibration and testing <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 DECs.</p> <p>Additional information:</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> • CSA Group, N290.6, Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of an Accident, Toronto, Canada. • IEC, 61226, ed. 3.0, Nuclear Power Plants – Instrumentation and Control Important to Safety – Classification of 		

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Instrumentation and Control Functions, Geneva, 2009.</p> <ul style="list-style-type: none"> 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. IEEE, 497, Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations, Piscataway, New Jersey, 2010. 		
7.10	<p>The safety support systems shall ensure that the fundamental safety functions are available in operational states, DBAs and DEC. 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 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"> sufficient capacity to meet the load requirements of the systems that perform the fundamental safety functions availability and reliability commensurate with the systems to which they supply the service 	<p>The text was modified to include two new requirements for emergency support systems, item 2.</p> <p>The standby generators and the Qualified Power System provide back up to Class IV electrical system.</p> <p>The purpose of the Qualified Power Supply (QPS) System is to provide power to specific equipment and instrumentation required for maintaining essential safety functions following the Main Steam Line Break incident, Seismic event and Main Control Room (MCR) rendered uninhabitable event (Section 8.3.11 of Part 2 of the Safety Report). The QPS provides power to specific equipment and instrumentation required to maintain essential safety functions following an event and is sized accordingly. A safety related 125V DC system supports black-start capability of the system. Equipment associated with the QPS system is located either outside the powerhouse or within rooms that have been "hardened" to meet the postulated conditions following a MSLB event (except SG2 and associated cable). The QPS system is continuously energized from one of the two normal sources and is monitored in the Main Control Room (MCR). The system Design Manual [NK21-DM-54400-002] specifies the functional and performance requirements for the QPS system. The power sources shall be capable of supplying a continuous load of 2000 kW(e) to designated unit or common loads for its 72 hour mission time with a target unavailability of 1x10E-2. This load is selected based on the original QPS load with added margin for some additional 600 V loads (e.g., SCA services, ECI D2O isolation valve operation, EFADS valves operation) that may be required in future. The mission time for seismic shutdown was</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The emergency support systems shall:</p> <ol style="list-style-type: none"> be independent of normal and backup systems support continuity of the fundamental safety functions until long-term (normal or backup) service is re-established: <ol style="list-style-type: none"> without the need for operator action to connect temporary onsite services for at least 8 hours without the need for offsite services and support for at least 72 hours have a capacity margin that allows for future increases in demand be testable under design load conditions, where practicable <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</p>	<p>extended to 72 hours; however the unavailability does not apply to RLE seismic shutdown events.</p> <p>The station has two sources of standby power on site – the station batteries and the standby generators, 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 automatically started, following the loss of Class IV power, to supply power to the critical Class III loads or when HPECI is initiated (Section 8.4.3 of Part 2 of the Safety Report).</p> <p>A review of the same clause in a draft version of RD-337 indicated that the Bruce A design meets the intent of this requirement, as documented in [RABA 0804]. 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 Qualified Power Supply and the Emergency Water Supply System are capable of supplying adequate emergency services to ensure that the reactor can be placed in and kept in a safe shutdown state.</p> <p>The purpose of the Bruce Power Nuclear Emergency Response Plan (NERP) [BP-PLAN-00001] 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, 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>The capacity margin of the Bruce A and B emergency support systems to allow for further increases in demand is limited, as it was</p>	




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>important to safety, in all plant states.</p> <p>Pre-installed equipment can be credited for accident mitigation after 30 minutes where only 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>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, R009] will be used to determine how to address the emergency support system loading issue.</p> <p>QPS, EBC, as well as the Class III, II and I and Standby generators, are part of the Seismic success path as shown in Table 2-2 [Section 2.5.1.3, Part 2 of the Safety Report]. PEVS is not required since the main steam system is qualified for RLE conditions. Qualified Power Supply (QPS), Power House Emergency Vent System (PEVS) and Emergency Boiler Cooling (EBC) are environmentally qualified as are the parts of the water systems needed to ensure operation of the EBC and the containment boundary [Section 2.5.4.2 of Part 2 of the Safety Report]. The safe shutdown path following an RLE must be capable for ensuring that safe conditions exist for at least 72 hours following the event. Systems and structures that are environmentally qualified can achieve their specified safety functions over the required mission time. This mission time depends upon the accident sequence that generates the harsh conditions. For LOCAs, a three-month mission time is considered for all systems required for the safe shutdown path [RABA 0804].</p> <p>Environmental Qualification Requirements of Safety Related Systems and Structures for the Bruce A Nuclear Generating Station [NK21-EQR-03651-00001] contains the detailed requirements for each of the systems subject to environmental qualifications.</p> <p>Bruce A completes one SG run every week for 2 hours at full load. In addition, two other SGs are black started during the Emergency Transfer Tests but they are not run. A full black start and block loading of the standby generator is performed once a year during the annual shutdown.</p>	
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</p>	<p>There is no change in the requirements.</p> <p>The guaranteed shutdown states are defined in the Clause 63.15 of the OP&Ps [BP-OPP-00002, R012]. The primary function of the Moderator system during outages is to ensure that the reactor</p>	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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, and functional tests to be performed.</p>	<p>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 [NK21-OSR-32000-00001, R00]. 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>Analysis shows that the safety limit for poison concentration of 10.3 ppm of Gadolinium for pre-equilibrium (the plutonium peak) would be sufficient to prevent recriticality [Appendix 9 Main Moderator and Moderator Auxiliary System Failures, Part 3 of Safety Analysis]. Despite the analysis findings, the CNSC has mandated a minimum poison concentration of 18.6 ppm.</p> <p>Typically the test frequency is determined by safety assessments, probabilistic risk assessment and unavailability analyses. The functional tests to be performed are not reflected in the design documentation; therefore this is assessed as a gap (Gap).</p>	
7.12	The design of the NPP, including that of external buildings and SS 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 A design achieves all objectives detailed in sub clauses 7.12.1 to 7.12.3 is documented in NK21-REP-71400-00003, NK21-REP-71400-00004 and NK21-REP-71400-00005.</p>	C
7.12.1	Suitable incorporation of operational procedures, redundant SSCs, physical barriers, spatial separation, fire protection	There are no changes in the requirements.	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>systems, and design for fail-safe operation shall achieve the following general objectives:</p> <ol style="list-style-type: none"> 1. prevent the initiation of fires 2. limit the propagation and effects of fires that do occur by: <ol style="list-style-type: none"> a. quickly detecting and suppressing fires to limit damage b. confining the spread of fires and fire by-products that have not been extinguished 3. prevent loss of redundancy in safety and safety support systems 4. provide assurance of safe shutdown 5. ensure that monitoring of safety-critical parameters remains available 6. prevent exposure, uncontrolled release, or unacceptable dispersion of hazardous substances, nuclear material, or radioactive material, due to fires 7. prevent the detrimental effects of event mitigation efforts, both inside and outside of containment 8. ensure structural sufficiency and stability in the event of fire 	<p>A review of the same clause in a draft version of RD-337 indicated that the Bruce A design meets the requirements, as documented in [RABA 0804].</p> <p>The Fire Safety Assessments performed for Bruce A consists of three separate assessments:</p> <ol style="list-style-type: none"> 1. The Fire Hazards Assessment [NK21-REP-71400-00003 R05] 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 evaluates the conditions of the plant as operated. 2. Fire Safety Shutdown Analysis [NK21-REP-71400-00004, Rev. 6] 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. 3. Code Compliance Review [NK21-REP-71400-00005-R05] evaluated the existing Bruce A 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>The Code Compliance Review includes a line-by-line detailed 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>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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"> • 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 • the use of physical barriers to segregate redundant SSCs important to safety <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>The Fire Safety Assessment and supporting documentation provides the basis for the development and implementation 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 of Part 2 of the Safety Report. The results of fire protection assessment are presented in Safety Factor 7.</p>	



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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">• CSA Group, N293, Fire protection for nuclear power plants, Toronto, Canada.• NRC, National Building Code of Canada, Ottawa, Canada, 2010.• NRC, National Fire Code of Canada, Ottawa, Canada, 2010. <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">• operator-initiated manual actions• associated fire safe shutdown circuit analysis• multiple spurious operations <p>Guidance on the above fire safety aspects is provided in:</p>		




Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design


File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> U.S. NRC, NUREG-1852, Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire, 2007. Nuclear Energy Institute, NEI 00-01, Guidance for Post-Fire Safe Shutdown Circuit Analysis, Washington, D.C., 2005. <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> IAEA, NS-G-2.1, Fire Safety in Operation of Nuclear Power Plants, Vienna, 2000. IAEA, Safety Report Series No. 8, Preparation of Fire Hazard Analysis for Nuclear Power Plants, Vienna, 1998. IAEA, NS-G-1.7, Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants, Vienna, 2004. National Fire Protection Association (NFPA), Fire Protection Handbook, Quincy, Massachusetts, 2008. NFPA, 805, Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants, Quincy, Massachusetts, 2010. NFPA, 804, Standard for Fire Protection for Advanced Light Water Reactor Electric Generating Plants, Quincy, Massachusetts, 2010. NEI, 00-01, Guidance for Post-Fire Safe Shutdown Circuit Analysis, Washington, D.C., 2005. NEI, 04-02, rev. 1, Guidance for Implementing a Risk-Informed, Performance-Based Fire Protection Program under 10 		


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>CFR 50.48(c), Washington, D.C., 2005.</p> <ul style="list-style-type: none"> • Society of Fire Protection Engineers (SFPE), SFPE Handbook of Fire Protection Engineering, Bethesda, Maryland, 2008. • U.S. NRC, NUREG/CR-6850, EPRI 1011989, Fire Probabilistic Risk Assessment Methods Enhancements, Washington, D.C., 2010. • 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. • U.S. NRC, Regulatory Guide 1.189, Fire Protection for Operating Nuclear Power Plants, Washington, D.C., 2009. • U.S. NRC, NUREG-1852, Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire, Washington, D.C., 2007. 		
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> <ol style="list-style-type: none"> 1. Persons not intimate with the initial event (including the public, occupants, and emergency responders) are protected from injury and loss of life. 2. Persons intimate with the initial event have a low probability of injury or death. <p>To demonstrate that the above life safety objectives have been achieved, the design shall provide:</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 design does not fully meet this requirement, as documented in [NK21-CORR-00531-11005]. Compliance with the provisions of this requirement is in practice accomplished through compliance with the CSA standard for fire protection [CSA N293-07], the National Fire Code [NFCC], and relevant parts of the National Building Code [NBCC].</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>	C


Article No.	Clause Requirement	Assessment	Compliance Category
	<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>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>	<ul style="list-style-type: none"> • A Code Compliance Review (CCR) • A Fire Hazard Assessment (FHA) • A Fire Safe Shutdown Analysis (FSSA) <p>Recently revised versions of the FSSA, FHA and CCR reports for both Bruce A have been deemed acceptable by the CNSC staff. As a follow up from the Bruce A FSSA that specified Operator actions that are potentially required to meet the station fire safe shutdown goals for some of the postulated fires, Bruce Power will conduct a review of Bruce A Operator manual actions. This review will assess if any gaps exist in the required response to hazards identified in the FSSA. This review has already been conducted at Bruce B and determined that no gaps exist. A plan to disposition gaps against CSA N293-07 as identified in the revised FSSA, FHA and CCR is in place and being tracked against Action Item 1207-3890.</p> <p>Gap assessments have also been conducted against other fire protection-related standards (NBCC, NFCC and NFPA-801) and submitted to CNSC staff. New editions have been issued for the above four standards (CSA N293, NBCC, NFCC, NFPA-801). These are discussed in the following:</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 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</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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>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>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-801: As discussed in Section 3.6 of this Safety Factor Report, the requirements of NFPA-801 are incorporated into CSA N293-12.</p>	
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</p>	<p>There are no differences in the text.</p> <p>A review of the same clause in a draft version of RD-337 indicated that the Bruce A design meets this requirement, as documented in [RABA 0804].</p> <p>Bruce Power, in its Fire Safety Management Plan [BP-PLAN-00008, R003], 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>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	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.	<ol style="list-style-type: none"> 1. Ensure that fires do not significantly increase the risk of radiological releases to the public. 2. Protect plant operating personnel from the hazards of fires in accordance with applicable building codes and fire codes. 	
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>As discussed in Part 2, Section 2.5.1.1 of the Safety Report, to address Seismic Qualification for Bruce A, a Seismic Margin Assessment (SMA) was conducted [NK21-REP-03611-00005, Rev. 000]. The assessment was in accordance with the SMA guidelines of EPRI NP-6041SL with modifications to fit the unique characteristics of the CANDU reactor system. The SMA is based on the evaluation of all structures, systems and components that make up the "success path", including the reactors and their auxiliary systems, control systems, electrical systems, as well as the civil structures. The electrical and mechanical components are captured on the Safe Shutdown Equipment List (SSEL). Seismic qualification priority list is provided in Table 2-3 of Part 2 of the Safety Report.</p> <p>In the EPRI approach to SMA, it is necessary to demonstrate operation and survival of components and structures to bring the plant to a safe shutdown and maintain it there for 72 hours. The set of components selected to demonstrate this ability is called the success path. The path selected for the Bruce A SMA is shown in Table 2-2, Part 2 of the Safety Report.</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 motion within 20 km of the Bruce site. The process for identifying seismic activity is outlined in the Abnormal Incidents Manual [NK21-OM-09034, Rev. 113]. 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</p>	AD

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>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> <p>Therefore, this is considered to be an acceptable deviation.</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"> SSCs whose failure could directly or indirectly cause an accident leading to core damage SSCs restricting the release of radioactive material to the environment SSCs that assure the subcriticality of stored nuclear material SSCs such as radioactive waste tanks containing radioactive material that, if released, would exceed regulatory dose limits <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>A new requirement for a beyond design basis earthquake (BDBE) that meets the requirements for identification of DEC's is introduced.</p> <p>Bruce A Safety Report describes review level earthquake as the 84th percentile 10E-4 per annum probability of exceedance (10,000 year recurrence) Uniform Hazard Spectrum (UHS) which is estimated to result in annual core damage frequency of less than about $2 \times 10E-5$. The Seismic Margin Assessment [NK21-REP-03611-00005, Rev. 000] presents the results of the seismic margin assessment performed on the Bruce A Unit 1 & 2 systems, structures and components to confirm their seismic capability. The SMA verified the seismic capacity of the piping, which in turn established that the Review Level Earthquake will not cause Large Loss of Coolant Accident or Secondary Side Line Breaks. In the assessment off-site power is assumed to be unavailable during the 72 hour time period due to the postulated low seismic capacity of certain switchyard components.</p> <p>An assessment of the capability of Bruce A to accommodate a Review Level Condition (RLC) for high winds and seismic events has been completed and documented in "Bruce Power External Hazard Robustness Assessment – Ability of Bruce A to Accommodate a Review Level Condition for Seismic Events and High Winds" [Enclosure 4 of NK21-CORR-00531-11801]. The general characteristics of a RLC for an external event are:</p> <ul style="list-style-type: none"> The RLC shall be more severe than the plant's design basis. The RLC shall be more severe than conditions that have recently been experienced in the vicinity of the plant. Where possible, the RLC should be linked to a generally accepted standard. If the RLC is defined probabilistically, the return period for the RLC shall be 10,000 years or more. 	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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 DECAs 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 qualification by testing.</p> <p>Guidance</p> <p>The seismic design of an NPP should account for:</p> <ul style="list-style-type: none"> • technical safety objectives and corresponding load categories • seismic input motion • seismic classification • structural layout criteria • seismic analysis and design of structural systems, subsystems and equipment • seismic testing and instrumentation <p>Design and beyond design load categories are defined to demonstrate structural performance in operational states, DBAs and DECAs. In addition, beyond design load categories are</p>	<p>The steps in this assessment included:</p> <ol style="list-style-type: none"> 1. Definition of the RLC 2. Identification of the Systems, Structures and Components (SSCs) required to mitigate the effects of the RLC 3. Determination of the capability of the identified SSCs to accommodate the RLC 4. Identification of SSCs that cannot accommodate the RLC <p>For seismic events and high winds, the SSCs credited to prevent severe core damage are defined by the PSA for these hazards. The assessment identified a number of recommendations, several of which have been dispositioned. The remaining assessment recommendations will be further evaluated via a conceptual engineering process that is currently planned for completion by the end of 2015. Since the assessment is limited to the direct effects of a single initiator and covers the SSCs required to prevent severe core damage, compliance with the new requirement for a BDBE introduced in this clause cannot be confirmed. Therefore, it is assessed as gap (Gap).</p> <p>Guidance for conduct of seismic qualification is provided in DPT-PDE-00017. The extent of seismic qualification of Bruce A is assessed in NK21-REP-20091-00001. Reconciliation completion and Seismic Margin Assessment as part of assessing and improving seismic margins is underway. Several U1/U2 reconciliations remain active as a result of modifications completed during the Bruce A U1/U2 Restart project. These reconciliations have now been integrated into the Bruce A Legacy registration project commitment (AI 090734) to be complete by December 31, 2014. Seismic Margin Assessments are required to support the completion of the reconciliations and legacy registration project commitments</p>	



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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 DECs.</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 10E-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 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>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<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. 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</p>		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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"> 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 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 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 <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 Steel Structures for steel structures assuming that the structures are ductile or type D. These ductility requirements should provide margins for the BDBE.</p>		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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"> • in-structure response spectra • in-structure time response histories <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 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</p>		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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> <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 up to 2</p>		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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"> 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. American Society of Civil Engineers (ASCE), 04-98, Seismic Analysis of Safety-Related Nuclear Structures, Reston, Virginia, 2000. ASCE/Structural Engineering Institute, 43-05, Seismic Design Criteria for Structures, Systems and Components in Nuclear Facilities, Reston, Virginia, 2005. American Society of Mechanical Engineers (ASME), Boiler and Pressure Vessel Code Section III, Division 1-Subsection NE, Rules for Construction of Nuclear Facility Components, New York, 2010. CSA Group, N287 series on requirements for concrete containment structures for CANDU nuclear power plants. CSA Group, N289 series on seismic design and qualification of nuclear power plants. CSA Group, A23.3, Design of Concrete Structures, Toronto, Canada. CSA Group, S16, Design of Steel Structures, Toronto, 		




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Canada.</p> <ul style="list-style-type: none"> • CSA Group, N291, Requirements for Safety-Related Structures for CANDU Nuclear Power Plants, Toronto, Canada. • Electric Power Research Institute, TR-103959, Methodology for Developing Seismic Fragilities, Palo Alto, California, 1994. • European Standard, EN-15129, Anti-seismic Devices, European Committee for Standardization: Brussels, 2009. • European Standard, EN-1337-3, Structural Bearings – Elastomeric Bearings, European Committee for Standardization: Brussels, 2000. • European Standard, EN 1337-1, Structural Bearings – General Design Rules, European Committee for Standardization: Brussels, 2000. • IEEE, 344, IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, Piscataway, New Jersey, 2004. • NRC, National Building Code of Canada, Ottawa, Canada, 2010. • U.S. NRC, Regulatory Guide 1.57, Design Limits and Loading Combinations for Metal Primary Reactor Containment System Components, Washington, D.C., 2007. • U.S. NRC, Regulatory Guide 1.91, Evaluations of Explosions Postulated to Occur on Transportation Routes Near Nuclear Power Plants, Washington, D.C., 1978. • 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. 		
7.14	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	A new requirement has been added to have design provisions to gather baseline data in order to support maintenance ...etc.	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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"> 1. Proven alternative methods, such as surveillance of reference items, or use of verified and validated calculation methods, shall be specified. 2. Conservative safety margins shall be applied, or other appropriate precautions shall be taken, to compensate for possible unanticipated failures. <p>Details of alternate approaches to SSC monitoring shall be provided in the design documentation.</p> <p>The design shall provide facilities for monitoring chemical conditions of fluids, and of metallic and non-metallic materials. In addition, the means for adding or modifying the chemical</p>	<p>A review of the same clause in a draft version of RD-337 indicated that the Bruce A design meets the requirement, as documented in [RABA 0804].</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 system.</p> <p>Bruce A has extensive testing programs to demonstrate that the special safety systems meet their ongoing reliability requirements. Section 03.5 of the Bruce Operating Policies & Principles (OP&Ps) 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 & 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 [PT-PE-00008/09/10] and meet the criteria specified in Component Categorization [BP-PROC-00666, R001]. Life Cycle Management is one of the key elements of BP-PROG-11.01, Equipment Reliability Program.</p> <p>Design provisions are implemented to minimise the radiation doses to</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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>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,</p>	<p>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. 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, as presented in [RABA 0804], 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 moderator sampling as described in Section 11.2 of Part 2 of the Safety Report.</p>	



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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> <ul style="list-style-type: none"> the intended design life, design loading conditions, operational requirements and safety significance of SSCs the requirements of applicable codes, standards and regulations the responsibilities of the designer, vendor, construction organization, operating organization and contractors interdependence of SSCs important to safety and possible effects of failures of SSCs of lower safety significance on SSCs of higher safety significance plant design, layout and the accessibility of SSCs during construction, commissioning, and during the intended service life monitoring, inspection and testing programs used during the construction, commissioning and service for NPPs of similar or identical design and layout technologies and methodologies available for monitoring, inspection and testing, as well as for the repair, replacement or modification of SSCs research and development activities 		




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> operating experience human factors training and qualification of personnel availability of adequately trained and qualified personnel availability of required laboratory or testing facilities and equipment <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"> ASME, Boiler and Pressure Vessel Code-2010, Section XI, Rules for In service Inspection of Nuclear Power Plant Components, New York, 2010. 		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> • CNSC, RD-334, Aging Management for Nuclear Power Plants, Ottawa, Canada, 2011. • CNSC, RD/GD-210, Maintenance Programs for Nuclear Power Plants, Ottawa, Canada, 2012. • CSA Group, N287.7, In-service Examination and Testing Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, Toronto, Canada. • CSA Group, N285.4, Periodic inspection of CANDU nuclear power plant components, Toronto, Canada. • CSA Group, N285.5, Periodic inspection of CANDU nuclear power plant components, Toronto, Canada. • CSA Group, N291, Requirements for Safety-Related Structures for CANDU Nuclear Power Plants, Toronto, Canada. • IAEA, Safety Guide NS-G-2.6, Maintenance, Surveillance and In-Service Inspection in Nuclear Power Plants, Vienna, 2002. 		
7.15	Civil Structure	This is not a requirement/guidance clause (this is a title only).	NA
7.15.1	<p>The NPP design shall specify the required performance for the safety functions of the civil structures in operational states, DBAs and DEC's.</p> <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>A new requirement for DEC's is added.</p> <p>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 DBAs is extended to include DEC's (new requirement).</p> <p>(Gap) As discussed in Part 2, Section 7.4.1 of the Safety Report, Bruce A design does not meet these requirements, as documented in [NK21-CORR-00531-11005]. Specifically, internal hazards were not a primary consideration for the original Bruce A design and layout of civil structures important to safety. As a result, the requirements associated with internal hazards such as pipe whip and jet impingement were not fully addressed. As discussed in supporting documentation for NK21-CORR-00531-11567 CNSC has accepted the results of the Pipe Whip and Jet Impingement Assessment of</p>	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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>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</p>	<p>Piping Inside the Reactor Vault. The results of the assessment concluded that no design changes are required in the Units 1 and 2 vaults as a result of pipe-whip or jet impingement.</p> <p>Section 2.5.3 of the Bruce A Safety Report [NK21-SR-01320-00001, Rev. 005] shows that features incorporated into the Bruce A design provide an adequate level of protection against any credible turbine generator missile. 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] presents analysis of turbine generated missiles 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]. 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). A missile probability analysis for the Siemens 13.9 m² retrofit design of LP is documented in NK21-REPT-411110-00003. The probability of missile strikes on PHT pump/motors was calculated taking into consideration that there is no reinforced concrete barrier to protect the HT pump motors at Bruce A. Using the EPRI Guidance for Performing a Simplified Risk-Informed Turbine Missile Analysis, it was found that the turbine generated missile total damage probability on PHT pump/motors is 2.13x10E-7 occurrence/year. A bounding calculation of SCDF associated with turbine missiles striking and damaging Group 1 electrical equipment concluded that this specific event is a low risk contributor to the severe core damage frequency at Bruce A (5.43x10E-8 occurrence/year). Therefore, this particular scenario can be screened out at Bruce A and will not be retained for further assessment. Combined events analysis did not identify any combinations of hazards related to turbine generated missiles that would not screen out [K-449958-REPT-00009]. As discussed in [RABA 0804] as a minimum, the structures have been designed and</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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"> • normal condition loads which are expected during the assumed design life of the NPP • AOO loads (or severe environmental loads) • DBA loads (or abnormal or extreme environmental loads) • DEC loads (or beyond-design loads) <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 of aging on the structure and its material. The design should include sufficient safety margins for the buildings and structures that are important</p>	<p>built in accordance with the requirements of the National Building Code of Canada, 1965. Loads and loading combinations, considered in the design of the containment structures are summarized in Part 2, Section 2.3.2 of the Safety Report. As discussed in Section 7.13, the Seismic Margin Assessment addresses the earthquake.</p> <p>Bruce A Containment Operational Safety Requirements are presented in NK21-OSR-34200-00004. Therefore, DEC 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, 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 and this FAI was closed following CNSC's review of the analysis. 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.</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 trucks). As reported in [NK21-CORR-00531-10963] Bruce Power has completed all short term modifications to emergency water to be added to the steam generators and IFBs using EME pumps.</p>	



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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"> the type of structure, and its structural and functional characteristics the geometry of the structures, including sketches showing plan views at various elevations and sections (at least two orthogonal directions) the relationship between adjacent structures, including any separation or structural ties the type of base slab and its arrangement with the methods of transferring horizontal shears (such as those seismically induced) to the foundation media <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, 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>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> base slab and sub-base containment wall and dome design containment wall openings and penetrations pre-stressing system containment liner and its attachment method <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 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"> N287.1, General Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, for general requirements in documentation of design specification and design reports 		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> N287.2, Material Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, for material N287.3, Design Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants for design N287.4, Construction, Fabrication and 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 N287.6, Pre-operational proof and leakage rate testing requirements for concrete containment structures for nuclear power plants, for pressure test before operation <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 containment should be designed and constructed in accordance with CSA N291, Requirements for safety-related structures for CANDU nuclear power plants.</p>		




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design of other safety-related structures should include:</p> <ul style="list-style-type: none"> • internal structures of reactor building • service (auxiliary) building • fuel storage building • control building • diesel generator building • containment shield building, if applicable • other safety-related structures defined by the design • turbine building (for boiling water reactor) <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> • American Concrete Institute (ACI), 349-06, Code Requirements for Nuclear Safety-Related Concrete Structures & Commentary, Farmington Hills, Michigan, 2007. • ASME, Boiler and Pressure Vessel Code (BPVC) Section III, Division 2, Section 3, Code for Concrete Containments, New York, 2010. • IAEA, NS-G-1.10, Design of Reactor Containment Systems for Nuclear Power Plants, Vienna, 2004. • U.S. NRC, NUREG/CR-6486, Assessment of Modular Construction for Safety-Related Structures at Advanced Nuclear 		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Power Plants, Washington, D.C., 1997.</p> <ul style="list-style-type: none"> U.S. NRC, Regulatory Guide 1.76, Design Basis Tornado and Tornado Missiles for Nuclear Power Plants, Washington, D.C., 2007. U.S. NRC, Regulatory Guide 1.91, Evaluations of Explosions Postulated to occur on Transportation Routes near Nuclear Power Plants, Washington, D.C., 1978. 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. 		
7.15.2	<p>The design shall enable implementation of periodic inspection programs for structures important to safety in order to verify that the as-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>The change is to clarify that the constructed structures meet their functional and performance requirements.</p> <p>A review of the same clause in a draft version of RD-337 indicated that the Bruce A design meets the intent of this requirement, as documented in [RABA 0804].</p> <p>CSA N287.7-08 Periodic Inspection Program for Bruce NGS A Concrete Containment Structures and Appurtenances [NK21-PIP-21100-00001, R002] 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.</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 A are constructed on bedrock that minimizes the likelihood of any significant settling of the structures [RABA 0804].</p> <p>As presented in Sections 6.2.1 and 6.2.2 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</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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 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>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. The pressure is normally maintained at 6.9 to 10.3 kPa absolute (1.0 to 1.5 psia) in the vacuum building, and at slightly subatmospheric in the rest of the containment envelope (-2.5 kPa to -3.5 kPa(g)). The design target leakage rate for the containment boundary, except for the vacuum building, was set at 1% of the total contained mass per hour at 68.9 kPa(g) (10 psig) for the reactor vaults and fuelling duct/fuelling machine rooms; and, 62 kPa(g) (9 psig) for the pressure relief duct and pressure relief manifolds. However, safety analysis is performed assuming a higher limit in order to assure margins. The operational target leak rate for the main volume of the vacuum building is 47 L/s (100 scfm) at 7 kPa(a) (1 psia), and for the upper chamber it is 1.4 L/s (3 scfm).</p> <p>The Operational Safety Requirements for Bruce A Containment System [NK21-OSR-34200-00004, R001] 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.</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
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>A review of the same clause in a draft version of RD-337 indicated that the design of Bruce A recognizes the need for lifting heavy loads in a variety of locations and suitable cranes have been installed to perform these lifts. 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 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 crane that 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 the north end of the building, the crane has access to grade level.(Section 3.2.3)</p> <p>Two 10 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. A 32 Mg (35 ton) crane permits the handling of equipment for the reactivity mechanisms rehearsal facility located at the north end of the bay. 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. (Section 3.7.2.2.).</p> <p>A 90 Mg (100 ton) bridge crane with a 4.5 Mg (5 ton) auxiliary hoist serves the north, deep section of the bay for irradiated fuel shipping cask handling and loading, and spans an adjacent area for loading</p>	Gap

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>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. In the secondary irradiated fuel bay a 4.5 Mg (5 ton) auxiliary hoist on the overhead crane and a tray handling tool are used to lower the trays onto a cable driven cart. (Sections 10.2.2.2.2 and 10.2.5.2.4)</p> <p>Provision has been made for future installation of a 112.5 Mg (125 ton) crane for handling cask decontamination and loading of fuel shipping casks at the north end of the secondary irradiated fuel storage bay. A 31.5 Mg (35 ton) crane is currently installed. 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 irradiated fuel bay. 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-007, R01]; [NK21-CORR-00531-09809]; 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&B", File #76100, May 24, 2013] [Memorandum from R. Dunn to D. Andrews "Reactivity Deck Crane Restriction, Bruce A&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. To address these concerns, the reactivity deck above the Calandria in Bruce A is analyzed for its perforation and dynamic adequacy with catastrophic collapse to bear the impact caused by accidental dropping of a PHT pump motor during craning operations over the reactivity deck [Bruce BA Reactivity Deck PHT Pump Motor Drop Analysis, NK21-CALC-31360-00003]. This engineering calculation is carried out to establish the maximum drop height (i.e., safe limit on drop height) of 110,000 lb</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
		PHT pump motor. Permanent deformations with no through perforation and no catastrophic collapse of the reactivity deck, is predicted due to the impact caused by dropping of the pump motor from 8 feet height. 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 A 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. Therefore, it is assessed as a gap. (Gap 2).	
7.16	<p>SSCs important to safety shall be designed so that they can be manufactured, constructed, 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&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>New requirements related to construction, commissioning etc. are introduced in the first and the last two paragraphs.</p> <p>As discussed in [RABA 0804], 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&P) and Impairment Manual (IM).</p> <p>The Bruce Power Engineering Change Control Program [BP-PROG-10.02, R009], Section 4.5 Commissioning Modifications and Projects process, as documented in BP-PROC-00615, 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> <ul style="list-style-type: none"> Installed systems, equipment and components will perform in accordance with specifications and design intent before they are 	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Due account should be taken of relevant experience that has been gained in the 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"> 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. 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. <p>The design authority should provide general 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>placed into service.</p> <ul style="list-style-type: none"> Systems, equipment and components, which were altered to facilitate a change, are returned to their original configuration. Commissioning results are properly documented. Systems, equipment and components are ready for turnover. <p>The Engineering Change Control Program is implemented by the following procedures:</p> <ul style="list-style-type: none"> BP-PROC-00539, Design Change Package BP-PROC-00542, Configuration Information Change BP-PROC-00615, Commissioning Modifications and Projects BP-PROC-00743, Site Services Engineering Change Control BP-PROC-00877, Modification Installation Quality Assurance <p>It is noted that these requirements are targeting new reactors.</p>	




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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 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 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>		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> IAEA, Safety Standards Series No. NS-G-2.9, Commissioning for Nuclear Power Plants, 2003. IAEA, SSR 2/2, Safety of Nuclear Power Plants: Commissioning and Operation, 2011. U.S. NRC, NUREG-0800, Chapter 14, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition, 2007. 		
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"> 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 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 <p>Additional requirements are provided in RD-334, Aging Management for Nuclear Power Plants.</p> <p>Guidance</p> <p>The design should also consider the following:</p> <ul style="list-style-type: none"> identification of all SSCs subject to aging management 	<p>A new sentence referring to additional requirements defined in RD-334 is added to this clause.</p> <p>Bruce A design meets the requirement, as documented in the Equipment Reliability Program [BP-PROG-11.01, R004]. 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 will be used to demonstrate and improve safety throughout the plant operating life. The PSR will be further enhanced by a safety basis process and Composite Safety Profile (CSP) to provide an integrated measure of safety and predicted change in safety of the plant on year over year basis for a defined period. The CSP will combine probabilistic and deterministic safety risk issues into a consistent measure of overall plant safety. The safety basis process and CSP ranking of safety issues will be used to identify the significant risks areas in order to help optimized plant safety improvement and the IIP. Implementation of the IIP will ensure safety is maintained and improved in a cost effective manner.</p> <p>The Assessment of Systems Important to Safety for the Safety & 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</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> • use of advanced materials with greater aging resistant properties • need for materials testing programs to monitor aging degradation • 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 	<p>list of SSCs to be in scope of the Nuclear Safety & Licensing portion of the Nuclear Asset Management Program. Risk prioritization in the ageing and obsolescence (AOP) process described in BP-PROC-00533 is applied to all components of Bruce Power plants, which entails identification of those SSCs that pose the greatest risk to safety, environment, production or those that can serve to provide the most significant impact on overall plant performance (e.g., Criticality Category 1, 2 and SPVs). The AOP provides a risk priority ranking of the SSCs based upon consequence of failure, likelihood of failure, and a current state factor. All components for which the AOP process is applied shall require a Risk Prioritization Number (RPN), which is the product of consequence of failure, likelihood of failure, and the current state factor.</p> <p>The scoping and identification of critical SSCs is part of the Equipment Reliability Program implementation. BP-PROC-00778 describes the process for the Responsible System Engineer (RSE), with support from Reactor Safety, Corporate & 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 functional criticality analysis and identifies:</p> <ul style="list-style-type: none"> • Scoping criteria. • Functions related to safety and reliability. • Critical structures and components that support these functions. • Non-critical components. • Run to failure components. <p>BP-PROC-00778 uses the Master Equipment List (MEL) as a basis. Components and structures not on the MEL (such as piping, cables, and supports), shall 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, PASSPORT Equipment Data Management.</p> <p>DPT-RS-00012, Systems Important to Safety (SIS) Decision Methodology, determines which plant systems meet the criteria of</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
		<p>'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, R004].</p> <p>This code-to-code comparison between CNSC REGDOC-2.6.3 and RD-334 is documented in Safety Factor 4.</p>	
7.18	The design shall provide for the detection, exclusion and removal of all foreign material and corrosion products that may have an impact on safety.	<p>There is no change in the requirement; the text is modified to provide clarification.</p> <p>Bruce Power has a Chemistry Management control program [BP-PROG-12.02, R005] 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, 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>	C
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	<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</p>	C

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	considerations shall include facility access, as well as lifting and packaging capabilities.	<p>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 A plant and are described in Section 10 of Part 2 of the Safety Report.</p>	
7.20	<p>The design shall provide a sufficient number of 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>Additional information may be found in:</p>	<p>The change is for clarification only; it replaces "all plant states".</p> <p>A review of the same clause in a draft version of RD-337 indicated that the Bruce A design meets this requirement, as documented in [RABA 0804]. 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, such as the lack of a second exit from the main heat feed pump room, which was 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 A 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 11.5.2.3 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> <p>The communication systems are described in Part 2, Section 11.5 of</p>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> CSA Group, N293, Fire protection for nuclear power plants, Toronto, Canada. CNSC, G-225, Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills, Ottawa, Canada, 2001 or successor document. IAEA GS-R-2, Preparedness and Response for a Nuclear or Radiological Emergency, Vienna, 2002. NRC, National Building Code of Canada, Ottawa, Canada, 2010. NRC, National Fire Code of Canada, Ottawa, Canada, 2010. 	the Safety Report.	
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> <ol style="list-style-type: none"> reduce the likelihood of human error as far as reasonably achievable provide means for identifying the occurrence of human error, and methods by which to recover from such an error mitigate the consequences of error <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,</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, 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. 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.</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"> reduce the likelihood of human error as far as reasonably achievable provide means for identifying the occurrence of human error, and methods by which to recover from such an error mitigate the consequences of error <p>This procedure is based upon NUREG-0711, Human Factors Engineering Program Review Model, and conforms with CNSC</p>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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>	<p>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 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, 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 and Appendix E. 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 Bruce A MCR has been in operation for over 30 years and has undergone modifications based on requirements from Bruce 3 and 4 Restart as well as Bruce 1 and 2 Refurbishment. Based on this experience, it can be concluded that appropriate information in a usable format 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.</p> <p>Secondary Control Area for Bruce 3 & 4 was designed during the Bruce 3 & 4 Restart project with Human Factors systematically incorporated. The appropriate information for the SCA was determined by completing a functional analyses, task analyses, HSI design and conducting a MCR uninhabitable validation during the design process. The results of the HF activities are summarized in NK21-REP-06700-00001, Bruce A Restart Human Factors Engineering Summary Report. The HF assessment that was conducted in support of the SCA for Units 1 & 2 is summarized in</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>1. assess the general state of the plant, whether in operational states, DBAs or DEC's</p> <p>2. confirm that the designed automatic safety actions are being carried out</p> <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 decision and to act</p> <p>3. following an event, the physical environment is acceptable in</p>	<p>NK21-REP-63760-00002, Human Factors Assessment of the Bruce Unit 1 and 2 Secondary Control Area.</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> <ul style="list-style-type: none"> 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. Site Management Centre (SMC) - is the on-site facility where station management augmentation and technical staff assemble. 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>The SMC and CESC are back-up facilities to each other.</p> <p>Currently, Bruce Power is building a state-of-the-art Emergency Management Centre (EMC) off-site and unifying 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 and Appendix G. 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 DPT-PDE-00013, Appendix F or for</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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"> • engineering design of specific SSCs • procedure development • training development 	<p>minor changes DPT-PDE-00013, Section 4.6 - Step 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 2014. 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 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</p>	




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> consideration of human actions in safety analyses specifications of staffing and minimum shift complement <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 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</p>	<p>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 described in in Appendix B of DPT-PDE-00013:</p> <ul style="list-style-type: none"> o HF Program Management (planning) o Operating Experience Review o Functional Analysis and Function Allocation o Task Analysis o Staffing and Qualification o Treatment of Important Human Actions o Human System Interface Design o Procedure and Training Program Development o Design Verification o Design Validation o Design Implementation o Human Performance Monitoring <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-PROC-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,</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>design solutions are based. The specific HF analyses should be:</p> <ul style="list-style-type: none"> • appropriate to the activities in question that they cover, considering the risk of the activities and the novelty of the design • carried out throughout the development of the design • use methods, techniques, and good practices that are considered acceptable by trained and experienced human factors specialists • share the information produced between groups engaged in different parts of the design <p>The HF analyses could include:</p> <ul style="list-style-type: none"> • function analysis • task analysis • human reliability analysis • hazard analysis • link analysis • information requirements analysis • staffing analysis • usability analysis • operability and maintainability analysis <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</p>	<p>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 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>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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</p>		




Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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> <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</p>		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>results should be used to improve the design. Validation should confirm that the system, including the human components and procedures 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"> • ANSI/ANS, 58.8-1994, Time Response Design Criteria for Safety-Related Operator Actions, La Grange Park, Illinois, reaffirmed 2008. • CNSC, G-323, Ensuring the Presence of Sufficient Qualified Staff at Class I Nuclear Facilities – Minimum Staff Complement, Ottawa, Canada, 2007. • CNSC, G-276, Human Factors Engineering Program Plans, Ottawa, Canada, 2003. • CNSC, G-278, Human Factors Verification and Validation Plans, Ottawa, Canada, 2003. • CNSC, P-119, Policy on Human Factors, Ottawa, Canada, 2000. • CSA Group, N290.6, Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of 		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>an Accident, Toronto, Canada.</p> <ul style="list-style-type: none"> CSA Group, N290.4, Requirements for Reactor Control Systems of Nuclear Power Plants, Toronto, Canada. IEC, 61839, Nuclear Power Plants – Design of Control Rooms – Functional Analysis and Assessment, Geneva, 2000. IEC, 60964, Nuclear Power Plants – Control Rooms – Design, Geneva, 2009. 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. 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. U.S. NRC, NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications- Final Report, Piscataway, New Jersey, 2011. U.S. NRC, NUREG-0711, Human Factors Engineering Program Review Model, Washington, D.C., 2002. U.S. NRC, NUREG-0700, Human System Interface Design Review Guidelines, Washington, D.C., 2002. U.S. NRC, NUREG-6393, Integrated System Validation: Methodology and Review Criteria, Washington, D.C., 1997. U.S. NRC, NUREG-6684, Advanced Alarm Systems: Revision of Guidance and Its Technical Basis, Washington, D.C., 2000. U.S. NRC, NUREG/CR-6633, Advanced Information Systems Design: Technical Basis and Human Factors Review Guidelines, Washington, D.C., 2000. 		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
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 for:</p> <ul style="list-style-type: none">• basic design approach• structural performance objectives• threat characterisation• loading development• material properties• principles of analysis and design• structural acceptance criteria• design of SSCs <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>	Due to sensitivity of information the assessment is documented elsewhere.	RNA
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-</p>	Due to sensitivity of information the assessment is documented elsewhere.	RNA




Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>basis threats (DBTs). More severe but unlikely threats are referred to as beyond-design-basis threats (BDBTs). Both types of 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 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>		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	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.		
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 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>	Due to sensitivity of information the assessment is documented elsewhere.	RNA



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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> <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 available to licensees and applicants upon request to the CNSC.</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<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"> • penetration – the depth of the crater due to the missile impact • spalling – the ejection of the target material from the front face of the target (impacted face) • scabbing – the ejection of material from the rear face of the target • just perforation – the missile just penetrates the target with residual velocity equal to zero <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</p>		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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>Due to sensitivity of information the assessment is documented elsewhere.</p>	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>For more severe events, there shall be a safe shutdown path that comprises at least one means for each of the following:</p> <ol style="list-style-type: none"> 1. reactor shutdown 2. fuel cooling 3. retention of radioactivity from the reactor <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 should include the following:</p> <ul style="list-style-type: none"> • For DBTs, there should be no scabbing of the rear face of structural elements, possibly with limited, easily repairable, superficial spalling of concrete. 		

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> 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. 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. <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 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> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> ACI, Standard 349, Code Requirements for Nuclear Safety-Related Concrete Structures and Commentary, Farmington Hills, Michigan, 2007. ASCE, Ed. 2, Design of Blast-Resistant Buildings in Petrochemical Facilities, Reston, Virginia, 2010. ASCE, 58, Manual and Reports on Engineering Practice, Structural Analysis and Design of Nuclear Plant Facilities, Reston, Virginia, 1980. Communications Security Establishment, TRA-1, Harmonized Threat and Risk Assessment (TRA) Methodology, Ottawa, Canada, 2007. CNSC, RD-321, Criteria for Physical Protection Systems and Devices at High-Security Sites, Ottawa, Canada, 		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2010.</p> <ul style="list-style-type: none"> • CNSC, RD-363, Nuclear Security Officer Medical, Physical, and Psychological Fitness, Ottawa, Canada, 2008. • CNSC, G-274, Security Programs for Category I or II Nuclear Material or Certain Nuclear Facilities, Ottawa, Canada, 2003. • CNSC, RD-346, Site Evaluation for New Nuclear Power Plants, Ottawa, Canada, 2008. • CNSC, G-208, Transportation Security Plans for Category I, II or III Nuclear Material, Ottawa, Canada, 2003. • CSA Group, N291, Requirements for Safety-Related Structures for CANDU Nuclear Power Plants, Ottawa, Canada. • 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. • IAEA, TECDOC-1276, Handbook on the Physical Protection of Nuclear Materials and Facilities, 2002. • IAEA, INFCIRC-225, Rev.5, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, Vienna, 2011. • NEI, 07-13, Methodology for Performing Aircraft Impact Assessments for New Plant Designs, Washington, D.C., 2011. • Unified Facilities Criteria, 3-340-02, Structures to Resist the Effects of Accidental Explosions, Washington, D.C., 2008. • United Kingdom Atomic Energy Authority, Guidelines for the Design and Assessment of Concrete Structures Subjected to Impact, Oxfordshire, United Kingdom, 1990. 		
7.22.4	The design of computer-based I&C systems important to safety shall provide a cyber security defensive architecture.	This is a new clause/section. Due to the sensitivity of information the assessment is documented elsewhere.	RNA



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Computer-based I&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&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&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>The design of a cyber security program should consider:</p> <ul style="list-style-type: none">• 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• application of defence in depth protective strategies to provide a high level of assurance that the program has adequate cyber security capability		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none">• addressing potential security vulnerabilities in each phase of the computer-based I&C systems lifecycle for computer-based systems important to safety• inclusion of security controls for a secure development environment during the development phases <p>A site specific program should include the following elements:</p> <ul style="list-style-type: none">• defensive strategy• asset identification, and security controls• roles and responsibilities• policies and procedures• awareness and training• configuration management• information protection• coordination with other security programs• incident reporting and recovery plan• program maintenance <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>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Security design requirements for computer-based I&C systems should be informed by vulnerability analyses. Vulnerabilities addressed in the design should include:</p> <ul style="list-style-type: none"> 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 non-performance of the safety functions by the systems in the presence of undesired behaviour of connected systems <p>The following should be considered for the protection of computer-based I&C systems and components important to safety functions:</p> <ul style="list-style-type: none"> the computer-based I&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 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 computer-based systems and components should include computer hardware, software, firmware, and interfaces both autonomous and non-autonomous computer-based systems or components subject to cyber security, should be protected computer-based systems and components for the functions of emergency preparedness system, physical security 		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>and safeguards, should be protected, if applicable for the design</p> <p>The computer-based I&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">• all systems, components and network cabling important to safety should be installed in a plant location that physically secures the equipment• 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)• unnecessary or unauthorized access to the setpoint adjustments and calibration adjustments should be limited• connections needed for temporary use should be disabled when not in use (e.g., connection of maintenance and development computers)• unused data connections should be disabled• all data connections for systems and components should be placed within enclosures• 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• access to the safety systems should be logged, and the security logs should be checked periodically• wireless communication should not be implemented for safety systems• safety systems should be designed such that virus protection software is not required		




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none">dedicated communication of plant data between the plant and the emergency support facilities (either onsite or offsite) should be provided using secure protocols <p>Security functions and security supporting functions of I&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">implementation should not adversely impact performance, including response time, effectiveness or operation of safety functionswhere practical, implementation directly in the safety system should be avoidedif implemented in safety system displays and controls, the security control should not adversely impact the operator's ability to maintain the safety of the plantif 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 functionssecurity controls within a safety system should be developed and qualified to the same level of qualification as the system in which the control resides		

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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"> • IAEA, Nuclear Security Series No. 17, Computer Security at Nuclear Facilities, Vienna, 2011. • IEEE, 7-4.3.2, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, Piscataway, New Jersey, 2010. • IEC, 61513, Nuclear Power Plant -Implementation and Control Important to Safety - General Requirements for Systems, Geneva, 2011. • NEI, 08-09, rev.6, Cyber Security Plan for Nuclear Power Reactors, Washington, D.C., 2010. • NEI, 10-04, rev.2, Identifying Systems and Assets Subject to the Cyber Security Rules, Washington, D.C., 2012. • U.S. NRC, Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, Washington, D.C., 2010. 		
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</p>	Due to sensitivity of information the assessment is documented elsewhere.	RNA

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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- 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"> • CNSC, RD-336, Accounting and Reporting of Nuclear Material, Ottawa, Canada, 2010. • CNSC, GD-336, Guidance for Accounting and Reporting of Nuclear Material, Ottawa, Canada, 2010. 		
7.24	<p>Future plant decommissioning and dismantling activities shall be taken into account, such that:</p> <ol style="list-style-type: none"> 1. 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 2. 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 3. consideration is given to the future potential requirements for storage of radioactive waste generated as a result of new facilities being built, or existing facilities being expanded <p>Guidance</p>	<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 A 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 12.1 of the Bruce A Operating Licence [PROL 15.00/2015].</p>	IC




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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">• CNSC, G-219, Decommissioning Planning for Licensed Activities, Ottawa, Canada, 2000.• CSA Group, N294, Decommissioning of Facilities Containing Nuclear Substances, Ottawa, Canada.• IAEA, TECDOC-1657: Design Lessons Drawn from the Decommissioning of Nuclear Facilities, Vienna, 2011.• IAEA, Safety Guide WS-G-2.1, Decommissioning of Nuclear Power Plants and Research Reactors, Vienna, 1999.• 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.• NEA, No. 6833, Decommissioning Considerations for New Nuclear Power Plants, Organization for Economic Cooperation and Development, Paris, 2010.		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
8.	System-Specific Requirements	This is not a requirement/guidance clause (this is a title only).	NA
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>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"> 1. withstand static and dynamic loading, including thermal expansion and contraction 2. withstand vibration (such as flow-induced and acoustic vibration) 3. ensure chemical compatibility, including service-related contaminants 4. meet thermal material limits 5. meet radiation damage limits <p>The reactor core design shall include provisions for a guaranteed</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 A Fuel and Reactor Physics document NK21-OSR-31000-00001, R001] 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 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 A licensing limits are provided in the OP&P [BP-OPP-00002, R012].</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</p>	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>shutdown state as described in section 7.11.</p> <p>The design of the core shall be such that:</p> <ol style="list-style-type: none"> the fission chain reaction is controlled during operational states 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>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>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 DEC's, are not exceeded, taking into account engineering</p>	<p>where acceptance of some permanent strain is necessary to be compatible with the functional requirements. In this case, the permanent strain limits can be calculated by the use of Tables N-421, N-421.1 and N0424. Deflections are limited under design 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 [NK21-SR-01320-00002, Rev. 005].</p> <p>System and component design pressures and temperatures are tabulated in Part 2, Subsection 4 of the Bruce A 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. 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 the Bruce A 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 A 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 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, Bruce A operation has not led to any unacceptable pressure tube fretting. Still, to mitigate against the possibility of fretting due to flow induced vibration of the inlet bundle, flow straighteners were considered for insertion into the inlet shield plugs of inner zone</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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&C to:</p> <ul style="list-style-type: none"> maintain the variables and systems within prescribed operating ranges monitor variables and systems that can affect the fission process over anticipated ranges for operational states, DBAs and DEC's 	<p>channels. It is yet to be determined whether Flow Straightening Inlet Shield Plugs or standard inlet shield plugs will be installed in Unit 4. 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. 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 A 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-PROG-12.02, R005] 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 design provisions for chemical control are presented in Section 11.2.3 of Part 2 of the Safety Report and the Chemistry Design Manual.</p> <p>As discussed in [RABA 0804] the Heat Transport system's main circuit provides reliable cooling of the fuel under all operating conditions for the life of the plant. The 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 5.1.2 of Part 2 of the Safety Report demonstrates the reliability of the HT system pressure boundary design and Section 5.1.3 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</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>These I&Cs should be demonstrated to be effective.</p> <p>Defence in depth</p> <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"> • prevention of unacceptable reactivity transients • shutdown of the reactor as necessary to prevent progression of AOOs to DBAs, or DBAs to DEC's • maintain and monitor the reactor in a safe shutdown state <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, 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"> • There is a high level of confidence that the proposed 	<p>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). It is noted that this requirement is applicable to PWRs and due to the unique design features of CANDU reactors this requirement cannot be met.</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 A 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 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. [RABA 0804].</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</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>design limits can be met within the expected operational range of the reactor, taking into account:</p> <ul style="list-style-type: none"> the analytical methods and data for the design calculations uncertainty analyses and experimental comparisons presented for the design calculations 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) special problems (such as power spikes due to densification), possible asymmetries, and misaligned reactivity devices 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: <ul style="list-style-type: none"> calculations (instrument-calculation correlations) involved in the processing operating procedures used the requirements for periodic check measurements the accuracy of design calculations used in developing correlations when primary variables are not directly measured the uncertainty analyses for the information and processing system the requirements for instruments, the calibration and calculations involved in their use, and the uncertainties involved in conversion of instrument readings into power distribution the limits and set points for control actions, alarms, or automatic trip for instrument systems and demonstration that 	<p>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 detailed guidance provided in this section is applicable to new reactor designs. It is noted that extensive tests were undertaken both prior to and since the start of operation using the 37 element fuel bundles in Bruce A. 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: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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)</p> <ul style="list-style-type: none">• measurements in previous reactors and critical experiments, including their use in the uncertainty analyses• measurements needed for start-up confirmatory tests and the required periodical measurements <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">• power generated in the fuel• power generated directly in the coolant and moderator• power generated directly in the core internals		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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 DEC. 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 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</p>		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>established.</p> <p>Conservatism should be considered based on:</p> <ul style="list-style-type: none">• the use of a coefficient (i.e., the analyses in which it is important)• whether state of the art tools have been used for calculation of the coefficient• the uncertainty associated with such calculations, experimental checks of the coefficient in operating reactors• any required checks of the coefficient in the start-up program following significant core reconfiguration <p>The design calculation should cover and be supported by the following:</p> <ul style="list-style-type: none">• 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• 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.• 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		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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 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">• a bounding value of power coefficient of reactivity has been calculated for all permitted operating states and used in control, stability, and safety analyses• 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• 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 <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</p>		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 suppressed.</p> <p>Assessment of reactor core stability should include:</p> <ul style="list-style-type: none"> • phenomena and reactor aspects that influence the stability of the nuclear reactor core • calculations and considerations given to xenon-induced spatial oscillations • potential stability issues, due to other phenomena or conditions • verification of the analytical methods for comparison 		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>with measured data</p> <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> <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 "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>		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The nuclear design should establish:</p> <ul style="list-style-type: none"> neutron flux spectrum above 1 million electron volts (MeV) in the core, at the core boundaries, and at the inside vessel wall, if applicable 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 computer codes used in the analysis the database for fast neutron cross-sections the geometric modelling of the reactor core, internals, and vessel(s) uncertainties in the calculations <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> 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. CSA Group, N286.7, Quality Assurance of Analytical, Scientific, and Design Computer Programs for Nuclear Power Plants, Toronto, Canada. CSA Group, N290.4, Requirements for reactor control systems of nuclear power plants, Toronto, Canada. CSA Group, CAN3-N290.1, Requirements for the Shutdown Systems of CANDU Nuclear Power Plants, Toronto, 		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Canada.</p> <ul style="list-style-type: none"> IAEA, NS-G-2.5, Core Management and Fuel Handling for Nuclear Power Plants, Vienna, 2002. IAEA, NS-G-1.12, Design of the Reactor Core for Nuclear Power Plants, Vienna, 2005. U.S. NRC, Regulatory Guide 1.77, Assumptions Used for Evaluating a Control Rod Ejection Accident for Pressurized Water Reactors, Washington, D.C., 1974. U.S. NRC, Regulatory Guide 1.203, Transient and Accident Analysis Methods, Washington, D.C., 2005. <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> <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</p>		



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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> <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: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

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 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.</p>		
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</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. The fuel bundles are made up of 37 cylindrical elements (pencils), which contain compacted and sintered uranium dioxide pellets in zirconium alloy sheaths. The fuel bundles are 495.3 mm (19.5 inches) long, the same as the bundles at Bruce B. The fuel channel cross-section and the 37-element fuel bundle cross-section are shown in Figures 4-20 and 4-21</p>	Gap


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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>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 testing and analysis, to ensure that fuel assembly requirements are met.</p>	<p>respectively. A summary of the 37-element fuel design data is given in Table 10-1. Table 10-2 lists fuel channel specifications and operating conditions. The fuel elements are held together in a bundle by end plates and are separated by spacers attached to the sheaths near the mid-plane of the bundle, as shown in Figure 10-1.</p> <p>Inter-element spacers are of the skewed split spacer type. One half of the spacer is attached to each of the 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 inches). The fuel is supported in the pressure tube on bearing pads located near the ends and middle of each outer fuel element.</p> <p>Qualitative acceptance criteria have been established to assess fuel and fuel channel integrity fitness-for-service (FFS) following an AOO. The 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 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 A 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.</p> <p>Fuel is designed for normal operating conditions with a nominal designated bundle power of 900 kW, while it is assessed for fission</p>	


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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 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>gas release and sheath strain for operation at 1035 kW. The operating envelope was derived from operating data from the four Bruce A Units covering a period of five years. The data were scaled up to full power. The envelope plotted covers 99.99 percent of bundle power histories, that is, less than 0.01 percent of bundles in the sample fall above the curve. Many test reactor irradiations have successfully demonstrated high power performance, including the following two on constant power in the NRU reactor at the Chalk River Nuclear Laboratories, as follows:</p> <p>One bundle (number HS) ran at an outer-element linear power of approximately 52 kW/m to a burnup of 200 MWh/kgU. Another bundle (number GA) ran at an outer-element linear power of approximately 70 kW/m to a burnup of 300 MWh/kgU [RABA0804].</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. Bruce Power is installing 37M fuel in Bruce A Units 3 and 4, and plans to install 37M in all Bruce A and Bruce B units. The 37-element CANDU fuel bundles used in Bruce A are readily inspectable in the new fuel storage area prior to loading and in the primary irradiated fuel storage bay after irradiation. In all accidents, other than large break LOCAs, the regulatory requirement is that fuel failures must be avoided. In order to do this derived limits are imposed which must be met during accident conditions. These limits depend upon the type of accident under study, but all are conservative enough to ensure that there is no distortion in the fuel that would render post-accident core cooling insufficiently effective [RABA 0804].</p> <p>The following mechanisms are identified to have the potential to cause fuel degradation under accident conditions:</p> <ul style="list-style-type: none"> – Fuel sheath strain. – Fuel (pellet)/cladding mechanical interaction. – Fuel pellet fragment axial relocation. 	

Article No.	Clause Requirement	Assessment	Compliance Category
	<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> <ul style="list-style-type: none"> • hydriding • cladding collapse • cladding overheating • fuel pellet overheating • excessive fuel enthalpy • pellet-clad interaction • stress-corrosion cracking • cladding bursting • mechanical fracturing <p>Fuel coolability</p> <p>Fuel coolability applies to DBAs and, to the extent practicable,</p>	<ul style="list-style-type: none"> – CANLUB degradation. – Iodine corrosion of the sheath. – Fuel element bowing and bundle deformation (including end plate deformation). – Fuel sheath collapse into axial gaps. – Lobe collapse or fuel sheath longitudinal ridging. – Sheath oxidation. – Hydride formation. – Hydride migration. – Pre-defected fuel element degradation (Fuel oxidation, sheath oxidation and embrittlement). – Sheath embrittlement or through-wall oxidation. – Beryllium assisted crack penetration. – Athermal strain. <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. For those DBAs where fuel cooling is an issue, the analyses have shown that, with the exception of the in-core LOCA, there is no damage to the reactivity control devices. For the in-core LOCA, the damage to shutoff rods has been evaluated and accounted for in the safety analyses.</p> <p>For a large break LOCA there may be some damage to the fuel, and in some cases distortion to the pressure tube, but sufficient post-accident cooling is available to ensure that the acceptance criteria are met and offsite dose limits are not exceeded [RABA 0804].</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</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>DECs. Fuel coolability criteria should be provided for all damage mechanisms in DBAs and DECs. 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 braze penetration.</p> <p>Other considerations</p> <p>The design should also include:</p> <ul style="list-style-type: none"> all expected fuel handling activities the effects of post-irradiation fuel assembly handling cooling flow of other components of LWR fuel assembly (such as control rods, poison rods, instrumentation, or neutron sources) <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</p>	<p>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 by performing pre-simulations of any change in fuelling strategy [RABA 0804].</p> <p>Operational Safety Requirements for Bruce A Fuel and Reactor Physics [NK21-OSR-31000-00001, R001] 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 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 A licensing limits are given in the Bruce A Operating Polices and Principles [BP-OPP-00002, R012].</p> <p>BP-PROC-00363, "Nuclear Safety Assessment", takes into account the effects of ageing and ensures the safety analysis provides a basis for safe operation.</p> <p>The impact of the condition of the pressure tubes on the thermal margin has been taken into account with new bundle designs such as the modified 37-element (37M) fuel bundle, and the consequences of this have been factored into the safety analyses (NK21-CORR-00531-09574).</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 NK21-CORR-00531-10943.</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>assembly (including LWR control 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 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</p>		




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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> <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"> • ANSI/ANS, 57.5, Light Water Reactor Fuel Assembly Mechanical Design and Evaluation, La Grange Park, Illinois, 1996. • CNSC, G-144, Trip Parameter Acceptance Criteria for the Safety Analysis of CANDU Nuclear Power Plants, Ottawa, Canada, 2006. 		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> 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. 		
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 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>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 A 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 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. SDS2 is equipped with double-ended coiled platinum detectors. These detectors are characterized by sensitivity to both neutron and gamma fluxes. The platinum and platinum-clad detectors are used for the reactor regulating system. 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. The setback parameters are scanned every 2 s and if a parameter is out of limits and reactor power exceeds the setback endpoint, demand power is ramped down at a suitable rate until</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>either the condition clears or the endpoint is reached. Each setback parameter has a unique setback rate and endpoint. If the SETBACK fails to control the power, and the STEPBACK setpoint is reached, the control absorbers drop into the core. 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.</p> <p>If the other computer also opens its control absorber clutch contacts, the clutches will be de-energized allowing 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 reactor power and re-closes the clutch partial absorber drop, but most STEPBACK conditions will cause the absorbers to be fully inserted. If process parameters other than flux move outside the normal control band, then the SETBACK and STEPBACK functions are activated as necessary. 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 required under these expectations. The control system in Bruce A 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, 28 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.</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>Detailed design description of reactivity control mechanisms is presented in Section 4.2.7 Part 2 of the Safety Report. The simultaneous adjustment of water level in all zone control compartments provides bulk reactivity control. The differential adjustment of the water level in individual zone compartments is designed to control the spatial power distribution.</p> <p>According to [RABA 0804], the control system is designed to ensure that serious process failures are limited to less than 1 in 3 years, in accordance with the Siting Guide to which the Bruce A reactors are licensed. The inherent characteristics of Bruce A 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>	



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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>Guidance</p> <p>Reactivity control</p> <p>The reactivity control should ensure that:</p> <ul style="list-style-type: none">the acceptable fuel design limits are not exceeded as a result of a wide range of AOOsno single malfunction of the reactivity control function can cause a violation of the acceptable fuel design limits <p>The nuclear design reactivity control requirements and control provisions should:</p> <ul style="list-style-type: none">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 isotopescompensate for the reactivity change caused by changing the temperature of the reactor from the zero-power hot		

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>condition to the cold shutdown condition</p> <ul style="list-style-type: none"> compensate for the reactivity effects caused by changing the reactor power level from full power to zero power assure reactivity management during the fuelling cycle, and intermediate times during the fuel cycle compensate for the effects on the power distribution and stability of the high cross-section neutron capture of the xenon-135 cover uncertainties associated with the control rods, including: <ul style="list-style-type: none"> manufacturing tolerances methods errors operation other than planned control element absorber depletion measurement uncertainty in shutdown margin demonstration <p>Reactivity devices configurations and reactivity worth</p> <p>The nuclear design should establish the following for reactivity device configurations, including (where applicable) control rod patterns, and reactivity worth for:</p> <ul style="list-style-type: none"> 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 predicted reactivity devices' worth and reactivity 		




Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design


File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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</p> <ul style="list-style-type: none"> allowable deviations from the patterns indicated above, such as for misaligned rods, stuck rods, or rod positions used for spatial power shaping 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 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 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 equipment, operating limits, and administrative procedures necessary to restrict potential rod worth or reactivity insertion rates 		
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</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</p>	IC


 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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>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</p>	<p>3.5 of Appendix 3 of the Bruce A Safety Report [NK21-SR-01320-00003, Rev. 004]. 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 to the bleed condenser and two relief valves on the bleed condenser shell 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 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. The heat transport system is generally isolated from interconnected systems through double isolation valves.</p> <p>For the Bruce A 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.</p> <p>Table 5-6 in Part 2 of the Bruce A Safety Report, lists the materials used for the major components in the HT system. The cobalt content is given in the table, where applicable. 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 5.1.3 of the Safety Report contains details on the zirconium alloy and 400 series steels. Carbon steel is used for the 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 is used as the steam generator tubing as it combines a high corrosion resistance to pitting, cracking and localized attack with a</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>meet – or contribute to meeting – the following objectives:</p> <ul style="list-style-type: none"> maintain sufficient reactor coolant inventory for core cooling both in and after all postulated initiating events considered in the design basis remove heat from the core after a failure of the reactor coolant pressure boundary, in order to limit fuel damage remove heat from the core in appropriate operational states, DBAs and DECAs with the reactor coolant pressure boundary intact transfer heat from other safety systems to the ultimate heat sink <p>The design of each reactor auxiliary system should ensure that automatic action by the system cannot impair a safety function.</p> <p>The design authority should demonstrate the adequacy of the following:</p> <ul style="list-style-type: none"> flow rate and pressure drops across major components major thermalhydraulic parameters, such as operating pressure and temperature ranges valve performance (flow, pressure drop, opening and closing times, stability, water-hammer) pump performance (head, flow, two-phase flow, seal performance) vibration of components and pipes control of gas accumulation (in particular, prevention of 	<p>low corrosion product release rate in both the HT and secondary side water. Incoloy is used for the pressurizer heaters.</p> <p>The design intent of the Bruce A 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 5.1.2.4), 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 5.1.3.4 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 Heat Transport System [NK21-OSR-33100-00001, R00] 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 submissions contain the technical basis of the Bruce Power HTS Aging Management Program and the Bruce A safety analyses, with aged HTS conditions, for Loss of Flow (LOF) events. The safety analysis results extend support for Bruce A Units 3 and 4 to operate at reactor power of up to 92.5% FP to 8250 Effective Full Power Days (EFPD), which is projected to be reached by approximately March 31, 2014 for the lead unit. The analysis results also support operation of Bruce A Units 1 and 2 at 92.5% FP to 3400 EFPD, representing approximately 10 years of operation. [F. Saunders to K. Lafrenière, "Bruce A HTS Aging Assessment", NK21-CORR-00531-07083 and F. Saunders to K. Lafrenière, "Bruce A Units 1 and 2 Return to Service: Loss of Flow Analysis to Evaluate Heat Transport High Pressure Trip Coverage", NK21-CORR-00531-08187]. 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 in Electrical System Failures were performed. The analyses demonstrate that where fuel sheath dryout cannot be precluded following LOF events at 92.5% FP, the HTHP and HTLF trips are effective in maintaining fuel sheath temperature below 600°C for the aged conditions under consideration. The results demonstrate that current dual parameter trip coverage for LOF events is acceptable to at least 3400 EFPD for Bruce A Units 1 and 2 and to</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>combustible gas accumulation)</p> <ul style="list-style-type: none"> • maximum allowable heat-up and cool-down rates • consideration of pressurized thermal shock due to operation (including inadvertent operation) of auxiliary systems • flow stability, including loop-to-loop stability and void-enthalpy oscillations (CANDU) • design of instrumentation taps <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"> • 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 • capability to withstand thermal shock, particularly in spray nozzles and connections to the main RCS circuit • control of pressure, such as via heaters, sprays, coolers or steam bleeding <p>Primary pressure relief</p>	<p>8250 EFPD for Bruce A Units 3 and 4 (corresponding to approximately March 31, 2014 for Units 3 and 4).</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 5.1.2.1.4 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 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. Special facilities are provided to detect moisture in the annulus gas system that may be attributed to a leak in a pressure tube. 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).</p> <p>Manual sampling capability was provided in the original design to allow the operator to monitor the integrity of the calandria tubes and pressure tubes, and to detect significant leakage from those</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


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"> • flow rate in single and two phase flow • consideration of corrosion of valve surfaces • provisions for ensuring that relief discharge does not lead to an unacceptable harsh environment inside containment • relief valve stability <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"> • primary pump performance characteristics, including head and flow characteristics, flow coastdown rate, single and two-phase pump performance • pump operating parameters (e.g., speed, flow, head) • pump net positive suction head needed to avoid cavitation • pump seal design and performance (including seal temperature limitations, if applicable) • vibration monitoring provisions <p>Additional information</p>	<p>components. Reactor Coolant Boundary Leakage Detection system is discussed in Section 5.1.2.6, 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 A design did not consider DEC's.</p> <p>As part of Fukushima related improvements, Bruce Power is implementing design changes to provide complementary design features which allow emergency makeup water to be added to the Bruce A primary heat transport system and moderator system. The water is provided by portable Emergency Mitigating Equipment (EME) pumps which are stored in a building adjacent to the site and at a higher elevation. This is tracked under AI 2014-07-3688.</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Additional information may be found in:</p> <ul style="list-style-type: none"> IAEA, NS-G-1.9, Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants Safety Guide, Vienna, 2004. 		
8.2.1	<p>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> <p>The design shall also facilitate surveillance in order to determine the metallurgical conditions of materials for which metallurgical changes are anticipated.</p>	<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, R020] describes the pressure boundary quality assurance program for Bruce Power Inc. for nuclear pressure boundary, and conventional pressure boundary activities in accordance with CSA Standard N285.0-08 including Update No.1 (2011). 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 currently has approved Certificates of Approval valid until 06-June-2016 that demonstrates compliance with CSA N285.0 2008 Update No.1 as per the PROL.</p> <p>The processes for ensuring compliance with inspections required by CSA N285.4 are addressed in separate supporting documents, which meet the N285.4 standard requirements. Bruce A Periodic Inspection Plan [e.g., NK21-PIP-03641.2-00001] identifies the systems, components, and areas that require periodic inspections; specifies the inspection methods and the inspection frequency. For example: B-PLAN-31100-00001 Fuel Channel Life Cycle Management Plan; B-PLAN-33125-00001 PHT Feeder Piping Life Cycle Management Plan etc. present the 6-year inspection plan for feeders and fuel channel pressure tubes.</p> <p>In order to provide access for maintenance and inspection, 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</p>	C

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>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 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>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 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 and a feed and bleed circuit. The system flowsheet is illustrated in Part 2 of the Safety Report [NK21-OSR-33100-00001 Rev. 005]. Figure 5-9 and the system design data are tabulated in Table 5-4 of the same chapter.</p> <p>The combination of the reactor coolant system and its associated systems, i.e., pressurizer, feed and bleed system and D2O storage system, can accommodate this requirement. The reactor coolant and pressurizer systems alone cannot cope with a cold shutdown on any CANDU [RABA 0804]. 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 D2O storage system in conjunction with the feed and bleed system. The HT bleed-flow flows through the bleed valves, to the bleed condenser, bleed cooler and</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>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.</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 [0A/1/2/3/4 Instrumentation Monitoring and Control Equipment Power Requirements During Extended Loss of AC Power, NK21-EPR-54900-0001]. During DEC's emergency power will be provided to critical monitoring instrumentation, including HTS header level, thereby allowing HTS inventory to be monitored.</p>	
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 5.1.1.5 of the Safety Report [NK21-SR-01320-00002, Rev. 005], the function of the Bruce A 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. Two banks of filters and ion exchange units (two filters and four ion exchange units per bank) are provided for purification of the HT bleed flow. Lithium is added to the HT coolant for pH control so lithium compatible ion exchange resins are used. A deuterium /hydrogen addition station is provided to limit the amount of oxygen in the system fluid resulting from radiolysis of heavy water. The filter vessels, including the cartridges, are of the disposable type.</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 6.0 HTS Coolant Activity of Bruce NGS A Heat Transport System OSRs [NK21-OSR-33100-00001, R00].</p> <p>The Safety Limit for steady state iodine content is defined to ensure that the radiological dose from postulated accidents (resulting in</p>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>release of coolant from the HTS system) will not exceed applicable regulatory limits. The applicable analysis that establishes the limit for Iodine-131 concentration is the assessment of consequential steam generator and preheater tube leaks arising from transient loads following DBAs or upset conditions documented in Section 6.8.3.2 of Appendix 6 Heat Transport Auxiliary System Pipe Breaks Outside Containment, Part 3 of the Safety Report [NK21-SR-01320-00003, Rev. 004]. The steady-state Iodine-131 content reflects the number of fuel defects that exist in the reactor core. The permissible HTS activity during steady state operation must account for the effect of Iodine-131 spiking, which transiently increases the radioactive content in the coolant when the reactor shuts down.</p> <p>The maximum Safety Limit on tritium concentration in the HTS coolant (3 Ci/kg) is set in Section 6.8.3.2 of Appendix 6 Heat Transport Auxiliary System Pipe Breaks Outside Containment, Part 3 of the Safety Report to minimize concerns regarding public doses from Design Basis Accidents with consequential Steam Generator tube leaks. This limit applies at all times operation or during transients) whenever the potential for a break in the HTS exists. The limit on tritium concentration is not affected by reactor power or HTS pressure.</p>	
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</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. The maintenance cooling system is also designed to permit the draining of</p>	IC




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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>steam generators and pumps.</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. The condenser steam discharge valves allow up to 60% reactor power to be discharged directly to the condenser for indefinite periods, and 75% reactor power to be discharged for short periods following severe turbine upsets. The condenser limit can be supplied either by the CSDVs alone or by the CSDVs at reduced load along with simultaneous steam flow through the turbine. This can allow an indefinite period at low turbine generator loads and still maintain the ability to quickly return to full power. The steam condensed in the condenser returns to the feed cycle and re-enters the steam generator.</p> <p>A review of the same clause in RD-337 indicated that the Bruce A design does not fully meet this requirement, as documented in [NK21-CORR-00531-11005]. The clause does not specify reliability requirements for this backup heat sink. As systems important to safety, in accordance with S-98, reliability models have been, or are being, developed for these systems. The review of singletons in the safety-related systems noted that there were some singletons in the Bruce A MCS and EBC systems that would result in the single failure criterion not being met, even if the worst condition were excluded. This latter exclusion would also mean that the systems would not meet the requirements of the single failure criterion prescribed in CNSC REGDOC-2.5.2.</p> <p>As part of the Bruce 1&2 Return to Service, a review of all the safety groups against the IAEA single failure criterion was performed and is documented in Enclosure 1 of [NK21-CORR-00531-04342]. This review looked at the Negative Pressure Containment System (including all sub-systems), Emergency Coolant Injection System, Shutdown Systems 1 and 2, Emergency Boiler Cooling System, and the Maintenance Cooling System. The results indicated there were no MCS or EBC system singletons that required action.</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
		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.	
8.3	Steam supply system	This is not a requirement/guidance clause (this is a title only).	NA
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>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>The changes introduced in this clause are editorial in nature and do not impact the intent of the requirement.</p> <p>Bruce A original design has not provided MSIVs, as this requirement did not exist at that time. However, 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>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 equipment is environmentally qualified. As described in Part 2, Section 6.7.3 of the Safety Report, the Bruce A PEVS is a standby safety support system designed to mitigate the consequences following a steam piping or feedwater piping failure. The fundamental function of the overall system is to protect Class I, II, III and IV power on all units by mitigating the consequence of secondary steam line breaks. 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. Similar to Bruce B, vertical centrally pivoted instrumented panels have been installed in the Main Control Room to prevent steam ingress.</p>	IC

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	Steam lines up to and including the first isolation valve and, where applicable, steam generators shall be qualified to withstand a DBE.		
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 DECAs.</p>	<p>The changes to the text in this clause are minor and do not impact the requirements.</p> <p>For Bruce A original design, protection of equipment from harsh environments was not a principal consideration in the system layout design. As a result, the Bruce A design has not considered the separation requirements. Environmental qualification of electrical and control systems was provided to mitigate the lack of separation. Section 8.3.2 of [RABA 0804] presents further justification; it is not practicable to consider changing the layout of the Bruce plant to meet the intent of this requirement.</p> <p>The Bruce A EQ program 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. The results of that review are given in EQ Requirements of Safety Related Systems and Structures for the Bruce A Nuclear Generating Station [NK21-EQR-03651-00001, R003] which demonstrates that enough systems have been qualified to ensure that the Control, Cool and Contain functions are maintained at Bruce A for a wide range of accident scenarios [RABA 0804].</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>	Gap
8.3.3	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>The second paragraph is modified to clarify the intention of the requirement.</p> <p>A review of the same clause in a draft version of RD-337 indicated</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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> <ul style="list-style-type: none"> • 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 • the over-speed protection system should meet the single-failure criterion, and should be testable when the turbine is in operation • 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 • 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 	<p>that the Bruce A design meets this requirement 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 10E-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. [RABA 0804].</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. For Bruce A, Section 2.5.2 of the Safety Report [NK21-SR-01320-00002] indicates that a feature incorporated into the design to provide an adequate level of protection against any credible turbine generator missile is the separation of the 600 V Class II switchgear (and associated Class I supplies), such that a single missile cannot disable both halves of the system. Further details are provided in Clause 7.15.1.</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> an in-service inspection and testing program for main steam and reheat valves should be established 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) 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 <p>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> 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. 		
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 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</p>	<p>A new requirement is introduced to cover reactor shutdown capability for DECAs.</p> <p>The safety analysis in Part 3 of the Safety Report [NK21-SR-01320-00003, Rev. 004] 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.</p> <p>Section 4.2.6 of Part 2 of Safety Report describes the two fully capable, separate, independent and diverse shutdown systems. Each</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 DEC's, 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>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>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>Following submissions to the CNSC on the restart of Bruce A Units 1 and 2, the CNSC requested that Bruce Power should re-examine the depth of shutdown for SDS1 and determine if it was practicable to increase the shutdown margin. The results of the SDS1 shutdown depth assessment confirm that Bruce 1&2 with a 12-bundle core configuration are within the limits determined for the existing safety case of Bruce 3&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>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 for Bruce Units 3 & 4 to calculate the margin to criticality provided by SDS1 following such events – Part 3, Appendix 4, Section 4.5.1.1 of the Bruce A Safety Report [NK21-SR-01320-00003, Rev. 004]. The</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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> <ul style="list-style-type: none"> 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 o diverse methods should be considered in the design of sensors, logic and actuation of the shutdown means <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>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), approximately 50 days from the initial startup of the reactor. 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 was also documented in the Bruce A Safety Report [NK21-SR-01320-00003, Rev. 004]. 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, at which time the operator can add poison to ensure continued indefinite subcritical state. SDS2 inherently has reactivity depth to maintain indefinite shutdown.</p> <p>As described in Section 4.2.6 of Part 2 of the Safety Report, SDS1 has 30 neutron absorbing rods that are referred to as shutoff rods. Each shutoff rod is a stainless steel-cadmium-stainless steel sandwich in the form of a tube with an active length of 5.65 m and an active outside diameter of 112.7 mm. The total static reactivity depth provided by inserting all the shutoff rods is 41 (± 3) mk for equilibrium fuelling conditions. With the two most effective rods missing, the static reactivity depth of the remaining shutoff rods is 31 (± 2) mk. The two effective rods are defined in such a way that when they are missing, the static reactivity of the rest is at a minimum. The liquid injection shutdown system consists of an arrangement of seven horizontal tubes with nozzles that are designed to inject heavy water poisoned with gadolinium nitrate into the moderator. SDS2 utilizes rapid injection of concentrated gadolinium nitrate solution into the bulk moderator through seven 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. SDS1 uses a spring assisted gravity rod drop as its actuation means. The rods are held out by a power driven clutch system and upon activation of the trip parameter, the power to the clutches is removed and the rods are inserted. Thus, no active power</p>	




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

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>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</p>	<p>mechanism is required to insert the rods in SDS1. SDS2 uses a poison injection system driven by stored energy in high-pressure gas tanks. 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>The Operational Safety Requirements for Bruce A Shutdown Systems [NK21-OSR-63720-63730-00001, R000] 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>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	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.		
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 extent of trip coverage provided by all available 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. With the exception of a few cases, trip coverage maps for the various events demonstrate that two trips are effective; however, the applicable trips to every event are not identified as direct or indirect trip (Gap). Acceptance criteria are not explicitly specified for AOOs. Further details are presented in the assessment against CNSC REGDOC-2.4.1 requirements in Safety Factor 5.</p> <p>As discussed in Safety Factor 5, the procedure on Nuclear Safety Assessment (NSA) [BP-PROC-00363], defines the elements, functional requirements, implementing procedures and key responsibilities associated with the NSA process. It states that 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. 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 are revised to reflect plant conditions applicable to the licence duration. The results of new analysis are consistently used to confirm the adequacy of the OLCs and if necessary used to derive a more</p>	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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>	<p>suitable value for use as an operating limit.</p> <p>The topic of trip coverage will be addressed as part of the comprehensive Bruce Power 2019 PSR.</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 Safety Report.</p>	




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none">• be quantifiable and well understood• 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• cover uncertainties in analysis, input plant and analysis parameters, as well as code validation <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 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>		

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Guidance on applying the requirements for number and diversity of trip parameters is given in REGDOC-2.4.1, Deterministic Safety Analysis.</p> <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>There are no changes to this requirement.</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&Ps 63.1 Shutdown System Availability [BP-OPP-00002, R012].</p> <p>As described in Part 2, Section 6.1.3 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 10E-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 A Shutdown Systems [NK21-OSR-63720-63730-00001, R000]. Section 2.1 SDS1 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 Internal Events At-Power</p>	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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>The reliability of the shutdown function should be such that the cumulative frequency of failure to shutdown on demand is less than 10E-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 10E-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>PSA NK21-03611.1 P NSAS (E10) - B1401/RP/005 Ver01 includes all sequences including failure to shut down into the fuel damage category FDC1, whose value is estimated as 4.65E-7 occurrences per reactor per year. Thus the guidance goal of cumulative frequency of failure to shut down on demand being less than 10E-5 is demonstrated by the fuel damage category FDC1 in the Level 1 PSA.</p> <p>Results of the Level 2 Internal Events At-Power PSA NK21-03611.5 P NSAS Ver1 indicate that the contribution to the large release frequency from all sequences involving failure to shutdown is about 2.3E-7 occurrences per reactor per year. Accordingly, the proposed safety goal of 10E-7/yr is not met, which constitutes a gap with respect to the guidance portion of this clause (Gap).</p>	
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</p>	<p>A new requirement for manual actuation and for monitoring shutdown status in the secondary control room is introduced.</p> <p>A review of the same clause in a draft version of RD-337 indicated that the Bruce A design meets this requirement, as documented in [RABA 0804]. All shutdown system actions that are required in the short term are automatic for all accidents considered at Bruce A.</p>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	control room.	<p>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 1-24 through 1-33 of Section 1 of Part 3 of the Safety Report [NK21-SR-01320-00003, Rev.004]. It can be seen that for the shutdown actions required by the operator there is substantial time for such actions, usually 15 minutes or more.</p> <p>The design requirements for Secondary Control Area function are presented in the Bruce A Secondary Control Area Design Manual [NK21-DM-63760-001, Rev. 00, January 2004]. The SCA and associated field panel areas provide control and monitoring capability remote from the MCR Complex to ensure that:</p> <ol style="list-style-type: none"> 1. Reactor units are shut down. 2. Reactor units are cooled down. 3. Common containment is maintained. <p>The above functions shall be accomplished by monitoring and controlling Unit 0, 1- 4, (and in particular the applicable Critical Safety Parameters (CSP)):</p> <ol style="list-style-type: none"> a. From the SCA and associated field panels, and b. By local field control actions. 	
8.5	<p>All water-cooled nuclear power reactors shall be 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</p>	<p>The changes are editorial in nature and provide clarifications rather than imposing new requirements.</p> <p>As described in Section 6.3.3.1 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. An inverted U-bend provides an air gap which forms an interface between the light water and heavy water systems. Four branch lines then penetrate the containment structure.</p> <p>Another source of water for ECI is the grade level tank. This tank is connected to the suction side of the four 50% ECI pumps, and is</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>possible mixing due to in-leakage.</p> <p>The ECCS shall meet the following criteria for all DBAs involving loss of coolant:</p> <ol style="list-style-type: none"> 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. 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>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>located north of Unit 4.</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>A possible third source of emergency coolant is gravity feed from the emergency water storage tank in the vacuum building. No credit is taken for this source of inventory, however, and the line connecting it to the common supply header is normally closed.</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 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. 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.</p> <p>The safety analysis documented in Part 3 of the Safety Report has</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>ECCS piping in an extension of containment that may contain radioactivity from the reactor core shall be subject to the following requirements:</p> <ol style="list-style-type: none"> 1. As a piping extension to containment, it meets the requirements for metal penetrations of containment. 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. 3. All ECCS recovery flow paths are housed in a confinement structure which prevents leakage of radioactivity to the environment and to adjacent structures. 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. <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 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>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&Ps, which states: The Emergency Coolant Injection System shall only be temporarily blocked from the control room following procedures approved by the Vice President, Bruce A Operations Division and under conditions concurred with by the CNSC.</p> <p>As described in Part 2, Sections 6.3.3 and 6.2.5.4 of the Safety Report, 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.</p> <p>ECI Pump room is classified as a confinement area and as such, there is monitoring for activity within the structure. Three sumps are located in the east service area/ECI recovery area, and normally discharge to the ALW collection tanks. The ECI recovery sump collects leakage from the recovery pump area. During high pressure ECI operation, discharge from the sump is returned to the containment ECI recovery sump. The ECI trench sump collects leakage from ECI piping and equipment in the pipe trench. The third sump in the east service area Room 040 collects drainage from the floor of the east service area. 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, Abnormal Incidents Manual (AIM) [NK21-OM-09034, Rev. 110] procedures direct the</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<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"> mechanisms for core bypassing (e.g., downcomer bypass during blowdown in PWRs, or core bypass via steam generators in CANDU) effects of non-condensable gas on ECCS performance phenomena that can impede core refill and rewet (such as periods of stagnation, steam binding in PWR steam generators, parallel channel effects in CANDU) effect of multi-dimensional flow in heat transport system headers in CANDU 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) effect of the pressurizer 	operating staff to sample for heat exchanger leaks following a LOCA.	



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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">the design is capable of recirculating coolant even in the presence of the maximum quantity of debris that may be present after a LOCApossible chemical effects in the reactor 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)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 transferwear on bearings and seals has been considered, including abrasion by small particles and chemical corrosionnatural 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 <p>Sections 7.14 and 7.16 describe the inspection, test and maintenance requirements which should include:</p> <ul style="list-style-type: none">commissioning tests to verify flow, pressure drop and (if applicable) tank isolation after injection for accumulators and other makeup tanks		




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> commissioning tests to verify pump head, flow and system pressure drop for pumped injection <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 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	Containment	This is not a requirement/guidance clause (this is a title only).	NA
8.6.1	Each nuclear power reactor shall be installed within a containment	The new text added is mostly clarification rather than imposing new	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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"> 1. the containment structure and related components 	<p>requirements.</p> <p>As described in Section 6.2 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 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.</p> <p>In addition to the containment system, there are three confinement areas for each unit. They consist of the moderator confinement area, the instrument room confinement area, and the miscellaneous equipment room confinement area. There is also the high-pressure emergency coolant injection recovery room area common to all four units. These are areas outside the main containment envelope where failure of a system could result in a limited release of activity but where there is little stored energy in the systems involved, or where the integrated energy release would be small. These confinement areas are enclosed and ventilated in such a way that activity release from these areas can be adequately controlled. The moderator and auxiliary confinement areas are provided with a separate D2O vapour recovery system.</p> <p>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 that a closed envelope is provided to</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2. equipment required to isolate the containment envelope and maintain its completeness and continuity following an accident</p> <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>contain potential activity in the event of an accident.</p> <p>Twelve main pressure relief valves, four instrumented 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.</p> <p>The dousing system consists of an emergency water storage tank in the top of the vacuum building and a system of spray headers. 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.</p> <p>The equipment to pump down and maintain the vacuum building pressure, and the equipment to circulate the water in the elevated storage tank, is located in the vacuum building basement (which is not a part of containment). Heat removal from containment is provided by an air-to-water cooling system. 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 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 valves. Each filter contains a demister, heater, prefilter, upstream HEPA filter, charcoal filter and</p>	


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>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. Several upgrades to the system are underway to meet the reliability target and the current Provincial Emergency Preparedness guidelines.</p> <p>In regard to severe accidents, it should be recognized that Bruce A 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 A original design for the containment system has not provided complementary design 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>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.</p> <p>In regard to its potential role as a complementary design feature, the Bruce A 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</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
		<p>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 initiates this containment isolation.</p> <p>As discussed in [RABA 0804] 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 [NK21-OM-09034, Rev. 113] 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>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. The instrument air for Unit 0, the common services area, is supplied by the service air system. Each reactor unit has three compressors, one operating and two on standby, each with a capacity of 282 L/s (600 scfm). The normal</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<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"> • containment penetration isolation times • containment spray performance • filtered venting capability • vacuum building actuation • hydrogen mitigation system capability (e.g., recombiners) • systems and equipment used for containment heat removal • concrete condition and possible concrete degradation <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"> • CSA Group, N287.3, Design Requirements for Concrete Containment Structures for CANDU Nuclear Power 	<p>steady demand is about 282 L/s (600 scfm) and the maximum unit demand is 470 L/s (1,000 scfm). Two 100% air dryers of 470 L/s (1,000 scfm) capacity are provided per unit. The individual instrument air systems are provided with air receivers of sufficient capacity to supply air during a Class IV power failure until Class III power becomes available.</p> <p>Manual inter-unit instrument air ties are provided between Units 1 and 2, Units 3 and 4, and Units 0 and 2 in the event of instrument air supply unavailability in a given unit. Instrument air for the service area is taken from the service air system through two 100% air dryers of approximately 377 L/s (800 scfm) capacity. In the event of Class IV power failure, only instrument air will be available from the service air system.</p> <p>Thus, the instrument air system is backed up by Class III power. Should all power fail, then the vault vapour recovery system inlet and outlet dampers would fail closed, isolating containment.</p> <p>The instrument air system has been environmentally qualified to ensure containment boundary requirements and to provide monitoring capability of the post-accident radiation monitoring system (PARMS).</p>	


 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	Plants, Toronto, Canada. <ul style="list-style-type: none"> CSA Group, N290.0/N290.3, package, General requirements for safety systems of nuclear power plants and Requirements for the containment system of nuclear power plants, Toronto, Canada. 		
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> <ol style="list-style-type: none"> effects of other potential energy sources, such as possible chemical reactions and radiolytic reactions limited experience and experimental data available for defining accident phenomena and containment responses conservatism of the calculation model and input parameters <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</p>	<p>The changes are editorial in nature and have no impact on the requirements.</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 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 test pressures for the containment envelope are summarized in Section 6.2.2.1 of Part 2 of the Safety Report.</p> <p>These values 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. According to Section 6.2.2.1 of Part 2 of the Safety Report, the design target leakage rate for the containment boundary, except for the vacuum building, was set at 1 percent of the total contained mass per hour at: 68.9 kPa gauge (10 psig) for the reactor vaults and fuelling duct fuelling machine rooms: and, 62 kPa gauge (9 psig) for the pressure relief duct and pressure relief manifolds. However, safety analysis is performed assuming a higher limit in order to assure margins. The operational target leak rate for the main volume of the vacuum building is 47 L/s (100 scfm) at 7 kPa (a) (1 psia), and for the upper chamber it is 1.4 L/s (3 scfm). Containment pressure is continuously monitored and periodically tested to demonstrate that the leakage</p>	C

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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>requirements are being met.</p> <p>The SMA [NK21-REP-03611-00005, Rev. 000] documents the assessment of the containment system capability to survive an RLE. It was concluded that the Bruce A structures could not be screened out simply on the basis of the EPRI screening criteria. However, due to the similarity of the Bruce A and the Bruce B structures, it was concluded that the structures could be screened by comparison to Bruce B. Bruce B was designed by dynamic analysis for a DBE, defined as a Regulatory Guide 1.60 ground motion spectrum anchored to 0.05 g.</p> <p>According to [RABA 0804], with regard to the strength of the containment above design pressure, the concrete containment at Bruce is robust. Superficial cracking would begin at 140 kPa (g) with no increase in expected leak rate. The transition from elastic to plastic behaviour occurs at 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.</p>	
8.6.3	<p>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>	<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 A Containment System [NK21-OSR-34200-00004, R001] describes the containment envelope and presents the safety limits and surveillance requirements for the systems and its components.</p>	C


 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>Airlocks can be tested individually. 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 6.2.2.7 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. Bruce NGS A CSA N287.7-08 Periodic Inspection Program for Bruce NGS A Concrete Containment Structures and Appurtenances (Excluding Vacuum Building) [NK21-PIP-21100-00001, R002] 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 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 A CSA N287.7-08 Periodic Inspection Program for Bruce NGS A Vacuum Building [NK21-PIP-25100-00001, R001]. 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. The current period between inspections is 12 years.</p>	
8.6.4	Leakage rate limits	The text in item 2 under Test Acceptance Leakage Rate Limits is modified and now refers to applicable codes and standards.	IC


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The safety leakage rate limit shall assure that:</p> <ol style="list-style-type: none"> normal operation release limits are met AOOs and DBAs will not result in exceeding dose acceptance criteria <p>The design leakage rate limit shall be:</p> <ol style="list-style-type: none"> below the safety leakage rate limit as low as is practicably attainable consistent with state-of-the-art design practices <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>Bruce A containment design does not match the state of the art design practice in leakage rates as described in the Guidance. Bruce A containment meets the current CNSC requirements for licensing basis events, and dose acceptance criteria for DBAs.</p> <p>As described in Section 6.2.2.1 of Part 2 of the Safety Report [NK21-SR-01320-00002], the design target leakage rate for the containment boundary, except for the vacuum building, was set at 1 percent of the total contained mass per hour at: 68.9 kPa gauge (10 psig) for the reactor vaults and fuelling duct fuelling machine rooms: and, 62 kPa gauge (9 psig) for the pressure relief duct and pressure relief manifolds. However, safety analysis is performed assuming a higher value (2.32%) [NK21-SR-01320-00003] in order to assure margins. The operational target leak rate for the main volume of the vacuum building is 47 L/s (100 scfm), and for the upper chamber, it is 1.4 L/s (3 scfm), both at 7 kPa (a) (1 psia).</p> <p>The repressurization time calculated for the Bruce A intact containment is 46 hours, taking no credit for reverse flow function and assuming containment leakage at 2.32 percent volume/hr, compressed air in-leakage at 400 kg/hr. Sensitivity studies show that the repressurization time is 51 hours if the reverse flow function of an APRV is credited. The repressurization time is 88 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.</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 repressurization times has been assessed. The repressurization time is reduced by 10 hours for a large break LOCA scenario, resulting in a repressurization time of 36.4 hours.</p> <p>Further detailed information on the appropriate limits, and the basis for these limits, can be found in the Bruce A OSRs for containment [NK21-OSR-34200-00004], Operational Safety Requirements For Bruce A 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</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<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>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> <ul style="list-style-type: none"> CSA Group, N287.7, In-service Examination and 	<p>operational. The licensing limits used are specified in Appendix A of the OP&Ps., Section 21 and Appendix 21 Negative Pressure Containment System.</p> <p>The containment envelope (excluding the vacuum building) is maintained at all times at a slightly negative pressure -2.5 to -3.5 kPa gauge. This pressure is monitored in the control room. The system is sensitive enough to pick up changes in pressure caused by breathing air from any workers in containment and is readily capable of detecting any gross breach of the containment envelope. The vacuum building is normally maintained between 6.9 and 10.3 kPa absolute and again monitoring of this value from the control room will readily detect any gross breach. As described in [RABA 0804], since the containment at Bruce A 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 leakage rate value of 2.32 percent 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 are for single and dual failure events. 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 10E-5 per reactor year but less than 10E-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 A would meet the proposed limit using the 2.32% 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 noted earlier, currently there is no AOO classification for Bruce A. See Section 4.4.1 for further discussion on this topic.</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Testing Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, Toronto, Canada.</p> <ul style="list-style-type: none"> CSA Group, N287.6, Pre-operational proof and leakage rate testing requirements for concrete containment structures for nuclear power plants, Toronto, Canada. 		
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>Keeping the number of penetrations through the containment to a minimum should consider the need for separation and</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 6.2.2.7 of Part 2 of the Safety Report.</p> <p>Regarding inspection of penetrations, as discussed in Clause 8.6.3, Bruce A periodic inspection program for the containment structure and related components was developed to comply with CSA N285.5-M90 Periodic Inspection of CANDU Nuclear Power Plant Containment Components.</p> <p>Bruce A does not meet the requirement for leak testing at the containment design pressure of resilient seals. Bruce A was 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 [RABA 0804].</p> <p>As documented in [NK21-CORR-00531-11005] the Bruce A vacuum type containment was not designed with testing capability for</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	redundancy, and be consistent with modern designs.	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 6.2.4 of the Safety Report [NK21-SR-01320-00002]. 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>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>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 6.2.2 of the Safety Report, the Bruce A 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>As documented in [NK21-CORR-00531-11005] Bruce A has piping systems penetrating containment that do not have redundant isolation valves. In the 1990's, a report was prepared on containment extensions at Bruce A [Ontario Hydro D&D Report 920232]. 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>The benefit of double isolation valves for the MCS was assessed for</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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>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"> 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. 2. All piping and components that are open to the containment atmosphere shall be designed for a pressure greater than the 	<p>Bruce 1&2 [NK21-CORR-00531-04342]. The assessment concluded that it is not practicable to make the change.</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>Many of the systems that connect to the PHT and penetrate containment have two isolation valves, but not all of them. One area where Bruce A does not comply with this requirement is for reactor cooling systems that penetrate containment. The maintenance cooling system has four isolation valves, one in each line penetrating containment, inside the containment wall. The ECI system contains dual isolation valves (inside containment) in the unit portion of the system that penetrates the reactor vault.</p> <p>As presented in [RABA 0804] in 1990 a report was prepared on containment extensions at Bruce A. This review covers all types of containment extensions, be they attached to the PHT or just to the containment atmosphere. Thus, while all of the systems at Bruce A were not specifically designed with this requirement in mind, the report has clearly identified where the second isolation point is for each extension, and thus the intent of the requirement for dual isolation has been met. This issue is discussed more fully in the comparison of Bruce A against the Darlington Design Guides, which was issued for the Bruce A Units 1&2 restart.</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. These include the six air dryer systems, the tritium monitoring system and the vacuum pump suction and discharge lines. The six air dryer systems include one for each vault, one for the central fuelling area and one</p>	




Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design


File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>containment design pressure.</p> <p>3. The piping and components shall be housed in a confinement structure that prevents leakage of radioactivity to the environment and to adjacent structures.</p> <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"> 1. two automatic isolation valves in series for lines that may be open to the containment atmosphere 2. two closed isolation valves in series for lines that are normally closed to the containment atmosphere 3. the line up to and including the second valve is part of the containment envelope <p>Closed systems</p>	<p>for the east service area. Each system consists of a loop of ducting from the containment 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. The central fuelling area system has no filter bank. The exhaust is to the irradiated fuel storage bay exhaust system, and a purge line is taken to each of the two dryers. 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. Potentially open flow paths communicating with water in the vacuum building are isolated by the operator-issued signal to motorized valves (i.e., the vacuum building active drainage lines). The lines up to the second valve have all been identified for inspection programs because they are considered as extensions of containment.</p>	


 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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"> 1. they meet the applicable service piping standards and codes 2. they can be continuously monitored for leaks 		
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>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>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. Access is provided to: the reactor vaults (AL2 to AL6 and TC5); the central fuelling machine service area (TC1 to TC4); the east fuelling machine service area (AL18); the fuelling machine duct (AL11, AL16 and AL17); the pressure relief ducts (AL12 and AL15); the pressure relief valve manifold (AL20, TC6 and TC7).</p> <p>With the exception of AL3, each airlock and transfer chamber has a set of doors, each of which can withstand the post-accident environment. With the exception of airlock AL3 and transfer chamber TC6, each door has a double set of inflatable seals and can also</p>	IC


Article No.	Clause Requirement	Assessment	Compliance Category
	<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>withstand the post-accident environment. These latter devices consist of a pair of bolted doors with compression seals. The bolted doors can only be opened when containment is not poised. Airlock AL2 and transfer chambers TC1 to TC5 have "composite doors" (i.e., a small personnel door integrated into the larger equipment door). AL3 is a special case as this equipment airlock is used to move long items (e.g., fuel channels, or fuel channel flasks) in or out of containment. Normally only the inner airlock door is closed. The airlock chamber and outer door are installed only if the airlock is to be used, and sealing surfaces are checked by pressurizing the airlock before either door is opened. 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 position.</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. At this time, an Airlocks Rehabilitation Program is underway. The proposed modifications will result in significant improvements to the airlocks and transfer chambers and to the Negative Pressure Containment System as a whole. The main objectives of the program are:</p> <ul style="list-style-type: none"> • To reduce predicted future unavailability of the airlocks and transfer chambers, thus minimizing their contribution to overall containment unavailability. • Specifically address concerns related to prevention of breach of containment resulting from Single Component Failures. • To improve the overall operation of the airlocks and transfer chambers through considerably reducing significant 	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>maintenance requirements.</p> <p>In order to achieve these objectives, several significant changes have been proposed. The two most significant modifications are:</p> <ol style="list-style-type: none"> 1. The addition of dual redundant air supplies for all airlocks and transfer chambers. 2. The modification of the equalizer valves to make them neutral position type, which ensures normally available two-door containment boundary [RABA 0804]. <p>With respect to the equalizer valve, it is normally open to the containment. If it is set in the neutral state as suggested by the proposed modification, then a small leak of compressed air in the airlock chamber would pressurize it. Such pressurization would increase the escape time for an operator trying to leave the containment in an emergency. Furthermore, under any residual pressure the door may blow open on the operator when the latch is operated to open the door. Therefore, the modification to put the equalizer valve to neutral state is not being considered at this time. The provision being made for dual air supply with back-up tanks should ensure that unavailability target for the containment system is met [RABA 0804].</p>	
8.6.8	<p>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> <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</p>	<p>There is a new requirement to account for DEC.</p> <p>The Bruce A 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..."</p> <p>[0804 RABA] further states that 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 steel liner, these local overstresses, though beyond the elastic design</p>	IC


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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"> CSA Group, N291, Requirements for Safety-Related Structures for CANDU Nuclear Power Plants, Toronto, Canada. 	<p>limits, present no concern with respect to the containment leak-tightness. Temperature transients accompanying hydrogen burns do not affect containment integrity. The Bruce A 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. 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.</p> <p>In addition, as described in Section 6.2.2.10 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 Ignition System for mitigation of short term hydrogen generation.</p> <p>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 which could result from potentially more severe pressure/temperature transients associated with hydrogen combustion. The system consists of 16 ignitors per unit (64 ignitors/station) located in the reactor vaults and fuelling machine ducts. The ignitors 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.</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>	


 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
		<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. 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. The system consists of 4 PAR units located nominally at elevation 649' with one PAR unit in each quadrant of the reactor vault (Currently installed in Units 1, 2, and 4 only). In addition, PAR will also provide short term hydrogen mitigation while the hydrogen ignition system is active.</p> <p>Bruce A PARs project is underway and is required to provide mitigation of the potential build up of hydrogen gas in the reactor vaults or other areas of Containment during a severe accident.</p>	
8.6.9	<p>The design shall enable heat removal and pressure reduction in the reactor containment in operational states, DBAs and DECs. Systems designed for this purpose shall be treated as part of the containment system, and are capable of:</p> <ol style="list-style-type: none"> 1. minimizing the pressure-assisted release of fission products to the environment 2. preserving containment integrity 	<p>The change is editorial, i.e., "all plant states" are replaced with "operational states, DBAs and DECs"; hence no change in the requirement.</p> <p>As described in Part 2, Section 6.2.2.4 of the Safety Report, the dousing system consists of an emergency water storage tank in the top 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, over the weir created in the upper vacuum chamber and sprays from the headers to the vacuum building main 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.</p>	IC


Article No.	Clause Requirement	Assessment	Compliance Category
	<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"> • pressure suppression pools, ice condensers, vacuum chambers • containment coolers and fans • sump or in-containment water cooling systems used as part of a LOCA recirculation • passive containment cooling • containment spray or dousing systems • free volume inside the reactor building • containment venting through filters or scrubbers <p>Pressure and energy management equipment 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</p>	<p>The dousing system is part of the Containment system that has an overall reliability of 10E-3 a/a.</p> <p>Heat removal from containment during normal operation is provided by a number of coolers. Each reactor vault has four axial fans and 10 main air-to-water heat exchangers. In addition, each vault has six wall-mounted coolers. Both the main coolers and the wall-mounted coolers are on Class III power, however, the wall-mounted units are manually started. 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.</p> <p>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 [RABA 0804].</p>	

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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>		
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"> 1. reduce the amount of fission products that might be released to the environment during an accident 2. prevent deflagration or detonation that could jeopardize the integrity or leak tightness of the containment <p>The design shall also:</p> <ol style="list-style-type: none"> 1. provide isolation of all sources of compressed air and other non-condensable gases into the containment atmosphere following an accident 2. ensure that, in the case of ingress of non-condensable gas resulting from a PIE, containment pressure will not exceed the design limit 3. provide isolation of compressed air sources to prevent any 	<p>There are no changes to the requirement.</p> <p>According to [NK21-CORR-00531-11005] 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) [NK21-OM-09034, Rev. 110] 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 6.2.2.11 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 subatmospheric 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 subatmospheric hold up period. An alternate exhaust path from the pressure relief valve manifold also is available.</p> <p>As discussed in Clause 8.6.8, the hydrogen ignition system is</p>	IC

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	bypass of containment	<p>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 16 ignitors (12 in the reactor vault and 4 in the fuelling machine duct) per unit (64 ignitors/station). The ignitors 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. In addition, two catalytic hydrogen recombiners are installed in Units 3 and 4 on a trial basis.</p> <p>Bruce A PARs project is underway to provide mitigation of the potential build up of Hydrogen gas in the Reactor Vaults or other areas of containment during a severe accident scenario.</p> <p>Bruce Power is considering the 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. The dual isolating valves for the containment bypass "T" in the EFADS piping will be available by approximately January 2015. Installation will be undertaken at the first dual Station Containment and Vacuum Building outage following January 2015. The purpose of the bypass line and isolation valves is to allow containment filtered venting system to be installed at a later date without the need for an additional containment outage. A decision regarding the installation of a passive filter will be provided to the CNSC by December 2015.</p>	
8.6.11	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	<p>A new requirement for selection of coverings and coatings is added,</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</p>	IC


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 include:</p> <ul style="list-style-type: none"> insulation materials, corrosion products, delaminated paints and coatings that may foul ECC recovery flow paths or prevent operation of equipment 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 materials that may react under post-accident conditions to generate combustible, corrosive or poisonous gases <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>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.) will 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 on Bruce A restart by replacing the strainer with a larger area device, and crediting analysis at Bruce B that shows the ECI recovery flow would not be lost due to suspended fibres. The calcium silicate insulation was removed on Units 3&4 and on Units 1&2 prior to restart.</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 A containment is coated with inorganic zinc primer. This type of paint can remove 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 [RABA 0804].</p>	
8.6.12	Following onset of core damage, the containment boundary shall be capable of contributing to the reduction of radioactivity	A new requirement for the complementary design features is introduced in item 4. "DECs" replaces "severe accidents" in the third	Gap


 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 (DECs) shall be demonstrated in design documentation, and shall include the following considerations:</p> <ol style="list-style-type: none"> 1. various heat sources, including residual heat, metal-water reactions, combustion of gases, and standing flames 2. pressure control 3. control of combustible gases 4. sources of non-condensable gases 5. control of radioactive material leakage 6. effectiveness of isolation devices 7. functionality and leak tightness of airlocks and containment penetrations 	<p>paragraph.</p> <p>A review of the same clause in RD-337 indicated that the Bruce A design does not fully meet this requirement, as documented in [NK21-CORR-00531-11005]. Bruce A 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 DECs. 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 or temperature transients associated with hydrogen combustion, as described in Section 6.2.2.10 of Part 2 of the Safety Report [NK21-SR-01320-00002]. Bruce Power is considering Containment Filtered Venting Systems (CFVS) and has included the necessary containment bypass tees and containment boundary isolating valves in the upcoming vacuum building outage work schedule.</p> <p>Bruce Power has installed PARs in Bruce A units 1, 2, 3, and 4. Bruce Power has submitted the long-term mixing analysis to support the determination of the number of PARs in both Bruce A and Bruce B containments. [Bruce Power – Performance Review of Bruce A and Bruce B – 2013].</p> <p>The Bruce A containment floor was not constructed with concrete used to limit the production of non-condensable gases due to core-concrete interactions. However, the concrete containment floor and, in particular, the fuelling vault floor, will withstand corium concrete interaction assuming that there is sufficient water on containment floor and sufficient floor surface area for corium relocation. Bruce Power is evaluating various options for longer-term provisions to ensure core cooling and In Vessel Retention (IVR) of corium debris in the event that an accident has progressed to a severe accident. These options include makeup water to the calandria, PHTS and shield tank. Bruce Power will continue to review the benefits of and the need for the installation of additional provisions for core cooling using emergency makeup provisions to the heat transport, moderator</p>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>8. effects of the accident on the integrity and functionality of internal structures</p> <p>The design authority shall demonstrate that complementary design features have been incorporated that will:</p> <ol style="list-style-type: none"> 1. prevent a containment melt-through or failure due to the thermal impact of the core debris 2. facilitate cooling of the core debris 3. minimize generation of non-condensable gases and radioactive products 4. preclude unfiltered and uncontrolled release from containment <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 implementation of offsite emergency measures. This period should be demonstrated, with reasonable confidence, to be</p>	<p>and shield cooling systems. The review will consider the Bruce specific analysis described above, the results of the CANDU Owner's Group (COG) post-Fukushima Joint Project (JP-4426) review of IVR, and the results of a Risk Informed Decision Making (RIDM) -based assessment. The original design did not include complementary design features for severe accidents; therefore this is assessed as a gap. (Gap 2)</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 6.2.2.11 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 subatmospheric 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 subatmospheric 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, 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"> • Enhancement of SAMG to include multi-unit events and IFB events. • Assessment of instrument and equipment survivability under severe accident and identification of equipment upgrades required. 	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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"> • ignition of flammable gases • generation of non-condensable gases • impact on filters by containment environmental conditions, such as radioactive materials, high temperature and high humidity <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>	<ul style="list-style-type: none"> • Assessment of plant habitability under severe accident conditions and identification of modifications required. • Improvement to understanding of severe accident phenomena including containment integrity, hydrogen production, aerosol behaviour, and in-vessel retention. <p>These actions are tracked through Station Specific Actions.</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. All systems 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</p>	<p>A new requirement is added to cover DEC.</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 the Emergency Boiler Cooling 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 Qualified Power Supply. Service water to heat exchangers and other components is supplied via the Unit Low Pressure Water Service System, the High Pressure Recirculating System or the Common Service Water System.</p>	IC

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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"> 1. acceptable conditions can be maintained in SSCs needed for mitigation of severe accidents 2. radioactive materials can be confined 3. releases to the environment can be limited <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>The Seismic and Environmental Programs that have been undertaken at Bruce A 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 [RABA 0804].</p> <p>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>The seismic and environmental programs that have been undertaken at Bruce A have demonstrated that the essential parts of the existing systems are capable of meeting their environmental and seismic requirements.</p> <p>As part of Fukushima enhancements and station improvements plans a project is initiated to provide complementary design features which allow emergency makeup water to be added to the Bruce A primary heat transport systems and moderator systems. The water is provided by portable Emergency Mitigating Equipment (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. This project is in the preliminary engineering phase. Design Requirements have been established and the locations of the connection points for quick connect installation have been identified. A Preliminary Design Plan has been prepared and walkdowns have taken place. Installation of the connections will be linked to outage schedules. Installation in all four units is targeted for completion by end of 2015 [NK21-CORR-00531-10873].</p> <p>Bruce Power is making short-term provisions and longer-term</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
		<p>provisions to provide make-up water to critical systems. The short-term provisions are either complete or are underway as follows:</p> <ul style="list-style-type: none"> • Modifications to allow emergency water to be added to the SGs via Emergency Boiler Cooling (EBC) system at Bruce A and the Emergency Water System (EWS) at Bruce B have been completed in all units. • The design of an alternate method of providing makeup water to the SGs using the Inter Unit Feedwater Ties (IUFT) is complete • 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>In addition as described in [B-REP-00701-09DEC2013-060] Bruce Power will increase the water level indication range in the Bruce A Fuelling Machine Duct ECI sump. In response to a beyond design basis accident resulting in loss of heat sink, water could be added to the reactor core to prevent fuel melting or, if fuel failure has occurred, to stabilize the accident. Knowledge of the water level inside containment is important to ensure that containment is not breached due to excessive water level in the Fuelling Machine Duct. Adequate level indication can also be used to ensure that any molten corium that has relocated to the concrete floor remains covered. Bruce Power committed to the modification to the level transmitter in [Letter, F. Saunders to K. Lafrenière, "Bruce Power Response to the CNSC Request Pursuant to Subsection 12(2) of the General Nuclear Safety and Control Regulations: Lessons Learned from Japanese Earthquake – July 28, 2011 Submission, NK21-CORR-00531-08831 / NK29-CORR-00531-09544]. The installation is targeted for completion by December 2017, as discussed in supporting documentation for NK21-CORR-00531-11567.</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 required to</p>	<p>A new requirement is introduced for the EHRS to function during DECAs, if required.</p> <p>As documented in [RABA 0804], Bruce A design does not provide this fifth (special) safety system, as these requirements were intended for new build NPPs. For Bruce A, the emergency heat removal function is provided by Emergency Boiler Cooling, Shutdown</p>	Gap



Rev Date: July 8, 2016


Status: Issued

Subject: Safety Factor 1 - Plant Design


File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 DECs, 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 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</p>	<p>Cooling, and Maintenance Cooling Systems.</p> <p>The emergency heat removal function is provided by the Emergency Water System, the Shutdown Cooling System and the Maintenance Cooling System. A redundancy and diversity assessment of these systems was performed for Bruce 1&2, and it was concluded that changes to plant design and procedures are not warranted.</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>The maintenance cooling system is normally used for completion of cooldown to less than 35°C after the shutdown cooling system has reduced the HT system temperature to 54°C (130°F) and could be used to cool down the HT system from 160°C (326°F) in the event the shutdown cooling system is unavailable. The maintenance cooling system is designed to withstand HT system temperature and pressure, and is classified as a Class I system in accordance with Section III of the ASME Code 1971 Edition with Winter Addenda [Section 5.1.1.3.3 of Part 2 of the Safety Report].</p> <p>The shutdown cooling circuit is designed to cool the HT system from 177°C (35°F) to 54°C (130°F) and to hold it at the latter temperature for an indefinite time. The system utilizes the preheaters and main HT pumps to transfer heat from the HT system coolant to a demineralized water recirculation loop. The system is shown in Figure 5-8 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 HT system be pressurized to allow main HT pump operation. The shutdown cooling system must also be pressurized by use of the boiler feedwater pumps to prevent boiling during operation with the HT system temperature greater than 100°C. The shutdown cooling system is designed and constructed to the same non-nuclear standards as the boiler feedwater system.</p> <p>It is noted that, although the combination of these systems provides a</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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"> post-LOCA heat removal may be provided by ECCS (refer to section 8.5) for non-LOCA events, emergency heat removal may be through primary or secondary cooling systems <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>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>	<p>reliable cooldown system, they are not completely independent of each other because they share the electrical supply systems needed for their operation. The Bruce A Loss of Shutdown Heat Sink analyses from high power and during shutdown modes have indicated that the frequency of the postulated event (sustained loss of all engineered heat sinks) is $<10E-4$ events /year. Thus, the failure rate of the function as performed by several systems is at least as low as that which would be provided by a safety grade EHRS designed to meet $10E-3$ failures per demand [RABA 0804].</p> <p>The MCS is environmentally qualified as are components of the EBC that support its functional capability. MCS and EBC, along with LPSW have been assessed as capable of surviving the RLE by the SMA process.</p> <p>The auxiliary boiler feedwater pumps and LPSW are powered by Class III, as are the Shutdown Cooling and Maintenance Cooling systems. The EBC is supplied with QPS. Both the MCS and SDC reject their heat to the LPSW system, which is independent of the normal feedwater system. The EBC system water source, should it be needed, is lake water from the fire pump suction headers in the water treatment building.</p> <p>In addition, as presented in [RABA 0804], the systems at Bruce A that currently perform the EHRS function meet the following requirements:</p> <ul style="list-style-type: none"> As systems important to safety the MCS, SDC and LPSW will have reliability targets per S-98 and OSRs that will define testing frequency. 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. The systems that perform the function do not rely on firewater system. <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 DECAs, if required. Therefore, this is assessed as a</p>	


 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<ul style="list-style-type: none"> a means of depressurizing the primary system is provided and the means of depressurization meets the requirements of a safety system, or the shutdown cooling system is capable of being operated at full primary pressure and temperature <p>Passive or non-passive (e.g., natural circulation or pumped) heat removal may be used. Non- 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>	gap (Gap).	
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"> sufficient capacity to support the safety functions of the connected loads in operational states, DBAs and DEC's availability and reliability is commensurate with the safety significance of the connected loads <p>The requirements of both the standby and emergency power</p>	<p>These are entirely new requirements. RD-337 has only Emergency Power Supply.</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 both Hydro One's 230 kV and 500 kV systems. According to Section 8.3.1.1, the design criteria for station service systems are as follows:</p> <ol style="list-style-type: none"> Not more than one unit should be lost due to a station service system fault. After the isolation of the Bruce A switchyard 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 unfaulted 230 kV or 500 kV buses. Adequate (dual bus or better) reliability must be provided for safety and production critical loads. Voltage regulation requirements must be met. The systems must be stable under postulated fault conditions. 	Gap


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>systems may be met by a single system.</p> <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"> 1. environmental and electromagnetic conditions to which electrical equipment and cables may be subjected 2. limits on electromagnetic emissions conducted or radiated from electrical equipment <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 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</p>	<p>6. The design must meet the requirements of all classes of power and lend itself to automatic and emergency transfer schemes.</p> <p>7. The unit concept is to be used, where all loads associated with main units are supplied from their respective unit supply buses and loads common to the plant are supplied from separate common supply buses.</p> <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 have an odd or even designation to match their source of supply. The station service system buses are classified by their level of reliability.</p> <p>An adequate supply of electrical power is required for the essential safety related system 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 A Electrical Systems [NK21-OSR-53000/55000-00001, R000]. These safety related systems must be capable of providing the basic nuclear safety functions, i.e., control, cool, contain and monitor. Bruce A 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 11.71 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 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</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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"> consideration of all modes of operation, plant states up to DEC's and all credible events that could impact the electrical power systems reliability and availability targets for systems and key equipment capacity and performance requirements 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 protective schemes and coordination of protection specification of acceptable ranges of voltage and frequency for continuous operation of the connected loads for each electrical power system identification of acceptable ranges for onsite and offsite transient disturbance events that could impact electrical power systems <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</p>	<p>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 Qualified Power System (QPS) 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 QPS is covered in Operational Safety Requirements for Bruce A Qualified Power Supply System [NK21-OSR-54400-00001, R000].</p> <p>The QPS system provides an alternate power supply to specific process and special safety system loads such as:</p> <ol style="list-style-type: none"> Emergency Boiler Cooling (EBC) valves Emergency Coolant Injection (ECI) valves Heat Transport (HT) main pump circuit breaker controls SDS2 Instrumentation Inactive drainage pumps (Unit 0 only) along with lighting loads in the MCR and equipment rooms (Unit 0 loads). <p>The QPS system provides the sole source of power to a number of common and unit safety related loads such as:</p> <ol style="list-style-type: none"> EBC pumps MCR emergency air conditioning QPS instrument rooms air conditioning <p>The QPS system is continuously energized and is monitored in the main control room.</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 QPS supply. Bruce NGS A Qualified Power Supply Design Manual [NK21-DM-54400-00002, Rev. 003] details the functional and performance requirements for the system. The design limits, seismic, environmental, reliability, maintainability, periodic inspection and safety requirements are described in this DM.</p> <p>The reliability of power supplies considers the following three ways in which Bruce NGS A could be separated from the Bulk Electrical System (BES):</p> <ul style="list-style-type: none"> A major system disturbance could result in loss of the 	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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"> unit generator performance during defined frequency and voltage excursions to ensure that generators remain connected to the electrical grid lightning and surge protection design provisions to protect the plant electrical distribution systems against transient over-voltage conditions such as switching and lightning surges <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"> prevent deviations from normal operation prevent single failures from impacting more than one redundant division of electrical power supply 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) <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</p>	<p>connection between the BES and the two stations with the 500 kV tie being maintained between the two stations. Restoration of BES supply to the complex would be accomplished by manual switching and in general would not involve repairs to system elements. The estimated frequency of this type of event is 0.037 per year to 0.145 per year.</p> <ul style="list-style-type: none"> A major system disturbance could result in loss of the connection between the two stations as well as the connection from both plants to the BES. Restoration of BES supply would be accomplished by manual switching and in general would not involve repairs to system elements. The estimated frequency of this type of event is 0.02 per year to 0.05 per year. A very severe storm could cause a prolonged outage of all circuits that terminate at Bruce NGS as a result of physical damage to all transmission circuits out of the station. The estimated frequency of this type of event is 0.0005 per year. <p>These factors were taken into account when the Bruce A emergency power system requirements were determined.</p> <p>Bruce Generating Station Units 1-4 Electrical Power Systems Design Manual [NK21-50000, Rev. 1] describes in detail the design basis for electrical power systems.</p> <p>As indicated in Section 8.6.11 the coatings on electrical cables could not be shown to meet the environmental conditions, primarily the radiation dose and temperatures associated with potential hydrogen burns, following some accidents. Therefore, as part of the Environmental Qualification program, some cables are being changed.</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 per [B-REP-00701-09DEC2013-060] 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&C needed for accident management actions following a loss of all AC</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>analysis should provide information concerning offsite power circuits coming from the transmission system to the plant switchyard. A switchyard common to 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>Additional information</p> <p>Additional information may be found in:</p> <ul style="list-style-type: none"> CSA Group, N290.5, Requirements for electrical power 	<p>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&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]. 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> <p>As per the Station Improvement Plan (Letter, F. Saunders to M. Leblanc, "Application for the Renewal of the Power Reactor Operating Licence for Bruce Nuclear Generating Station A", NK21-CORR-00531-10873), procurement of 400 kW generators was completed in 2012. Installation of electrical receptacles to provide power to U1/2/3/4 reactors, Unit 0 and EFADS has also been completed, including commissioning.</p>	




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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).</p> <ul style="list-style-type: none"> • IAEA, NS-G-1.8, Design of Emergency Power Systems of Nuclear Power Plants, Vienna, 2004. • IEEE, 1050, Guide for Instrumentation and Control Equipment Grounding in Generating Stations, Piscataway, New Jersey 1996. • IEEE, C62.23, IEEE Application Guide for Surge Protection of Electric Generating Plants, Piscataway, New Jersey, 1995. • IEEE, 141, IEEE Recommended Practice for Electric Power Distribution for Industrial Plants, Piscataway, New Jersey, 1993. • IEEE, 242, IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems, Piscataway, New Jersey, 2001. • IEEE, 308, IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations, Piscataway, New Jersey, 2001. • IEEE, 387, IEEE Standard Criteria for Diesel-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations, Piscataway, New Jersey, 1995. • IEEE, 279, IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations, Piscataway, New Jersey, 1971. • IEEE, 665, IEEE Standard for Generating Station Grounding, Piscataway, New Jersey, reaffirmed 2001. 		
8.9.1	The standby and emergency power systems shall have sufficient capacity and reliability, for a specified mission time, and in the	<p>New requirements are introduced.</p> <p>As described in Section 8.4 of Part 2 of the Safety Report, the station</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>presence of a single failure to provide the necessary power to:</p> <ol style="list-style-type: none"> maintain the plant in a safe shutdown state and ensure nuclear safety in DBAs and DEC's support severe accident management actions <p>Dedicated onsite fuel storage facilities shall have 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"> identify all events for which actuation of standby and emergency power sources are required 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 specify conditions for electrical protection to trip standby and emergency power sources to protect equipment from significant failure 	<p>has two sources of standby power on site – the station batteries and the standby 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. As described in Bruce A 250 VDC Class 1 Power Supply System (Units 1, 2 only) Design Manual [NK21-DM-55100, Rev. 002] 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. 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> <p>Four standby combustion turbine generator sets are available, each rated at 12 MW 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 automatically started, following the loss of Class IV power, to supply power to the critical Class III loads or when HPECI is initiated. Each generator is driven by a power gas turbine which derives its energy from the combustion of fuel oil. The fuel oil is stored in two above ground tanks, one tank per pair of combustion turbines. Fuel oil is fed from the tank, by gravity, to the two forwarding 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 used for "black" starting the standby generator when AC power is not available or as a backup to the AC</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>4. minimize challenges to standby and emergency power supplies as a result of an electrical system disturbance or transient 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> <ol style="list-style-type: none"> preferably be initiated automatically be capable of being periodically tested under load conditions representing full load demand and full mission time <p>Guidance</p> <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>pump if it fails in use. In addition as part of the reliability requirements as described in Bruce A Standby Generator Fuel Oil System Design Manual [NK21-DM-54660-001, Rev. 004] 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. Each storage tank normally supplies two standby generators, but can supply the other two as well.</p> <p>Class III standby power is automatically initiated, and QPS diesels start automatically on sustained under-voltage, but the loads to QPS are switched manually. Bruce A completes one SG run every week (SST 05.01, 05.02, 05.03 & 05.04) for 2 hours at full load. Also two other SGs are black started during the Emergency Transfer Tests but they are not run. A full black start and block loading of the standby generator is performed once a year during the annual shutdown.</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 or partial loss of Class IV power to a unit is performed to demonstrate the capability of the design to accommodate such failures. Appendix 2 Electrical System Failures summarises the results of analysis.</p> <p>The Operational Safety Requirements for Bruce A Qualified Power Supply System are documented in [NK21-OSR-54400-00001, R000].</p> <p>Currently the standby generators at Bruce A are meeting their reliability targets. As part of the upgrade of emergency and standby power supplies, there is initiative to ensure that the reliability targets continue to be met in the future as the control systems age and obsolescence issues become more prevalent. As specified in supporting documentation for NK21-CORR-00531-11567 this action</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	The stored energy supply for starting standby or emergency power sources should have sufficient stored energy for five consecutive start attempts.	is monitored under AI 1207-3283.	
8.9.2	<p>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> <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>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 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 uninterruptible. 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 A Electrical Systems [NK21-OSR-53000/55000-00001, R000] present the safety limits, applicable analysis and surveillance requirements for Bruce A 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>	Gap




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Battery chargers should be designed to prevent transients on the AC supply from affecting the 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"> • an AC power supply and a DC power supply to an inverter • a separate AC power supply from the same division • a feature to automatically switch between the inverter output and the separate AC supply <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> <p>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.</p>		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
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"> 1. be connectable to but not normally connected to the offsite or onsite standby and emergency AC power systems 2. have minimum potential for common mode failure with offsite power or the onsite standby and emergency AC power sources 3. be available in a timely manner after the onset of a station blackout 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>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>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 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. 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 or partial loss of Class IV power to a unit 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 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. The SAMG will address multiunit events involving a station blackout.</p>	Gap

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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>		
8.10	Control Facilities	This is not a requirement/guidance clause (this is a title only).	NA
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 DECAs.</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 change is for clarification only.</p> <p>As described in Section 3 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. There are five main panel sections, one for each of the four generating units and one for the switchyard and common systems. An operator's desk and two high-speed line printers are associated with each unit panel, and a terminal for the safety system-monitoring computer is provided for each unit. A single operator's desk and a line printer are used with the switchyard and common systems panels. The fuelling machine and fuel handling control consoles are located in the centre of the main control room.</p> <p>The control room is being protected from the effects of the steam environment following a steam or feedwater line break. It is adequately protected from the effects of radiation following all accidents due to the addition of shielding around the ECI recirculation</p>	IC

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The design of the MCR shall be such that appropriate lighting levels and thermal environment are maintained, and noise levels 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&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 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>lines. Fire protection of the main control room is also enhanced. The effect of external events on the control room has been considered. As a result of the Seismic Margin Assessment [NK21-REP-03611-00005, Rev. 000] the recommended upgrades for the control room ceiling consisted of installing restraining ties to attach each diffuser panel to the main support runners, and installing retaining tabs on each of the glass panels. These upgrades were implemented as a result of Units 3 & 4 SMA. The upgrades prevent the ceiling tiles and glass panels from falling. The masonry walls of the control room were judged adequate and did not need upgrading. Thus, the MCR is now considered seismically qualified to the extent necessary to ensure the success path.</p> <p>All safety functions that are initiated automatically in the MCR can also be manually initiated within the MCR.</p> <p>The design requirements for cabling of the instrumentation documented in [NK21-DR-63760-001] state that the safety system circuits required at the SCA and associated field panels shall be isolated from circuits leading to the MCR complex because a fire in the cable spreading area, could produce ground faults or hot shorts on any circuit passing through that area. Under normal circumstances, a single ground fault can be tolerated, but in a cable fire (with the potential for multiple ground faults), the conservative design shall be to isolate the cables to the MCR area.</p> <p>A review of the requirement in RD-337 for secure communication channels to the emergency support facilities indicated that the Bruce A design does not meet this requirement, as documented in [NK21-CORR-00531-11005]. The primary method of communication is by telephone and radio, but the systems are not secure, for example it is not seismically qualified.</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 main control room alarm annunciation system consists of a window annunciating system, two computer-driven CRTs for alarm message presentation and a facility to provide a printed record of all alarm conditions with sufficient information to enable them to be arranged in the chronological order of their occurrence. As well, an option has been</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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 DECs, release of radioactive material, fire, or explosive or toxic gases.</p> <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</p>	<p>installed to store alarm messages on the moving arm disc only instead of being printed. The messages may be printed out when required. Alarm summaries may be requested for the total unit or on a system basis. A sequence of events record is produced following all unit disturbances. Annunciator windows are illuminated independently of the computers for all alarm conditions that will cause reactor trips, power run-backs, turbine generator trips, high voltage breaker trips and other important system alarms that have to be monitored on dual computer failure. These windows are provided on the top section of some of the process system main control room panels. Unit alarms are displayed on two cathode ray tube displays located in the center of the unit control panels, and are printed out on printers adjacent to the operator's desk. Switchyard and common equipment alarms are displayed on a cathode ray tube display mounted on the common equipment and switchyard control panel and printed out on a printer that is located adjacent to the common systems operator's desk. This printer is also used to print out sequence of events alarms. Magnetic disk storage is provided for annunciation data so that only data selected on demand need be printed.</p> <p>There is an audible alarm that operates whenever a new alarm condition is displayed on the CRT or the annunciator windows. Local field annunciator units are used on control panels that are located in areas of the station remote from the main control room. Each of the emergency support centres has 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 used for direct contact with the Bruce Power emergency support centres. Availability of these forms of emergency communication are verified according to "Emergency Facility and Equipment Maintenance" procedure [SEC-EPP-00004] and by operational checks at the start of an emergency.</p> <p>Bruce Power is performing assessments, in conjunction with COG, of instrument survivability and habitability of control facilities under</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	to fulfill the required safety function in each facility. Criteria for control room habitability should be established.	severe accident conditions and identification of modifications required is underway. Control facilities include areas in the field where SAMG operator actions are required.	
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> <ol style="list-style-type: none"> 1. display safety-critical parameters within the full range expected in operational states, DBAs and DEC's 2. track data trends 3. indicate when process or safety limits are being approached or exceeded 4. display the status of safety systems <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 changes are editorial – “DEC's” replaced “BDBAs, including severe accidents” and “emergency response facility” replaced “emergency support centre”.</p> <p>As documented in [NK21-CORR-00531-11005], a review of the same clause in RD-337 indicated that Bruce A 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. 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 are verified according to “Emergency Facility and Equipment Maintenance” procedure [SEC-EPP- 00004] and by operational checks at the start of an emergency.</p> <p>Section 6.6 of Part 2 of the Safety Report describes the 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 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.</p> <p>Bruce A meets the intent of the requirement in the sense that the SSMC, the Bruce A 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 [RABA 0804].</p>	IC



Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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 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"> • reactivity control • reactor core and irradiated fuel cooling • heat removal from primary system • reactor coolant system integrity • radioactivity control • containment integrity <p>The SPDS should:</p> <ul style="list-style-type: none"> • have sufficient availability and reliability • not display unreliable or invalid data and alarms • be designed to meet the specified human factor usability requirements 		




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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 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>Very minor editorial changes are made to this section. The repetition is eliminated, e.g., some requirements are already in 8.10.1. No changes in the intent of the existing requirements.</p> <p>As described in Bruce A Secondary Control Area Design Manual Unit 034 [NK21-DM-63760-001, Rev. 00] the design requirements document [NK21-DR-63760-001, Rev. 00] defines the design parameters for a Secondary Control Area (SCA) function at Bruce A. The SCA and associated field panels provide alternate control locations following a Loss of Control from the Main Control Room (MCR) Complex. A Loss of Control from the MCR Complex will exist when either one or both of the following events occur: (1) the MCR Complex environment becomes uninhabitable and all operating personnel must abandon the area and (2) control and/or monitoring of safety and safety-related systems and Critical Safety Parameters (CSP) become unreliable. This is defined as the point where control and monitoring of these systems is sufficiently impaired to prevent them from performing their design function. For Bruce A, two SCAs are provided, as a retrofit. One SCA covers Units 1&2 and is located in the Construction Retube Building (CRB). The second SCA covers Units 0, 3 and 4, and is located in Unit 3. The Bruce A SCAs are physically separated and isolated from the MCR.</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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 that are as user-friendly as possible.</p> <p>Cabling for the I&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>The Bruce A SCA is a retrofit and as such is only designed to accommodate those events where there is a fire in the MCR or radiation fields that are too high to allow use of the MCR. Seismic events, Main Steam Line Breaks (MSLBs), major waterline breaks or Loss of Coolant Accidents (LOCAs) do not cause a Loss of Control from the MCR Complex and shall be executed from the MCR Complex. As described in Section 6.7.5 of Part 2 of the Safety Report, the secondary control area is seismically and environmentally qualified to provide control and indications that enable the operators to ensure the reactor units are shut down and monitored; the reactor units are cooled down and monitored and common containment is maintained and monitored. Seismically qualified egress routes are provided from the MCR to the SCAs.</p> <p>The Safety System Monitoring Computer and DCCs (the Bruce A version of the SPDS) do not connect to the SCA so this requirement is not met. However, sufficient instrumentation and controls are provided to ensure that the Critical Safety Parameters [NK21-OSR-60060-00001, R000] can be monitored and controlled from the SCA and its associated field panels. 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>The nominal mission time for the SCA and associated field panels shall be 72 hours. The actual mission time will depend on the severity of the Loss of Control from the MCR Complex event. The SCA area is not be equipped with washroom facilities and drinking fountains. The environment external to the SCA will be such that existing facilities will be available during a Loss of Control from the MCR Complex event [RABA 0804].</p> <p>Bruce Power is building a state-of-the-art Emergency Management Centre and unifying the existing Site Management and Corporate Emergency Support Centres into a single, modern command centre.</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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, 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>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 / 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.</p>	
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</p>	<p>New text is added to this clause mostly to clarify the requirements. Second and third paragraph are new requirements.</p> <p>As described in Bruce Power Nuclear Emergency Response Plan [BP-PLAN-00001, R004], there are a series of centres from which different activities are controlled.</p> <ul style="list-style-type: none"> - Main Control Room (MCR) <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"> - Work Control Area (WCA) <p>WCA is an on-site area adjacent to the MCR. When alerted by the station PA system on-shift Operations department staff assembles at the WCA and await further instructions and 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"> - Emergency Operations Centre (EOC) <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</p>	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>maintained, and that noise levels are minimized in accordance with applicable standards and codes.</p> <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"> 1. includes provisions to protect occupants over protracted periods from the hazards resulting from DBAs and DEC's 2. is equipped with adequate facilities to allow extended operating periods <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>Guidance</p> <p>The design provides emergency support facilities which include a technical support center and an onsite emergency response facility</p>	<p>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.</p> <ul style="list-style-type: none"> - Site Management Centre (SMC) <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 CESC.</p> <ul style="list-style-type: none"> - Corporate Emergency Support Centre (CESC) <p>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. CESC supports the SMC with the appropriate technical and financial resources. CESC staff is on call and is activated for events categorized as Abnormal Incident or higher. For events of lesser category the Bruce Power Communications Department will disseminate information as judged appropriate for the event. The backup location for the CESC is the SMC.</p> <p>As described in Section 11.5.2 of Part 2 of the Safety Report, each of the emergency support centres has 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 used for direct contact with the Bruce Power emergency support centres. Availability of emergency communications are verified according to "Emergency Facility and Equipment Maintenance" procedure [SEC-EPP-00004] and by operational checks at the start of an emergency.</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The TSC will provide the following functions:</p> <ul style="list-style-type: none"> provide technical support and plant management to plant operation personnel during emergency conditions handle peripheral duties and communication not directly related to reactor manipulations in order to relieve the burden of reactor operators during emergency conditions prevent congestion in the control rooms perform emergency support functions until the emergency response facility is functional <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 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</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. 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 [RABA 0804].</p> <p>Detailed discussion about emergency planning and arrangements is presented in Safety Factor 13.</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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>		
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"> 1. there are clear, well-defined, validated, and readily available operating procedures that identify the necessary actions 2. there is instrumentation in the control rooms to provide clear 	<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 but 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.</p>	Gap


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>and unambiguous indication of the necessity for operator action</p> <p>3. following indication of the necessity for 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 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</p>	<p>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> <p>A review of the same clause in a draft version of RD-337 indicated that the Bruce A design meets the intent of this requirement, as documented in [RABA 0804]. The Abnormal Incidents Manual [NK21-OM-09034] provides well-defined and validated procedures for handling accident situations.</p> <p>The instrumentation shown in Tables 1-24 through 1-33 of Part 3 of the Safety Report, as indicators of the need for operator actions, covers the entire range from safety system instrumentation to process instrumentation. In some cases, there is only one indicator but in general, there are usually several indicators. The complete list of operator actions called for in the safety analyses is given in Tables 1-24 through 1-33 of Section 1 Part 3 of the Safety Report. This table also shows what the indication of the need is. In general, the majority of the indications come from equipment in the control room. Some come from field locations depending upon the accident scenario.</p> <p>As described in Section 1.3 of Part 3 of the Safety Report, Table 1-1 to Table 1-10 provide a summary of the operator actions credited for the various accident categories. 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 [NK21-SR-01320-00003, Rev. 004].</p> <p>All necessary actions of the safety systems that are initiated automatically can also be manually activated from the MCR. The SCA is a late addition at Bruce A designed to cope with situations where the MCR becomes uninhabitable and, as such, was not designed to duplicate in full all the capabilities of the MCR. Additional details are provided in Section 8.10.</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</p>	


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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"> • there is sufficient time available for the operator to perform the required manual action • the operator can perform the actions correctly and reliably in the time available <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 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 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</p>	<p>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>	


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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"> • ANSI/ANS, 58.8, Time Response Design Criteria for Safety Related Operator Actions, La Grange Park, Illinois, 2008. • CSA Group, N290.4, Requirements for Reactor Control Systems of Nuclear Power Plants, Toronto, Canada. • CNSC, G-225, Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills, Ottawa, Canada, 2001, or successor document. • IEC, 60964, Nuclear Power Plants - Control Rooms – Design, Geneva, 2009. • IEC, 60965, Nuclear Power Plants - Control Rooms - Supplementary Control Points for Reactor Shutdown Without Access to the Main Control Room, Geneva, 2009. • NEI 99-03, Control Room Habitability Assessment Guidance, Washington, D.C., 2001. • U.S. NRC, NUREG-0696, Functional Criteria for Emergency Response Facilities, Washington, D.C., 1981. • U.S. NRC, Regulatory Guide 1.196, Control Room Habitability at Light-Water Nuclear Power Reactors, Washington, D.C., 2003. 		
8.11	The design shall include provisions to treat liquid and gaseous	A new requirement for the design to minimize the regeneration of	IC

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>effluents in a manner that will keep the quantities and concentrations of discharged contaminants within prescribed limits, and that will 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"> • CNSC, P-290, Managing Radioactive Waste, Ottawa, Canada, 2004. 	<p>radioactive and hazardous waste is introduced.</p> <p>As described in Section 13 of Part 2 of the Safety Report, the 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"> 1. Holding of radioactive isotopes, for natural decay. 2. Dilution and emission of liquid and gaseous active wastes in the respective plant effluent streams in a controlled and monitored process. 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. 4. Containment and temporary storage of solids in facilities within the plant buildings. 5. Transport of solid wastes is contracted to licenced disposal facilities. <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. Dry 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 WWMD 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</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
		<p>Report.</p> <p>Bruce Power's Environmental Safety Management program [BP-PROG-00.02, R008] 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] provides the requirements for compliance with applicable Federal, provincial, and municipal regulations.</p> <p>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.</p> <p>The intent of the evaluation is to ensure materials used have the smallest environmental footprint possible.</p> <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 WWMD operated by OPG is located on the Bruce site [NK21-CORR-00531-11005].</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 system of sufficient capacity to collect, hold, mix, pump, test, treat, and sample liquid waste before discharge, taking expected waste and accidental</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.</p> <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.</p>	IC

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	spills or discharges into account.	<p>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>A review of the same clause in a draft version of RD-337 indicated that the liquid waste management system at Bruce A meets this requirement, as documented in [RABA 0804]. 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>Bruce A has installed an enhanced active liquid waste treatment system consisting of a reverse osmosis subsystem and an evaporation-solid fixation system to enable treating high-level liquid waste.</p> <p>There is a closed recirculation system for purifying the water from each fuel storage bay. 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].</p>	
8.11.2	The design shall include gaseous waste management systems	There are no changes in the requirement.	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>capable of:</p> <ol style="list-style-type: none"> controlling all gaseous contaminants so as to conform to the ALARA principle and ensure that concentrations remain within prescribed limits collecting all potentially active gases, vapours, and airborne particulates for monitoring passing all potentially active gases, vapours, and airborne particulates through pre-filters, absolute filters, charcoal filters, or high efficiency particulate air filters where applicable delaying releases of potential sources of noble gases by way of an off-gas system of sufficient capacity <p>The design shall provide a ventilation system with an appropriate filtration system capable of:</p> <ol style="list-style-type: none"> preventing unacceptable dispersion of all airborne contaminants within the plant reducing the concentration of airborne radioactive substances to levels compatible with the need for access to each particular area keeping the level of airborne radioactive substances in the plant below prescribed limits, applying the ALARA principle in 	<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 or to the pressure relief manifold.</p> <p>As discussed in Section 13.4.2 of Part 2 of the Safety Report, the station has an off-gas system designed to provide continuous on-line treatment of the noble gas contaminated 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 [RABA 0804].</p> <p>The Bruce A 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 powerhouse is divided into three zones according to the potential contamination hazards in each area.</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>normal operation</p> <p>4. ventilating rooms containing inert or noxious gases without impairing the capability to control radioactive releases</p> <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 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>	<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 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. The station, exclusive of the containment envelope, is provided with four identical unit ventilation systems, each serving one unit.</p> <p>See Section 12.3.3 Zoning, Part 2, Section 12 Radiation Protection of the Safety Report presents more details of zoning arrangement for Bruce A design.</p>	
8.11.3	<p>The ventilation system shall include filtration that will:</p> <p>1. control the release of gaseous contaminants and hazardous substances to the environment</p> <p>2. ensure conformation to the ALARA principle</p> <p>3. maintain airborne contaminants within prescribed limits</p> <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>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 A 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 28.3 m³/s (60000 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.</p>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<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 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"> • CNSC, G-129, Keeping Radiation Exposures and Doses "As Low as Reasonably Achievable (ALARA)", Ottawa, Canada, 2004. • CSA Group, N292.3, Management of Low-and Intermediate-level Radioactive Waste, Toronto, Canada. • IAEA, Safety Standards Series GS-G-3.3, The Management System for the Processing, Handling and Storage of Radioactive Waste Safety Guide, Vienna, 2008. 	<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. A similar system is used for the secondary spent fuel bay in the Ancillary Services Building. Other areas in the common unit have exhaust fans with filters containing only pre-filters and absolute filters, considering 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</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>As described in the Application to Renew the Power Reactor</p>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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</p> <p>(greases, tramp uranium etc.) and prevent the spread of contamination into the reactor.</p>	<p>Operating Licence for Bruce Nuclear Generating Station A (PROL 15.00/2014) the Fuel Management program defines the fundamental business needs, constituent elements, functional requirements, implementing approaches and key responsibilities associated with all aspect of the fuel management process. The objectives of the fuel management program are:</p> <ul style="list-style-type: none"> • Optimum reactor core operating within operating and regulatory limits; • Operation of the reactor with fuel of an approved design, manufactured to strict quality assurance requirements; • Prevention of fuel damage throughout the fuel life cycle and timely removal of failed fuel from the core; • As low as reasonably achievable radiation exposure associated with fuel and Cobalt 60 activities; • Fulfilling Bruce Power's obligations under Canada's Safeguards Agreement; • Adequate support for fuel and fuel channel inspection; • Implementation of processes and procedures for all program activities required for the safe and reliable use of nuclear fuel. <p>This program is supported by BP-PROG-12.03 R003, Fuel Management BP-PROC-00455 R001, Fuel Procurement BP-PROC-00460 R002, Fuel Handling BP-PROC-00452 R000, Core Management procedures.</p> <p>Criticality Control Program is a Licence Condition 13.5 of the Bruce Power A Operating Licence. As required in Licence Condition Handbook (LCH-BNGSA-R8) Bruce Power is to maintain their nuclear criticality safety program in accordance with BP-PROC-00324 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 K_{eff} does not exceed the upper sub-critical limits established by the program.</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

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"> • ANSI/ANS, 57.1, American National Standard Design Requirements for Light Water Reactor Fuel Handling Systems (as applicable), La Grange Park, Illinois, 1992. • IAEA, NS-G-2.5, Core Management and Fuel Handling for Nuclear Power Plants, Vienna, 2002. • IAEA, NS-G-1.4, Design of Fuel Handling and Storage Systems for Nuclear Power Plants, Vienna, 2003. 	<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.</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"> 1. ensure nuclear criticality safety 2. permit appropriate maintenance, periodic inspection, and testing of components important to safety 3. permit inspection of non-irradiated fuel 4. prevent loss of or damage to the fuel 5. meet Canada's safeguards requirements for recording and reporting accountancy data, and for monitoring flows and 	<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>A review of the same clause in a draft version of RD-337 indicated that the Bruce A design meets this requirement, as documented in [RABA 0804]. Section 10.2.3 of Part 2 of the Safety Report provides design details about the new fuel storage and handling.</p> <p>New fuel bundles are received at a new fuel receiving area (located in Unit 3 on elevation 619) or at new fuel storage racks (located at Unit 3 reactor auxiliary bay). The new fuel bundles are enclosed in protective crates containing 42 bundles. The new fuel storage area maintains a capacity of 3444 fuel bundles. Facilities are provided to store the fuel in its protective crates and to move it to the new fuel loading facilities and inspection stations using a 1.8 Mg (2 ton) hoist and monorails 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 so that the fuel can be cleaned, visually inspected for damage</p>	C


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	inventories related to non-irradiated fuel containing fissile material	<p>and gauged for fuel spacer interlocking.</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 not possible to create a flooded situation.</p> <p>The protective covering of the bundles is removed by hand and the bundles are raised from the crates by hand and transferred to a handcart. They are then moved to an inspection area where the bundles are lifted by a lifting attachment connected to an air-balanced hoist. This lifting attachment allows the fuel to be rotated so that the fuel can be cleaned, if necessary, visually inspected for damage and gauged for fuel spacer interlocking.</p> <p>After inspection the serial numbers of the approved new fuel bundles are recorded and the new fuel bundles are transferred using the hoist and lifting attachment to the selected new fuel port transfer mechanism and 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 if required. A maximum of 16 bundles can be loaded into the transfer mechanism magazine. The fields in the new fuel loading area are less than $1.0 \times 10E-5$ Gy/h (1.0 mR/h), thus allowing unrestricted access under normal conditions. The damage mechanisms and the associated conditions are described in Part 2, Section 10.2.4.7.2 of the Safety Report.</p>	
8.12.2	<p>The design of the handling and storage systems for irradiated fuel shall:</p> <p>1. ensure nuclear criticality safety</p>	<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>A review of the same clause in a draft version of RD-337 indicated that the Bruce A design meets the intent of this requirement, as documented in [RABA 0804]. Section 10.2.3 of Part 2 of the Safety Report provides design details about the new fuel storage and</p>	Gap

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2. permit adequate heat removal in operational states, DBAs and DECs</p> <p>3. permit inspection of irradiated fuel</p> <p>4. permit periodic inspection and testing of components important to safety</p> <p>5. prevent the dropping of irradiated fuel in transit</p> <p>6. prevent unacceptable handling stresses on fuel elements or fuel assemblies</p> <p>7. prevent the inadvertent dropping of heavy objects and equipment on fuel assemblies</p> <p>8. permit inspection and safe storage of suspect or damaged fuel elements or fuel assemblies</p> <p>9. provide proper means for radiation protection</p> <p>10. permit adequate identification of individual fuel modules</p> <p>11. facilitate maintenance and decommissioning of the fuel storage and handling facilities</p>	<p>handling.</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 10-11 of Section 10 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 mechanism also permits the transfer of single bundles and transfer of bundles in a fuel carrier under abnormal conditions 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. 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,</p>	

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>12. facilitate decontamination of fuel handling and storage areas and equipment when necessary</p> <p>13. ensure implementation of adequate operating and accounting procedures to prevent loss of fuel</p> <p>14. include measures to prevent a direct threat or sabotage to irradiated fuel</p> <p>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</p> <p>A design for a water pool used for fuel storage shall include provisions for:</p> <ol style="list-style-type: none"> controlling the chemistry and activity of any water in which irradiated fuel is handled or stored monitoring and controlling the water level in the fuel storage pool detecting leakage preventing the pool from emptying in the event of a pipe break sufficient space to accommodate the entire reactor core 	<p>discharge mechanisms, etc.) requires considerable routine maintenance. This was expected at the time of Bruce A design and facilities are available to cope with it within the Central Service Area (CSA) or East Service Area of the plant. Decontamination facilities are available within the CSA to cope with the fuel handling and storage system 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. The Bruce A 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 1.11 m) results in relatively benign dose rates. Moreover, the impact of uncertainties in the following factors on the gamma fields calculated in have been assessed to be relatively small:</p> <ul style="list-style-type: none"> • depth of water cover above the uppermost fuel trays; • age (i.e., decay time) of the irradiated fuel; • irradiation history of the irradiated fuel; and • modelling approximations in the shielding calculation. <p>Loss of primary fuel bay water is considered in the accident analysis. 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</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>inventory at all times</p> <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 shall include provisions for DEC's by:</p> <ol style="list-style-type: none"> 1. ensuring that boiling in the pool does not result in structural damage 2. providing temporary connections to enable the refill of the pool using temporary supplies 3. providing temporary connections to heat removal systems for power and cooling water 4. providing hydrogen mitigation in the spent fuel pool area 5. ensuring that severe accident management actions related to the spent fuel pool can be carried out <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</p>	<p>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. 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 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 [B-REP-00701-09DEC2013-060]. 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.</p>	




Rev Date: July 8, 2016

Status: Issued


Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	product scrubbing as part of containment venting. Hydrogen mitigation in the spent fuel pool area may not be necessary if draining of the pool beyond make- up capability can be precluded.		
8.12.3	<p>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> <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>There are no changes to this requirement.</p> <p>The Delayed Neutron (DN) monitor 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 defective fuel bundle are inspected in the inspection section 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 on the HTS coolant and radioactive tritium concentration in the HTS coolant. The safety limits for HTS coolant activity are provided in Section 6.0 HTS Coolant Activity of Bruce NGS A Heat Transport System OSR [NK21-OSR-33100-00001, R00].</p>	IC
8.13	<p>The design and layout of the plant shall make suitable provision to minimize exposure and contamination from all sources. This shall include the adequate design of SSCs to:</p> <ol style="list-style-type: none"> control access to the plant minimize exposure during maintenance and inspection 	<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 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</p>	Gap

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>3. provide shielding from direct and scattered radiation</p> <p>4. provide ventilation and filtering to control airborne radioactive materials</p> <p>5. limit the activation of corrosion products by proper specification of materials</p> <p>6. minimize the spread of active material</p> <p>7. monitor radiation levels</p> <p>8. provide suitable decontamination facilities</p> <p>Guidance</p> <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,</p>	<p>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 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. Figure 12-1 to Figure 12-6 show the general zoning arrangement for Bruce A. 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</p>	

 <div> <div>candesco</div> <div>Division of Kinectrics Inc.</div> </div>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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 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"> • CNSC, G-129, Keeping Radiation Exposures and Doses "As Low as Reasonably Achievable (ALARA)", Ottawa, Canada, 2004. • IAEA, Safety Guide RS-G-1.1, Occupational Radiation Protection, Vienna, 1999. • IAEA, Safety Standards Series NS-G-1.13, Radiation 	<p>are provided in Table 12-1.</p> <p>Zoning [BP-RPP-00015, R011] 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 A.</p> <p>There are numerous decontamination centres within the 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. [RABA 0804]</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>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	Protection Aspects of Design for Nuclear Power Plants, Vienna, 2005.		
8.13.1	<p>The shielding design shall prevent radiation levels in operating areas from exceeding the prescribed 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 DEC's for those parts of the facility to which access is required.</p> <p>Guidance</p> <p>Shielding should be designed based on the zone 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</p>	<p>The changes are editorial and do not affect the requirements, e.g., "DBAs and DEC's" replaced "accident conditions".</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 A. Procedures for controlling temporary shielding at the station that is 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 inspections are provided in Section 5.1.2.7 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 A Safety Report, lists the materials used for the major components in the HT system. The major materials exposed to the reactor coolant are zirconium alloys, 400 series steels, carbon steel, Inconel and Incoloy. Part 2, Section 5.1.3 of the Safety Report contains details on the zirconium alloy and</p>	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	materials over the lifetime of the NPP.	<p>400 series steels. Carbon steel is used for the 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. [RABA 0804]</p> <p>The operator actions credited in the Safety Report during accidents, as listed in 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 [RABA 0804].</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> <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 and qualitative probability of contamination there are in the area. 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.</p>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
		<p>The predicted dose rates used to be average dose rates for each zone given in BP-RPP-00002; 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>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</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 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.</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 A 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>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	from the potentially contaminated area.	Radioactive wastes are handled via the solid and liquid waste management systems. Does rates outside containment are minimized due to shielding provided in the design.	
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"> for monitoring the local radiation dose rate at places routinely occupied by operating personnel where the changes in radiation levels may be such that access may be limited for periods of time to indicate, automatically and in real-time, the general radiation level at appropriate locations in operational states, DBAs and DEC's 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 <p>Monitors shall be provided for measuring the activity of radioactive substances in the atmosphere:</p> <ol style="list-style-type: none"> for areas routinely occupied by personnel 	<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 of hazardous changes in radiation levels under all operating and non-operating conditions. They also provide information of gamma dose rates. 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. These stations are equipped with foot monitors and friskers as a minimum. At some locations, hand monitors, whole body monitors and portal monitors also are available. (Section 12.3.4.1 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 diffusion samplers are used 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. 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. [RABA 0804]</p> <p>As described in Section 6.2.2.12 of Part 2 of the Safety Report, the Post-Accident Radiation Monitoring System (PARMS) provides on-</p>	Gap

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2. for areas where the levels of activity of airborne radioactive materials may, on occasion, be expected to necessitate protective measures</p> <p>3. to give an indication in the control room, or in other appropriate locations, of when a high concentration of radionuclides is detected</p> <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>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. Several upgrades to the system are underway to meet the performance requirement in terms of providing data for all single or dual failures accidents. Further details are provided in Safety Factor 15.</p> <p>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 body. [RABA 0804]</p>	
8.13.4	<p>The design shall provide for:</p> <p>1. appropriate disposal of radioactive materials, either to onsite storage or through removal from the site</p> <p>2. reduction in the quantity and concentration of radioactive materials produced</p>	<p>There are no changes in the requirements in this clause.</p> <p>A review of the same clause in a draft version of RD-337 indicated that an extensive Environmental Assessment for the Refurbishment for Life Extension and Continued Operations of the Bruce A Reactors was submitted in 2005 in support of the refurbishment of Units 1/2 and accepted by the CNSC. The review assessed the impact of the Bruce A units on the environment and contains further information on some of these topics.</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</p>	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	3. control of dispersal within the plant 4. control of releases to the environment 5. decontamination facilities for equipment, and for handling any radioactive waste arising from decontamination activities 6. minimization of radioactive waste generation	<p>transferred daily to OPG's WWMD 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 WWMD service department waste operation, where the waste goes through volume reduction; incineration or it is stored in OPG's WWMD 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 auxiliary bay floor of Unit 2. These tanks provide temporary storage before transfer to OPG's WWMD 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 WWMD waste operations site.</p> <p>Bruce Power is committed to minimizing radioactive wastes per BP-PROC-00878, Radioactive Waste Management, which is governed by BP-PROG-12.05, 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> 1. pathways to the human population, including the food-chain 2. the radiological impact, if any, on local ecosystems 3. the possible accumulation of radioactive materials in the	<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>A review of the same clause in a draft version of RD-337 indicated that the Bruce A design meets this requirement, as documented in [RABA 0804]. 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 AECS and later upgraded in 1999 [RABA 0804]. The purpose of the program is:</p>	IC


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>environment</p> <p>4. the possibility of any unauthorized discharge routes</p> <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>	<ol style="list-style-type: none"> To confirm that emissions of radioactive materials are properly controlled. To verify that the assumptions made in calculating facility Derived Release Limits (DRLs) remain valid. To permit an independent estimate to be made of doses to the public resulting from emissions. To provide data to aid in the development and evaluation of models which adequately describe the movement of radionuclides through the environment. <p>The Bruce Power Health Physics Laboratory performs the sampling and analysis in support of the program.</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. The monitoring sites are shown in Figure 12-7. 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, R005] 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.</p> <p>The EM7 - Radiological Environment Monitoring Program Routines [DPT-ENV-00007, R003] describes the process and methods for collecting and analysing environmental samples, calculating dose to the public, and preparing reports.</p> <p>A high level assessment of CSA N288.4 is performed and documented in Safety Factor 14.</p>	
9.	Safety Analysis	This is not a requirement/guidance clause (this is a title only).	NA
9.1	A safety analysis of the plant design shall include hazard analysis, deterministic safety analysis, and probabilistic safety assessment	<p>New requirements have been introduced.</p> <p>The radioactive sources other than the reactor core are not</p>	Gap


 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>(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>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).</p> <p>Additional details related to the requirements and guidance for identification of PIEs are provided in Safety Factor Report 5.</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 as documented in Safety Factor 6.</p>	
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>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"> 1. reflect the as-built plant 2. account for postulated aging effects on SSCs important to safety 3. demonstrate that the design can withstand and effectively 	<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, 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</p>	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>respond to identified PIEs</p> <p>4. demonstrate the effectiveness of the safety systems and safety support systems</p> <p>5. derive the OLCs for the plant, including:</p> <p>a. operational limits and set points important to safety</p> <p>b. allowable operating configurations, and 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>analysis assumptions and inputs of Part 3 of the Safety Report. Analysis of the main events impacted by ageing are 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. In addition, safety analysis 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>	

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<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 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.</p>		
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"> 1. applicable acceptance criteria (i.e., the success path criteria) 2. the hazardous materials in the plant and at the plant site 3. all qualified mitigating SSCs credited during and following the event all non-qualified safety or safety support systems are assumed to fail, except in cases where their continued operation would result in more severe consequences 4. operator actions and operating procedures for the event 	<p>There are no changes to this section.</p> <p>The Bruce A design documentation does include Hazard Analysis. The detailed hazard analysis of protection against fire is generated as per DPT-PDE-00027, DPT-PDE-00028 and DPT-PDE-00029, and is documented in NK21-REP-71400-00003, NK21-REP-71400-00004 and NK21-REP-71400-00005. Seismic margin in the event of earthquake is generated as per DPT-PDE-00017, and is assessed in NK21-REP-20091-00001. Other internal and external hazards are assessed in RABA-0601 (Enclosure 5 to NK21-CORR-00531-04059).</p> <p>As summarized in [B-REP-00701-09DEC2013-060] review of the basis for external events against modern state-of-the-art practices for evaluating external events magnitudes and relevant design capacity for these events was recommended in order to strengthen reactor defence-in-depth. The Bruce Power Probabilistic Risk Assessment (PRA) external hazards analysis involved a screening analysis that was completed in September 2012. As a result of the screening, seven hazards were determined to require further assessment</p> <ul style="list-style-type: none"> • High/Low Ambient Air Temperature • Lightning • Toxic/Chemical/Radiological Release • Turbine Generated Missiles • Transportation Accidents • External Flooding • Tornadoes/High Winds 	Gap

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>5. plant or operating procedure parameters for which the event is limiting</p> <p>The hazard analysis shall confirm that:</p> <ol style="list-style-type: none"> 1. the plant design incorporates sufficient diversity and separation to cope with credible common-cause events 2. credited SSCs are qualified to survive and function during and following credible common- cause events, as applicable 3. the following criteria are met: <ol style="list-style-type: none"> a. the plant can be brought to a safe shutdown state b. the integrity of the fuel in the reactor core can be maintained c. the integrity of the reactor coolant pressure boundary and containment can be maintained d. safety-critical parameters can be monitored by the operator <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"> 1. include a general description of the physical characteristics of the plant that outlines the prevention and protection systems to be provided 	<p>Analysis to assess the impacts of these unscreened events is underway. Bruce Power is implementing a Safety Report Improvement Program starting in 2014 including annual status and progress updates to the CNSC staff. The activities related to upgrade of the Safety Report, the schedule and program organization and interfaces are presented in Planning Basis for Safety Report Improvement at Bruce A and B [NK21-CORR-00531-10774/NK29-CORR-00531-11155]. The implementation of these activities is tracked under Action Item 090739 [NK21-CORR-00531-07548/NK29-CORR-00531-08524].</p> <p>In regards to point 4, the manual actions credited in the Fire Safe Shutdown Assessment have not been identified in operating procedures (Gap). These procedures must be developed or updated to incorporate these operator actions. As a result of the improvements of fire protection provisions to achieve alignment with N293-07 requirements and to follow up from the Bruce A FSSA that specified Operator actions that are potentially required to meet the station fire safe shutdown goals for some of the postulated fires, Bruce Power will conduct a review of Bruce A Operator manual actions. This review will assess if any gaps exist in the required response to hazards identified in the FSSA. This review has already been conducted at Bruce B and determined that no gaps exist. This action is monitored under AI 1207-3890.</p> <p>Detailed assessment is provided in Safety Factor 7 Hazard Analysis.</p>	




Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design


File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>2. include the list of safe shutdown equipment</p> <p>3. define and describe the characteristics associated with hazards for all areas that contain hazardous materials</p> <p>4. describe the performance criteria for detection systems, alarm systems, and mitigation systems, including requirements such as seismic or environmental qualification</p> <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>Table 2-1 in the SMA report in identifies the success path systems for safe shutdown. The Bruce A System Classification lists were updated to reflect the need for either seismic or environmental qualification and noted if they were a success path system. (See Safety Classification Lists Form 11822).</p>	


	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>The objective of the hazard analysis is to determine the adequacy of protection of the NPP 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 rules and criteria 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>		


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"> • CNSC, RD-346, Site Evaluation for New Nuclear Power Plants, Ottawa, Canada, 2008. • CNSC, RD/GD-369, Licence Application Guide: Licence to Construct a Nuclear Power Plant, Ottawa, Canada, 2011. • CSA Group, N293, Fire protection for nuclear power plants, Toronto, Canada, 2012. • CSA Group, N289.4, Testing procedures for seismic qualification of nuclear power plants, Toronto, Canada. • IAEA, NS-G-3.3, Evaluation of Seismic Hazards for Nuclear Power Plants, Vienna, 2002. • IAEA, NS-G-1.5, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Vienna, 2003. • IAEA, NS-G-3.1, External Human Induced Events in Site Evaluation for Nuclear Power Plants, Vienna, 2002. • IAEA, NS-G-3.5, Flood Hazard for Nuclear Power Plants on Coastal and River Sites, Vienna, 2003. • IAEA, NS-G-3.4, Meteorological Events in Site Evaluation for Nuclear Power Plants, Vienna, 2003. • IAEA, SSG-18, Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations, Vienna, 2011. • IAEA, NS-G-1.7, Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants, Vienna, 2004. • IAEA, NS-G-1.11, Protection Against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power 		

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
	Plants, Vienna, 2004. <ul style="list-style-type: none"> IAEA, NS-G-1.6, Seismic Design and Qualification for Nuclear Power Plants, Vienna, 2003. IAEA, SSG-9, Seismic Hazards in Site Evaluation for Nuclear Installations, 2 Vienna, 2010. 		
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"> CNSC, REGDOC-2.4.1, Deterministic Safety Analysis, Ottawa, Canada, 2014. CNSC, RD/GD-369, Licence Application Guide: Licence to Construct a Nuclear Power Plant, Ottawa, Canada, 2011. 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. CSA Group, N286.7, Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants, Toronto, Canada. IAEA, SSG-2, Deterministic Safety Analysis for Nuclear Power Plants, Vienna, 2009. IAEA NS-G-1.2, Safety Assessment and Verification for Nuclear Power Plants, Vienna, 2001. 	<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 code-to-code 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

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01


Article No.	Clause Requirement	Assessment	Compliance Category
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"> ASME/ANS, RA-Sa-2009, Standard for Level 1/Large Early Release Frequency PRA for Nuclear Power Plant Applications, La Grange, Illinois, 2009. CNSC RD/GD-369, Licence Application Guide: Licence to Construct a Nuclear Power Plant, Ottawa, Canada, 2011. CNSC, REGDOC-2.4.2, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, Ottawa, Canada, 2014. IAEA, SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 2010. IAEA, SSG-4, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 2010. IAEA, Safety Series No. 50-P-10, Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 1995. IAEA Safety Reports Series No. 25, Review of Probabilistic Safety Assessments by Regulatory Bodies, Vienna, 2002. IAEA, Safety Series No. 50-P-7, Treatment of External 	<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 code-to-code assessment against CNSC REGDOC-2.4.2 is documented in Safety Factor 6.</p>	RNA

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Hazards in Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 1995.</p> <ul style="list-style-type: none"> IAEA, Safety Report Series No.10, Treatment of Internal Fires in Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 1998. 		
10.	Environmental Protection and Mitigation	This is not a requirement/guidance clause (this is a title only).	NA
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 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>	<p>There are no changes to the requirement.</p> <p>Section 2 Site Description of Part 1 of the Safety Report [NK21-SR-01320-00001, Rev. 005] describes the potential effect of the plant on population, agriculture, industry, transportation, fishing and recreation.</p> <p>The Bruce A design does not incorporate the best available technology and techniques economically achievable principle as recommended in the guidance section. Therefore, it is assessed as a gap (Gap).</p>	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>A new requirement for pollution prevention is added to this clause.</p> <p>A review of the same clause in RD-337 indicated that the Bruce A design does not fully meet this requirement, as documented in [NK21-CORR-00531-11005]. In regards to Items 7 and 8, effects of entrainment and impingement of aquatic species in the cooling water intake structures are potentially significant for some fish species. Items 7 and 8 were addressed in the Environmental Assessment for the Bruce1&2 ISR project.</p> <ul style="list-style-type: none"> Entrainment: The CCW flow rates are proportional to the number 	C

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Some of the factors that shall be considered include:</p> <ol style="list-style-type: none"> resource requirements for the NPP such as fuel, energy, and water depletion of ground and surface water resources contamination of air, soil and water resources nuclear and hazardous substances used types of waste generated – gaseous, liquid and solid quantities of waste generated impact of cooling water intake on entrainment and impingement impact of water output on the thermal regime of the receiving environment <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 included in the</p>	<p>of CCW pumps and/or the number of units in service at the station. No feasible mitigation measures are available to reduce CCW flow while continuing to allow the safe operation of Bruce A.</p> <ul style="list-style-type: none"> Impingement: Similar to entrainment, no feasible mitigation measures are available to reduce CCW flow while continuing to allow the safe operation of Bruce A. <p>Bruce Power Environmental Policy documented in BP-MSM-1, 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 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 R008] 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.</p> <p>DPT-ENV-00016, 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>As described in [RABA 0804], 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, R017]. Revised DRL's will be</p>	

	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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 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</p>	<p>submitted to the CNSC in the near future. Limits for release following accidents are included in the Appendix to the Operating Policies and Principles as well as in the OSRs. Appropriate limits will be incorporated into the Safe Operating 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 CSA N288.1 and were included in the PROL renewal applications [NK21-CORR-00531-10873/ NK29-CORR-00531-11252]. These N288.1-aligned DRLs have been added to Appendix C of the current Bruce A and Bruce B PROLs [NK21-CORR-00531-11715].</p> <p>Pollution prevention principles have been incorporated into Appendix A of the Bruce Power Environmental Policy documented in BP-MSM-1, Management System Manual, where it states that: "Bruce Power commits to ... [m]inimizing our environmental impact and prevention of pollution by minimizing emissions, preventing spills, reducing waste, and reusing or recycling our resources."</p>	




Rev Date: July 8, 2016

Status: Issued

Subject: Safety Factor 1 - Plant Design

File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>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"> • the age of equipment and facilities involved • how the option is designed, built, maintained, operated and decommissioned • the process employed • the engineering aspects of the application of various types of control techniques • process changes • technological advances or changes in scientific knowledge and understanding • cost of achieving the environmental benefits or reducing the environmental impacts • socioeconomic factors • time limits for installation of new and existing plants • other environmental impacts (including energy requirements) • other such factors as deemed appropriate by the regulator <p>The selected condenser cooling technology should incorporate the latest in mitigation technology and techniques.</p> <p>Additional information</p>		

 <small>Division of Kinectrics Inc.</small>	Rev Date: July 8, 2016	Status: Issued
	Subject: Safety Factor 1 - Plant Design	File: K-421231-00011-R01

Article No.	Clause Requirement	Assessment	Compliance Category
	<p>Additional information may be found in:</p> <ul style="list-style-type: none"> • CNSC, G-296, Developing Environmental Protection Policies, Programs and Procedures at Class I Nuclear Facilities and Uranium Mines and Mills, Ottawa, Canada, 2006. • CNSC, REGDOC-2.9.1, Environmental Protection: Policies, Programs and Procedures, Ottawa, Canada, 2013. • CNSC P-223, Protection of the Environment, Ottawa, Canada, 2001. 		