FORM-14159 R000*

Periodic Safety Review - Final Document Review Traveler

Bruce Power

Bruce Power Document #:	Revision:	Information Classification	Usage Classification
NK21-SFR-09701-00006	R000	Internal Use Only	Information

Bruce Power Document Title:
Safety Factor 6 – Probabilistic Safety Analysis

Bruce Power Contract/Purchase Order:	Bruce Power Project #:
00193829	38180

Supplier's Name:	Supplier Document #:	Revision:
CANDESCO	K-421231-00016	R00

Supplier Document Title:
Safety Factor 6 – Probabilistic Safety Analysis

Accepted for use at Bruce Power by:	**Signature:**	**Date**
Name: Gary Newman Title: Chief Engineer & Sr. Vice President, Engineering	G Newman	27AUG2015

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

*Associated with BP-PROC-01024, Periodic Safety Reviews

Periodic Safety Review - Final Document Review Traveler

Sheet # 2 of 4

Bruce Power Document #:	NK21-SFR-09701-00006	Rev #: R000	**Information Classification:** Internal Use Only	**Usage Classification:** Information
Bruce Power Document Title:	Safety Factor 6 – Probabilistic Safety Analysis	Suppliers Name:	CANDESCO	
Bruce Power Contract/ Purchase Order:	00193829	Supplier Document Title:	Safety Factor 6 – Probabilistic Safety Analysis	
Bruce Power Project #:	38180	Supplier Document:	K-421231-00016	Rev #: R00

Reviewed By:

Name	Title	Department	Signature	Date
Ken Chuong	Sr. Technical Specialist	Nuclear Safety Analysis & Support	[signature]	July 27, 2015
Joan Higgs	Technical Advisor, Engineering	Nuclear Safety Analysis & Support	[signature]	JULY 27, 2015
Rob McLean	Sr. Technical Engineer	Nuclear Safety Analysis & Support	[signature]	28 JUL 2015

Recommended for Use By:

Name	Title	Department	Signature	Date
Phil Hunt	Division Manager	Reactor Safety Engineering	[signature]	19 Aug 2015

Periodic Safety Review - Final Document Review Traveler

Sheet # 3 of 4

Bruce Power Document #:	NK21-SFR-09701-00006	Rev #: R000	**Information Classification:** Internal Use Only	**Usage Classification:** Information
Bruce Power Document Title:	Safety Factor 6 – Probabilistic Safety Analysis	Suppliers Name:	CANDESCO	
Bruce Power Contract/ Purchase Order:	00193829	Supplier Document Title:	Safety Factor 6 – Probabilistic Safety Analysis	
Bruce Power Project #:	38180	Supplier Document:	K-421231-00016	Rev #: R00

Reviewed By:

Name	Title	Department	Signature	Date
Susan Brissette	Dept. Manager	Management Systems	SBrissette	31JULY 15

Recommended for Use By:

Name	Title	Department	Signature	Date
Susan Brissette	Dept. Manager	Management Systems	SBrissette	31 JULY 15

Periodic Safety Review - Final Document Review Traveler

Sheet # 4 of 4

Bruce Power Document #:	NK21-SFR-09701-00006	Rev #: R000	**Information Classification:** Internal Use Only		**Usage Classification:** Information
Bruce Power Document Title:	Safety Factor 6 – Probabilistic Safety Analysis	Suppliers Name:	CANDESCO		
Bruce Power Contract/ Purchase Order:	00193829	Supplier Document Title:	Safety Factor 6 – Probabilistic Safety Analysis		
Bruce Power Project #:	38180	Supplier Document:	K-421231-00016		Rev #: R000

Reviewed By:

Name	Title	Department	Signature	Date
Scott Ellis	Section Manager	Probabilistic Safety Analysis	[signature]	21-AUG-2015
Ed Arciszewski	Technical Advisor, Engineering	Probabilistic Safety Analysis	[signature]	21 Aug 2015

Recommended for Use By:

Name	Title	Department	Signature	Date
Phil Hunt	Division Manager	Reactor Safety Engineering	P. Hunt	21 Aug 2015

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

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**

Division of Kinectrics Inc.

Title: Safety Factor 6 - Probabilistic Safety Analysis

File: K-421231-00016-R00

NK21-SFR-09701-00006

A Report Submitted to Bruce Power

June 30, 2015

Issue	**Reason for Issue:**				
R00D0	For first internal Candesco review				
	Author: S. Kondratyuk	Verifier:	Reviewer: G. Archinoff T. Kapaklili	Approver:	Date: Nov 27, 2014
Issue	**Reason for Issue:**				
R00D1	For harmonization, which incorporates internal Candesco review comments				
	Author: S. Kondratyuk	Verifier:	Reviewer: G. Archinoff T. Kapaklili	Approver:	Date: Jan 13, 2015
Issue	**Reason for Issue:**				
R00D2	For final internal Candesco review				
	Author: S. Kondratyuk	Verifier:	Reviewer: G. Archinoff L. Watt	Approver:	Date: Feb 20, 2015
Issue	**Reason for Issue:**				
R00D3	Issued to Bruce Power for review				
	Author: S. Kondratyuk	Verifier: G. Buckley	Reviewer: G. Archinoff L. Watt	Approver:	Date: March 6, 2015

<table>
<tr><td rowspan="2">Issue
R00D4</td><td colspan="5">Reason for Issue:
Incorporates changes from Bruce Power review</td></tr>
<tr><td>Author:
S. Kondratyuk</td><td>Verifier:
G. Aldev</td><td>Reviewer:
G. Archinoff
L. Watt</td><td>Approver:</td><td>Date:
June 19, 2015</td></tr>
<tr><td rowspan="2">Issue
R00</td><td colspan="5">Reason for Issue:
For use</td></tr>
<tr><td>Author:
S. Kondratyuk</td><td>Verifier:
G. Aldev
C. Stallman</td><td>Reviewer:
G. Archinoff
L. Watt</td><td>Approver:
L. Watt</td><td>Date:
June 30, 2015</td></tr>
<tr><td colspan="3">Document Classification:
Report</td><td colspan="3">Security Classification:
Client Proprietary</td></tr>
</table>

Table of Contents

List of Tables

Acronyms and Abbreviations

BAPRA	Bruce A Probabilistic Risk Assessment
BDBA	Beyond Design Basis Accident
BP	Bruce Power
CAFTA	Computer Aided Fault Tree Analysis
CANDU	Canada Deuterium Uranium
CCF	Common Cause Failure
CNSC	Canadian Nuclear Safety Commission
COG	CANDU Owners Group
CSA	Canadian Standards Association
DBA	Design Basis Accident
EA	Environmental Assessment
EBCS	Emergency Boiler Cooling System
EME	Emergency Mitigating Equipment
EPRI	Electric Power Research Institute
FASA	Focus Area Self-Assessment
FDC	Fuel Damage Category
FT	Fault Tree
FV	Fussell-Vesely
GAR	Global Assessment Report
HI	Human Interaction
IAEA	International Atomic Energy Agency
IEs	Initiating Events
IFB	Irradiated Fuel Bay
ISR	Integrated Safety Review
LCH	Licence Conditions Handbook
LPSW	Low Pressure Service Water
LRF	Large Release Frequency
LTEP	Long Term Energy Plan
MAAP	Modular Accident Analysis Program

MCR	Major Component Replacement
MSM	Management System Manual
NGS	Nuclear Generating Station
NPP	Nuclear Power Plant
NSCA	Nuclear Safety and Control Act
OFI	Opportunities for Improvement
PDSs	Plant Damage States
PEVS	Powerhouse Emergency Venting System
PIE	Postulated Initiating Event
PRA	Probabilistic Risk Assessment
PROL	Power Reactor Operating Licence
PSA	Probabilistic Safety Assessment (synonymous with PRA)
PSR	Periodic Safety Review
QA	Quality Assurance
QPS	Qualified Power Supply
RAW	Risk Achievement Worth
RCs	Release Categories
SAM	Severe Accident Management
SAMG	Severe Accident Management Guidelines
SBR	Safety Basis Report
SCA	Safety Control Area
SCDF	Severe Core Damage Frequency
SFR	Safety Factor Report
SIS	Systems Important to Safety
SLOCA	Small Loss-of-Coolant Accident
SRF	Small Release Frequency
SSC	Structure, System and Component
ULHS	Unit Loss-of-Heat Sink

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

[1] RD-360 [4] was superseded by CNSC REGDOC-2.3.3 [6] in April 2015. CNSC REGDOC-2.3.3 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 IAEA 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 IAEA SSG-25, and therefore it is considered that the ISR envelops the guidelines in CNSC REGDOC-2.3.3.

and improvement of safety culture and the achievement of high levels of safety, as well as reliable and economic performance.

The specific objectives of the review of this Safety Factor[2] are to determine:

- The extent to which the existing Probabilistic Safety Assessment (PSA) study remains valid as a representative model of the nuclear power plant;
- Whether the results of the PSA show that the risks are sufficiently low and well balanced for all postulated initiating events and operational states;
- Whether the scope (which should include all operational states and identified internal and external hazards), methodologies and extent (i.e., Level 1, 2 or 3) of the PSA are in accordance with current national and international standards and good practices; and
- Whether the existing scope and application of PSA are sufficient.

1.2. Description

The review is conducted in accordance with the Bruce A ISR Basis Document [1], which states that the review tasks are as follows:

1. The existing PSA, including the assumptions used, the fault schedule, the representations of operator actions and common cause events, the modelled plant configuration and consistency with other aspects of the safety case;
2. Whether accident management programs for accident conditions (design basis accident conditions and design extension conditions) are consistent with PSA models and results;
3. Whether the scope and applications of the PSA are sufficient;
4. The status and validation of analytical methods and computer codes used in the PSA;
5. Whether the results of PSA show that risks are sufficiently low and well balanced for all postulated initiating events and operational states, and meet relevant probabilistic safety criteria; and
6. Whether the existing scope and application of the PSA are sufficient for its use to assist the ISR global assessment, for example, to compare proposed improvement options.

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:

[2] This Safety Factor is entitled “Probabilistic Safety Analysis”. However, Probabilistic Safety Analysis is referred to as Probabilistic Safety Assessment (PSA) throughout the document; moreover, Probabilistic Risk Assessment (PRA) is equivalent to PSA.

- 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.

    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.

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 probabilistic safety analysis that are referenced in the Bruce Power Reactor Operating Licence (PROL) [15] and Licence Conditions Handbook (LCH) [16] noted in Table C-1 of the ISR Basis document [1] are identified in Table 1.[3] The edition dates referenced in the third column of the table are the modern versions used for comparison. The PROL contains the following clauses pertinent to this Safety Factor:

- Licence Condition 4.4 of the Operating Licence [15] states that the licensee shall implement and maintain a reliability program in accordance with CNSC regulatory document S-98 entitled Reliability Programs for Nuclear Power Plants.
- Licence Condition 5.1 states that the licensee shall implement and maintain a plant design basis management program such that the structures, systems and components continue to meet the design basis and the plant can operate safely for the full duration of its design life. Per the LCH [16] and the outcome of the design basis management program, Bruce Power is to conduct and maintain a Level 1 and 2 PSA in accordance with Licence Condition 5.5.

[3] 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.

- Licence Condition 5.5, states that probabilistic safety assessments shall be performed in accordance with CNSC Regulatory Document S-294.

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-98 [19]	Reliability Programs for Nuclear Power Plants	CNSC RD/GD-98 (2012) [20]	NR
CNSC S-294 [21]	Probabilistic Safety Assessment For Nuclear Power Plants	CNSC REGDOC-2.4.2 (2014) [22]	CTC
CNSC RD-360	Life Extension of Nuclear Power Plants	CNSC RD-360 (2008) [4]	NR
CSA N286-05 [23]	Management System Requirements for Nuclear Facilities	CSA N286-12 [24]	NR
CSA N286.7-99	Quality Assurance of Analytical, Scientific And Design Computer Programs for Nuclear Power Plants	CSA N286.7.-99 (R2012) [25]	CV
CSA N290.15-10	Requirements for the Safe Operating Envelope of Nuclear Power Plants	CSA N290.15-10 [26]	NR
Assessment type: Clause-by-Clause (CBC); Code-to-Code (CTC); High Level (HL); No Assessment Required (NR); Confirm Validity of Previous Assessments (CV)			

CNSC RD/GD-98: Table C-1 of the ISR Basis Document [1] calls for a confirmation of validity of the previous reviews of Regulatory Document RD/GD-98 [20], Reliability Programs for Nuclear Power Plants, which sets out the requirements and guidance of the CNSC for the development and implementation of a reliability program for nuclear power plants in Canada. RD/GD-98 [20] captures the existing requirements previously found in the eponymous S-98 (Revision 1) [19] and also replaces the latter document. A review against S-98 was completed for the Bruce 1 and 2 ISR and submitted to the CNSC and the program was established and implemented as required by licence condition 4.4 of the PROL [15]. The ISR Basis document [1] identified this review as “Confirm Validity of Previous Assessment”. Recent progress made by Bruce Power with regard to RD/GD-98 compliance is described in the correspondence with CNSC regarding Action Item AI 090711 [27], [28]. Line-by-line compliance with this regulatory document is verified on an ongoing basis to ensure compliance with the PROL, and therefore it was not assessed as part of this Safety Factor.

CNSC REGDOC-2.4.2: CNSC REGDOC-2.4.2, Probabilistic Safety Assessment for Nuclear Power Plants [22] sets out the CNSC requirements with respect to the Probabilistic Safety Assessment. It supersedes the previous version of the eponymous S-294 [21]. CNSC REGDOC-2.4.2 includes amendments to reflect lessons learned from the Fukushima nuclear event of March 2011, as applicable to S-294. CNSC REGDOC-2.4.2 [22] sets out 10 high-level requirements on the scope, quality and frequency of Probabilistic Risk Assessment (PRA) activities to be conducted by the licensee of a nuclear power plant (NPP) in Canada. In comparison with S-294, CNSC REGDOC-2.4.2 contains additional guidance clauses that elaborate further on the requirements or provide direction on how to meet the requirements. In view of the importance of CNSC REGDOC-2.4.2 as the primary regulatory document for PSA, a clause-by-clause review was conducted against this standard and the results are included in Appendix B (B.1).

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 N286-12: Table C-1 of the ISR Basis [1] calls for a code-to-code review against Canadian Standards Association (CSA) standard CSA N286-05, although not for this Safety Factor. However, it is applicable to all Safety Factors and is addressed herein. 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” [29].

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 [30]. 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 [31]. 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.

CSA N286.7-99: CSA N286.7-99 [25] has been assessed as part of the 2013 interim PSR and has not changed since this assessment. Furthermore, the Bruce Power safety analysis Quality Assurance (QA) procedures ([32], [33]) cited in the Safety Factor 5 component of the 2013 interim PSR as demonstrating compliance with CSA N286.7-99 are unchanged. This assessment did not identify any gaps against this code. Therefore, review against this standard was not repeated as part of this Safety Factor.

CSA N290.15-10: CSA N290.15 [26] is the first edition of CSA standard for requirements for the safe operating envelope of nuclear power plants. This Standard provides requirements for the definition, implementation, and maintenance of the safe operating envelope at nuclear power plants. In addition, guidance material for existing Canada Deuterium Uranium (CANDU) nuclear power plants is provided in Annex A to support the requirements. The expectation is that Bruce Power will be compliant with this standard by September 2015 [34]. Therefore, there is no further discussion on this standard in this Safety Factor Report.

3.3. Regulatory Documents

In addition to those listed in the PROL [15] and Licence Conditions Handbook (LCH) [16], the Regulatory Documents identified in Table C-1 of the ISR Basis document [1] considered for application to review tasks of this Safety Factor are included in Table 2.

Table 2: Regulatory Documents

Document Number	Document Title	Reference	Type of Review
CNSC REGDOC-2.5.2 (2014)	Design of Reactor Facilities: Nuclear Power Plants	[35]	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 REGDOC-2.5.2: Table C-1 of the ISR Basis Document [1] calls for a code-to-code assessment of the differences between CNSC RD-337 and CNSC REGDOC-2.5.2 [35], followed by a clause-by-clause assessment against only those CNSC REGDOC-2.5.2 clauses without corresponding equivalent RD-337 clauses. It was decided to instead do a clause-by-clause assessment against all clauses of CNSC REGDOC-2.5.2 with relevance to this Safety Factor. CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants [35], which has superseded CNSC RD-337, sets out requirements and guidance for new licence applications for NPPs. It establishes a set of comprehensive design requirements and guidance that are risk-informed and align with accepted international codes and practices. The sections of CNSC REGDOC-2.5.2 that are relevant to PSA are assessed further in Appendix B (B.2), while a more detailed assessment is performed in Safety Factor 1 – Plant Design.

3.4. CSA Standards

In addition to those listed in the PROL [15] and LCH [16], the CSA standards identified in Table C-1 of the ISR Basis document [1] were considered for application to review tasks of this Safety Factor. These are identified in Table 3.

Table 3: CSA Standards

Document Number	Document Title	Reference	Type of Review
CSA N288.6-12	Environmental Risk Assessments at Class I Nuclear Facilities and Uranium Mines and Mills	[36]	CBC
Assessment type: Clause-by-Clause (CBC); Code-to-Code (CTC); High Level (HL); No Assessment Required (NR); Confirm Validity of Previous Assessments (CV)			

CSA N288.6-12: Standard CSA N288.6-12 [36] is determined not to be relevant to this Safety Factor. Rather, it is relevant to Safety Factor 14 – Radiological Impact on the Environment and an assessment is conducted in that Safety Factor Report.

3.5. International Standards

As applicable international guidance considered for application to review tasks of this Safety Factor are included in Table 4.

Table 4: International Standards

Document Number	Document Title	Reference	Type of Review
IAEA SSG-25 (2013)	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)			

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

The codes and standards discussed in the previous sub-sections have been determined to be sufficient for the completion of the review tasks of this Safety Factor. Accordingly, additional codes and standards are not considered in this Safety Factor Report.

4. Overview of Applicable Bruce A Station Programs and Processes

Within the organization of Bruce Power's programs and processes, probabilistic safety analysis falls under the broader function of Nuclear Safety Assessment, which also covers activities such as deterministic safety analysis and criticality safety assessment. The Nuclear Safety Assessment function, together with the Design Management Function, falls under Bruce Power's Plant Design Basis Management Program.

Nuclear safety is addressed at the highest level of the hierarchy in the Management System Manual (MSM) [37]. The high level policies described in the MSM find expression in the program on Plant Design Basis Management [38]. In addition, the boundaries within which the station may be operated safely are outlined for Bruce A in the Operating Policies and Principles BP-OPP-00002 [39]. The program is implemented through the following high-level procedures:

- BP-PROC-00363 on Nuclear Safety Assessment [40];
- BP-PROC-00335 on Design Management [41];
- BP-PROC-00582 on Engineering Fundamentals [42];
- BP-PROC-00502 on Resolution of Differing Professional Opinions [43];
- DIV-ENG-00009 on Design Authority [44].

The high-level procedure BP-PROC-00363 [40] is particularly relevant to this review of Safety Factor 6. Regarding PRA, the implementation of BP-PROC-00363 [40] on Nuclear Safety Assessment is supported by DIV-ENG-00010 [45], the purpose of which is to establish a process for the evaluation of the safe operation of the station utilizing PRA and comparing the results against established safety goal targets and limits.

The PRA process is made up of four distinct sub-processes. This process is initiated by the preparation of PRA. Unavailability models (for example, for Systems Important to Safety per DPT-RS-00012 [46]) are then derived from the PRA using prescribed techniques. The PRA or the unavailability models are then used to determine the economic importance of changes to the station design. Finally, for assessment of risk that is not represented in the presently issued PRA, there is an evaluation for those conditions that were not modelled into the PRA. Any resulting physical changes to the station systems that are not modelled will necessitate revision of the PRA and unavailability models.

Four lower level procedures define the actual required processes in PRA applications to ensure safe operation:

- Procedure DPT-RS-00008 [47] details the methods that must be utilized in the preparation and maintenance of unavailability models.
- For changes that may affect the design configuration of structures, systems and components associated with the safety-related systems in a nuclear power plant, procedure DPT-RS-00004 [48], Risk Assessment of Proposed Changes to Engineering, Operations, Surveillance and Maintenance, details the processes involved with the evaluation of these changes using either the PRA or the applicable unavailability model.
- Procedure DPT-RS-00003 [49], Evaluation of Risk Outside the Scope of the PRA, describes the process for making changes to the existing PRA in order to evaluate the risk associated when operating in an unanalyzed state.
- Procedure DPT-RS-00007 [50], Preparation and Maintenance of Probabilistic Risk Assessments, defines the process for preparing a PRA, as well as the systematic process of updating the PRA in order to maintain it as a “Living PRA”.

In addition to these four PRA procedures, there are related procedures that interface with them:

- DPT-RS-00002 [51], Risk Assessment of Operational Events, which prescribes how the risk of specific operational events should be evaluated.
- DPT-RS-00006 [52], Outage and Inage Risk Management, which describes the process to be used for Outage and Inage Risk Management with respect to Bruce Power safety goals and the licensing requirements applicable to reliability and risk.
- DPT-RS-00012 [46], Systems Important to Safety (SIS) Decision Methodology, which describes the logic and processes involved in evaluating the modelled systems in Bruce Power’s PRAs, to determine which Systems Important to Safety are risk significant.

Finally, three quality assurance related procedures also apply to PRA work:

- DPT-NSAS-00001 [32], Quality Assurance of Safety Analysis, which governs the quality assurance of safety analysis work in support of nuclear safety assessments;
- DPT-NSAS-00008 [33], Management of External Work for Nuclear Safety Analysis and Support, which prescribes how safety analysis work contracted to external parties should be managed; and
- DIV-ENG-00013 [53], Planning of Internal Work for Nuclear Safety Analysis, which prescribes how safety analysis work performed internally by Bruce Power should be planned.

The Bruce Power policies, programs and procedures that relate to PRA are identified in Table 5.[4]

Table 5: Key Implementing Documents

First Tier Documents	Second Tier Documents	Third Tier Documents	Fourth Tier Documents
BP-MSM-1: Management System Manual [37]	BP-PROG-10.01: Plant Design Basis Management [38]	BP-PROC-00363: Nuclear Safety Assessment [40]	DIV-ENG-00010: Probabilistic Risk Assessment Process [45]
			DPT-RS-00008: Preparation and Maintenance of Unavailability Models [47]
			DPT-RS-00004: Risk Assessment of Proposed Changes to Engineering, Operations, Surveillance and Maintenance [48]
			DPT-RS-00003: Evaluation of Risk Outside the Scope of the Probabilistic Risk Assessment [49]
			DPT-RS-00007: Preparation and Maintenance of Probabilistic Risk Assessments [50]

[4] Table 5 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.

First Tier Documents	Second Tier Documents	Third Tier Documents	Fourth Tier Documents
			DPT-RS-00002: Risk Assessment of Operational Events [51]
			DPT-RS-00006: Outage and Inage Risk Management [52]
			DPT-NSAS-00001: Quality Assurance of Safety Analysis [32]
			DPT-NSAS-00008: Management of External Work for Nuclear Safety Analysis and Support [33]
			DIV-ENG-00013: Planning of Internal Work for Nuclear Safety Assessment [53]
	BP-PROG-11.01: Equipment Reliability [54]	BP-PROC-00778: Scoping and Identification of Critical SSCs [55]	DPT-RS-00012: Systems Important to Safety (SIS) Decision Methodology [46]

Note that two programmatic documents that were used for the Bruce 1&2 ISR have since been superseded, namely, DIV-OD-00028 [56] and DPT-NSAS-00009 [57]. These have been replaced by the implementing procedure DIV-ENG-00010 [45], which provides general governance of all PRA related procedures, establishes the process by which PRA is carried out, and provides Bruce Power risk based nuclear safety goals.

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. Existing Probabilistic Safety Analysis

The existing PSA, including the assumptions used, the fault schedule, the representations of operator actions and common cause events, the modelled plant configuration and consistency with other aspects of the safety case were reviewed.

The Bruce A Probabilistic Risk Assessment (BAPRA) (synonymous with Probabilistic Safety Assessment), 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 [58]. 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 [59].

The preparation of the Level 1 and Level 2 PRAs is based on the Bruce Power PRA guides for specific plant states and types of initiating events considered. For example, the Level 1 and Level 2 At-Power Internal Events PRAs are prepared in accordance with the PRA guides [60] and [61], respectively. The PRA Guides provide technical details of Bruce Power's PRA methodology. A list of current Bruce A PRA analyses, and corresponding PRA guides, is given below.

1a) Level 1 At-Power Internal Events PRA [59];

1b) Level 1 At-Power Internal Events PRA Guide [60];

2a) Level 1 Outage Internal Events PRA [61];

2b) Level 1 Outage Internal Events PRA Guide [62];

3a) Level 2 At-Power Internal Events PRA [63];

3b) Level 2 At-Power Internal Events PRA Guide [64];

4a) Level 2 Outage Internal Events PRA [65];

5a) At-Power Internal Fire PRA [66],

5b) Internal Fire PRA Guide [67];

6a) At-Power Internal Flood PRA [68];

6b) Internal Flood PRA Guide [69];

7a) At-Power Seismic PRA [70];

7b) Seismic PRA Guide [71];

8a) At-Power High Wind PRA [72];

8b) High Wind PRA Guide [73].

In addition, Bruce Power has conducted and issued:

9a) External Hazards Assessments [74], [75], [76], [77], [78];

9b) External Hazards Screening and Disposition Guide [79].

The PRA guides used for the preparation of the Bruce A PRAs have been accepted for use by CNSC, as documented in the letters [80], [81], [82], [83], [84] and [85]. The External Hazard guide and assessments were accepted by CNSC per the response letter [86].

The current Level 1 and Level 2 Bruce A PRAs take into consideration applicable multi-unit impacts. Throughout the update history of the BAPRA model, as summarized in Appendix F of the current Level 1 At-Power Internal Events PRA [59], continuing efforts have been made to improve its plant-specificity. Specific improvements include updating test interval frequencies, plant-specific changes of fault trees for selected systems, updated modelling of initiating events, inclusion of uncertainty data, implementation of Common Cause Failure (CCF) events, updating failure database and merging the Level 1 and Level 2 databases, revisions of Human Interaction (HI) failure probabilities, integration of the At-Power and Outage Level 1 models, inclusion of the Emergency Mitigating Equipment (EME) into the Level 1 PRA, and merging the EME Fault Tree (FT) database into the BAPRA database to form a single BAPRA database for Level 1 and Level 2 At-Power models and Level 1 Outage model. Updates to the fault tree models are described in 2013 Bruce A Probabilistic Risk Assessment Level 1 At-Power Summary Report [87].

The structure and analysis of event trees used in BAPRA are based on the approach described in Appendix E of the Bruce A Probabilistic Risk Assessment Level 1 At-Power Event Tree Analysis for project B1130 [88]. Sections E.2 to E.26 of [88] describe the event tree (ET) analysis for each set of initiating events (IEs) considered, including a description of the IE, its ET diagram and functional fault trees, and associated assumptions. Section E.27 of [88] provides a summary of the failure criteria for the various branch point mitigating systems.

All fault trees were developed in the Computer Aided Fault Tree Analysis (CAFTA) environment, using the standard fault tree development process and structure outlined in Section 2.3.5 of the Bruce Power Level 1 At-Power PRA Guide [60]. Updates to the fault tree models are described in the 2013 Bruce A Probabilistic Risk Assessment Level 1 At-Power Summary Report [87].

The treatment of Common Cause Failures (CCFs) in the current BAPRA model is based on the methodology documented in [89].

The guidance on the methods used in the BAPRA model for quantification of human interaction (HI) failure events is described in Section 2.4 of the Bruce Power Level 1 At-Power PRA Guide [60].

The CNSC conducted an inspection [90] of the Bruce Power Probabilistic Safety Assessment, and the specific focus was compliance of the Level 1 and Level 2 At-Power Internal Events PRAs with the requirements of CNSC S-294.[5] The inspection based its conclusions on

[5] A detailed assessment of CNSC REGDOC-2.4.2, which superseded S-294, is included in Appendix B (B.1).

examination of sample PRA scenarios. The results of the inspection were that Bruce Power has followed the CNSC accepted methodology for producing the PSA reports (as described in the Level 1 and Level 2 PRA Guides [60] and [64]), specifically in the areas of initiating events' quantification, uncertainty, sensitivity and importance analyses. It was also found that Bruce Power has a process for making changes to the PRA models as required by the S-294 standard, that the containment analysis in the Level 2 PRA and the interface between the Level 1 and Level 2 analyses are in agreement with the methodology, as are the definitions of the Plant Damage States (PDSs) and Release Categories (RCs).

However, the inspection also found that the updates of the fault tree analysis are not sufficiently traceable, and that some assumptions in FT models are not supported by the methodology, that quantification of HI events should be refined and should be applied consistently, and that the treatment of basic event reliability parameters does not fully reflect the plant as built and operated. As a result of these findings, 8 Action Notices and 11 Recommendations were issued, as documented in the inspection report [91]. Bruce Power has submitted a response letter [92] describing specific corrective action plans that are being pursued to address the findings of the inspection. An Action Notice is defined in Appendix A of the CNSC Inspection Report [90] as "a written request that the licensee…take action to correct a non-compliance that is not a direct contravention of the NSCA, the applicable regulations, licence conditions, codes or standards, but that can compromise safety…and that may lead to a direct non-compliance if not corrected". Taking into account that the Action Notices do not reflect a direct non-compliance with codes and standards, it is therefore concluded that the findings of the CNSC Inspection [90] do not result in additional gaps in this Safety Factor report. Further details on the inspection conclusions can be found in Section 7.3.

The requirements considered within the scope of this review element are assessed to be met.

5.2. Consistency of Accident Management Programs with PSA Models and Results

Accident management programs for accident conditions (design basis accident conditions and design extension conditions) and their consistency with PSA models and results were reviewed.

Bruce Power has issued a Severe Accident Management (SAM) program [93], which has been developed to deal with the possibility of a severe accident occurring on a single reactor unit operating initially at high power. Severe Accident Management Guidelines (SAMG) is currently being updated to implement improvements proposed in the CANDU Owners Group (COG) joint project JP4426 in response to the events at the Fukushima Daiichi plant [94]. The scope of the project includes responses for multi-unit and Irradiated Fuel Bay (IFB) events in severe accident conditions, and SAMG for shut down units or low-power operation.

As part of the current SAM program, Bruce Power has issued a number of SAMG documents, including a hierarchy of guides and procedures implementing the SAM procedure [93], under the Technical Support Group User's Guide [95]. The hierarchy defines conditions for entry into a SAM process, and it contains a structured set of SAM tools (e.g., a Diagnostic Flow Chart [96] personnel instructions [97] [98] and a severe challenge status tree [99]) to provide a pre-planned, systematic approach to guide the plant response in case of a severe accident.

The current SAMG has been developed by taking PRA results across the Industry into account.

Although in this context, PRA has and is being used to inform the SAMG program, the actions undertaken by operating staff in executing EME actions are more clearly defined and hence are easier to model and credit in PRA. The accident management function is well represented in the current PRAs and is being extended to include credit for EME functions in the S-294 compliant PRA. Hence, it is Bruce Power's position that SAMG credits in the PRA need not be considered at this time. Bruce Power plans to retain the SAMG function as a residual risk management measure and not to credit it explicitly in PRA.

The requirements considered within the scope of this review task are assessed to be met.

5.3. Sufficiency of Scope and Applications of PSA

The scope and applications of the PSA were reviewed to determine if they are sufficient.

The sufficiency of the scope of a PRA can be judged on the basis of CNSC REGDOC-2.4.2 [22]. A clause-by-clause assessment of CNSC REGDOC-2.4.2 has been performed and is documented in Appendix B (B.2). In particular, Clause 4.1 of CNSC REGDOC-2.4.2 requires that a Level 1 and Level 2 PSA be performed for each NPP, with considerations including the reactor core and other radioactive sources such as the irradiated fuel bay, and taking into account multi-unit impacts.

The scope of the Bruce A PRA encompasses Level 1 and Level 2 analyses for the at-power and outage plant states, initiated by internal and external events, the latter subdivided into internal and external hazards. A full list of the current Bruce A PRAs is given in Section 5.1.

The main results of the Level 1 PRAs are frequencies of core damage states that can result from various accident sequences. The core damage states are defined based on their severity, time of progression and other features using insight from deterministic analyses. The frequencies of consequential core damage states are summed to obtain the Severe Core Damage Frequency (SCDF) for comparison against the corresponding safety goal.

The Level 2 PRAs further develop accident sequences from the Level 1 analyses, to obtain estimates of frequencies of radioactive releases outside of the reactor containment system. Release categories are defined based on their radioactive contents, duration and location of release, using deterministic analyses. The frequencies of specific release categories are summed to obtain estimates for comparison against the two safety goals associated with Level 2 PRA: Large Release Frequency (LRF) and Small Release Frequency (SRF).

As described in more detail in Section 5.5.1, the definition and quantitative values of the above safety goals, as used in the Bruce A PRA, are consistent with the requirements of Clause 4.2.2 of CNSC REGDOC-2.5.2 [35]. It is noteworthy that in the current regulatory framework the safety goals are defined on a per unit basis, whereas a definition of site-wide goals is lacking.[6]

[6] A recently proposed approach to site-wide characterization and assessment of Nuclear Power Plant risk can be found in the COG report [102]. Also, aspects of a whole-site PSA for CANDU reactors are the subject of a COG-JP-4499-001 [103].

Safety assessment of the irradiated fuel bay has been conducted outside the scope of PRA, as documented in [91]. This analysis was reviewed by CNSC and found acceptable [100].

In addition to the Level 1 and Level 2 internal events PRAs, several PRAs have been prepared for internal and external hazards, e.g. a fire PRA, a seismic PRA, an internal flooding PRA, and others. A full list of the current Bruce A PRAs is given in Section 5.1.

Bruce A PRAs are prepared and maintained under the general process described in the BP governing document [45], which establishes the requirements for the use of PRA at BP nuclear facilities. Within this framework, department procedure [50] provides instructions for the preparation and maintenance of plant-specific PRAs, defines the process for preparing a PRA as well as the systematic process of updating the PRA in order to maintain it as a "Living PRA".

In particular, regular updates of the BAPRA model incorporate accumulated significant changes stemming from design, operational, maintenance, analysis and PRA applications experience, as required to keep the PRA consistent with the as built and as operated state of the plant. The process of periodic risk reassessment in PRA, as defined in the procedure [50], is based on changes from significant operational events, approved, committed, or implemented changes to engineering, operations, surveillance and maintenance (based on [48]), evaluations of risk outside the scope of the existing PRA (based on [49]), design changes and component reliability updates (based on the Annual Reliability Report [101]), issues from operating experience, etc. In accordance with the governing document [38], a process of continuous maintenance of the PRA model has been implemented by Bruce Power since 2004. A full summary of updates of the BAPRA model is given in Appendix F of the current Level 1 Internal Events [59]. The development and implementation of the continuous and ongoing PRA maintenance process constitutes a strength as it exceeds the regulatory requirement of CNSC REGDOC-2.4.2 that PRA model be updated every five years (requiring more frequent updates only if the facility undergoes major changes).

To support continued safe and reliable operation of the plant, Bruce Power intends to continue to maintain and update the BAPRA for consistency with NPP testing and configuration management, taking into account the currently pursued asset management initiatives and associated with it risk-informed decision making practices.

The requirements considered within the scope of this review task are assessed to be met.

5.4. Status and Validation of Analytical Methods and Computer Codes Used in PSA

The status and validation of analytical methods and computer codes used in the PSA were reviewed.

Bruce A PRA models are built using analytical methods that are well-established in probabilistic risk analysis, as described in the Level 1 and Level 2 At-Power Internal Events PRAs [59] and [63]. These methods include event trees to model accident progression sequences and fault trees to model failure probabilities of mitigating systems. In addition, Bayesian methodology is used in updating frequencies of initiating events. The methodology used to model CCFs was submitted to the CNSC in the letter [89], and was accepted by CNSC per the response letter

[104]. The basic event reliability models and the methods used for quantification of HI failure events used in the BAPRA are described in Sections 2.5.2 and 2.4, respectively, of the Level 1 PRA Guide [60].

The BAPRA model assumptions have been validated by the plant system engineers and the reactor safety staff to ensure that plant design/operation is adequately reflected. In accordance with the procedure [47], the system unavailability models have been developed using fault trees consistent with those used in the PRA models.

The current Level 1 and Level 2 BAPRA models [59], [63] are implemented using a standard software package CAFTA, developed by Electric Power Research Institute (EPRI). The uncertainty and importance analyses have been performed using CAFTA-associated codes UNCERT and SYSIMP, and post-processing of fault trees has been done using a QRECOVER utility. In addition, the Modular Accident Analysis Program (MAAP) for CANDU, MAAP4-CANDU, is used in the Level 2 PRA [63] to assess the consequences of severe core damage progression challenging the containment system.

The computer codes for use in Level 1 and Level 2 Bruce Power PRAs have been accepted by CNSC, as stated in the letters [105] and [106], which acknowledge that the standard CSA N286.7-99 [25] or equivalent Quality Assurance (QA) computer code requirements are being followed by Bruce Power. Additional evidence of the regulator's acceptance of the PRA-related computer codes is documented in the correspondence between Bruce Power and the CNSC [107] [108] [109] [110].

The requirements considered within the scope of this review task are assessed to be met.

5.5. Compliance with Relevant Probabilistic Safety Criteria

The results of PSA were reviewed to determine if the PSA results show that risks are sufficiently low and well balanced for all postulated initiating events and operational states, and meet relevant probabilistic safety criteria.

5.5.1. Quantitative Safety Goals

The main results of the Bruce A PRA are reported as a comparison of the most important safety parameters with their respective Quantitative Safety Goals, which are numerical safety criteria to be used in association with PRA applications and against which the safety of nuclear reactors can be judged. The intent is to ensure the radiological risks arising from nuclear accidents associated with operation of nuclear reactors will be low in comparison to risks to which the public is normally exposed. Risk-based Safety Goals used in the Bruce A PRA to assess the acceptability of risk are defined in the Level 2 PRA Guide [64] for three safety parameters as follows:

- Quantitative Safety Goal for SCDF: Sum of frequencies of all event sequences that can lead to significant core degradation should not exceed 10^{-4} occurrences per reactor-year;

- Quantitative Safety Goal for SRF: Sum of frequencies of all event sequences that can lead to a release to the environment of more than 10^{15} Becquerels of Iodine-131 should not exceed 10^{-4} occurrences per reactor-year;
- Quantitative Safety Goal for LRF: Sum of frequencies of all event sequences that can lead to a release to the environment of more than 10^{14} Becquerels of Cesium-137 should not exceed 10^{-5} occurrences per reactor-year.

The results obtained in the Bruce PRA are summarized in Table 6, where the specific type of the PRA is identified in each row. These results individually meet all of Bruce Power's probabilistic safety goals. Note that, consistent with the requirements of Clause 4.2.2 of the CNSC REGDOC-2.5.2 [35], these safety goals are calculated on a per reactor (or per unit) basis (although multi-unit impacts on a single unit are considered). However, the results of the Bruce PRA cannot at present be compared with site-wide safety goals, as the latter have not been defined.

Clause 4.2.2 of CNSC REGDOC-2.5.2 [35] sets quantitative safety goals for aggregates of SCDF, SRF and LRF; namely, that the sum of SCDFs from all types of PRAs not exceed 10^{-5} occurrences per reactor-year, the sum of SRFs not exceed 10^{-6} occurrences per reactor-year, and the sum of LRFs not exceed 10^{-5} occurrences per reactor-year.[7] The guidance part of Clause 4.2.2 of CNSC REGDOC-2.5.2 [35] recommends that "calculations of the safety goals include all internal and external events as per CNSC REGDOC-2.4.2, PSA for Nuclear Power Plants" [22], noting however that "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". As can be seen from Table 6, each individual SCDF from the at-power internal events, outage internal events, internal flood, fire, seismic and high-wind PRAs meets the Bruce Power safety goal of 10^{-4} occurrences per reactor-year defined in the PRA Guide [64]. Similarly, each individual LRFs from the different PRA types meets the Bruce Power safety goal of 10^{-5} per reactor-year.

The sum of the individual SCDFs yields an aggregated SCDF of 3.24×10^{-5} occurrences per reactor-year, and the sum of the individual LRFs yields an aggregated LRF of 1.53×10^{-5} per reactor-year. Thus, the aggregated SCDF and LRF, obtained by summation across all Bruce A PRAs, do not meet the safety goals set in Clause 4.2.2 of CNSC REGDOC-2.5.2 [35]. This constitutes a gap against requirements for new NPPs (SF6-1).

[7] The requirements of CNSC REGDOC-2.5.2 [35] are intended for newly built NPPs. Consequently, the qualitative safety goals set in its Clause 4.2.2 are more stringent than those defined in the Bruce Power's PRA Guide [64]. Nevertheless, as explained in more detail in Section 3.3, CNSC REGDOC-2.5.2 is included in the scope of this ISR.

5.5.2. Reliability of Systems Important to Safety

The guidance portion of Clause 7.6 of CNSC REGDOC-2.5.2 [35] states that "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 Structure, System and Components (SSCs) important to safety identified in the design phase will necessarily be included in the reliability program".

RD/GD-98 [20] provides requirements and guidance of the CNSC for the development and implementation of the reliability program of an NPP.

At a high level, the conditions for the availability of systems at Bruce A are set out in the Operating Policies and Principles document [39]. The Bruce Power Equipment Reliability program document BP-PROG-11.01 [54] identifies the high-level reliability procedures that map to each RD/GD-98 program requirement. The definition of SIS and the treatment of such systems in the context of PRA are described in the methodology document [46].

Risk significant systems are listed in the Level 1 At-Power Internal Events PRA [59]. These systems are ranked according to the Fussell-Vesely (FV) and Risk Achievement Worth (RAW) importance measures, that describe to what extent the baseline SCDF changes due to setting a system's failure probability to zero (for FV) or to one (for RAW). The systems that are considered to be important to SCDF include the Low-Pressure Service Water (LPSW), Heat Transport Pressure and Inventory Control, and D_2O Storage, Recovery and Transfer Systems (PIC), Class 3 and Class 4 Electrical Systems (CL3 and CL4), Emergency Boiler Cooling System (EBCS) and Qualified Power Supply (QPS). In addition to these systems, an importance analysis conducted in the Level 2 At-Power Internal Events PRA [63] identified LPSW, QPS, and Powerhouse Emergency Venting System (PEVS) as being important to the release frequencies.

The 2013 Annual Reliability Report [101] contains detailed results on the thirteen Bruce A systems that comprise the SIS list. Quantitative unavailability models exist for eight of these systems: Standby Class 3 Power System, Qualified Power System, Emergency Coolant Injection System, Negative Pressure containment System, Heating, Ventilation and Air Conditioning System, Powerhouse Unit Ventilation and Emergency Venting System, Shutdown System 1 and Shutdown System 2. The unavailability targets for these systems were set out based on their design and operational requirements, per Section 2.3.2 of the COG guidance document COG-05-9011 [111]. For the remaining five systems (Heat Transport Pressure and Inventory Control, and D_2O Storage, Recovery and Transfer System, Class 4 Power Distribution System, Low Pressure Service Water System, Unit Instrument Air System and Common Instrument Air System), Bruce Power followed the COG guidance [111], where the applicable initiating events frequencies are used as system monitoring parameters.

As per guidance provided by CNSC RD/GD-98, the resulting unavailabilities are assessed against their respective targets. Clause 7.6 of CNSC REGDOC-2.5.2 requires that, for newly built reactors, "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 0.001". As shown in the Bruce A Annual Reliability Report [101], out of the eight SIS for which there are unavailability models (see above), 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.

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 [101], 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 validating the modelling assumptions, updating the Class 3 unavailability model if required and optimizing the testing program to reduce the unavailability. As per Bruce Power's response to CNSC action item 1307-4320, the targeted completion date to update the Class 3 unavailability model is the fourth quarter of 2014 [112].

The calculated unavailabilities of three SIS are above the 1E-03 value required by Clause 7.6 of CNSC REGDOC-2.5.2: 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 [111], this is considered as an acceptable deviation from the requirements of Clause 7.6 of CNSC REGDOC-2.5.2.Bruce Power is currently pursuing improvements of its reliability program. Recent progress made by Bruce Power with regards to RD/GD-98 compliance is described in the correspondence with CNSC regarding Action Item AI 090711 [27], [28]. In particular, the procedure DPT-RS-00012 [46] includes revisions to clarify the definition of Systems Important to Safety, also including the information on how to disposition systems with either RAW or FV importance measures. Having completed a mapping of the CNSC S-98 [19] clauses with the Bruce Power program implementing documents in the Bruce Power Equipment Reliability program BP-PROG-11.01 [54], a similar mapping will be done for the superseding document RD/GD-98 [20]. The timing of the detailed mapping will align with the implementation plan for the revised BP-PROG-11.01 which is currently targeted for October 31, 2015.

5.5.3. Reliability of the Shutdown Function

In addition to the gap described above against requirement Clause 4.2.2 of CNSC REGDOC-2.5.2, one gap against a guidance portion of Clause 8.4.2 has been identified. This concerns the recommendation that the reliability of the shutdown function should be such that the cumulative frequency of failure to shut down on demand is less than 10^{-5} failures per demand, and the contribution of all sequences involving failure to shut down to the large release frequency is less than 10^{-7}/yr. While the guidance goal of cumulative frequency of failure to shut down on demand being less than 10^{-5} can be demonstrated using the Fuel Damage Category FDC1 in the Level 1 PRA [59], results of the Level 2 Internal Events At-Power PRA [63] indicate that the contribution to the LRF from all sequences involving failure to shut down is about 2.3E-7 occurrences per reactor per year. Accordingly, the proposed safety goal of 10^{-7}/yr is not met, which constitutes a gap with respect to the guidance portion of this clause (SF6-2).

In view of the gaps identified above, the requirements considered within the scope of this review task are assessed to be partially met.

Table 6: Summary of Safety Parameters Obtained in Bruce A PRA

Type of PRA	Document References	Values of Safety Parameter(s) [per reactor year]	Notes
Level 1 At-Power Internal Events	[59]	SCDF=3.82E-06	PRA including Emergency Mitigating Equipment (EME)
Level 1 Outage Internal Events	[61]	SCDF=1.28E-05	
Level 2 At-Power Internal Events	[68] [113] [114]	LRF=1.47E-06, SRF=1.47E-06	PRA including EME (Ref. [114])
Level 2 Outage Internal Events	[65]	Not Available	No results for LRF or SRF are presented. The March 2014 CNSC submission [65] states that there is no need to complete a detailed Level 2 Outage Internal Events PRA, justifying this by the acceptably low SCDF from the Level 1 Outage Internal Events PRA and by a limited Level 2 Outage study.
Levels 1&2 At-Power Internal Fire	[66]	SCDF=8.72E-06 LRF=7.32E-06	PRA including EME

Type of PRA	Document References	Values of Safety Parameter(s) [per reactor year]	Notes
Level 1 At-Power Internal Flood	[68]	SCDF=5.5E-07 LRF<1E-06	PRA including EME It is stated in the reference cited that since the SCDF is <1E-06, the LRF will be too, hence no Level 2 PRA for internal flood would be performed.
Levels 1&2 At-Power Seismic	[70]	SCDF=1.7E-06, for events with return frequency up to 10000 yrs – equivalent to the Review Level Earthquake	PRA including EME Level 2 results are given in terms of a Containment Failure Frequency, CFF=1.3E-06
Levels 1&2 Outage Internal Fire	Not Available	Not Available	The January 2014 CNSC Submission [115] provides justification why outage PRA for internal fires, seismic events and internal floods does not need to be performed for S-294 compliance.[8]
Levels 1&2 Outage Internal Flood	Not Available	Not Available	The January 2014 CNSC Submission [115] provides justification why outage PRA for internal fires, seismic events and internal floods does not need to be performed for S-294 compliance.[8]

[8] In Reference [115], Bruce Power requests CNSC's agreement for this exclusion on the basis that "the risk from internal fires, internal floods and seismic events for a single unit on an outage is both low and well-managed in accordance with the principle that the level of detail in the PRA should be consistent with the level of risk". Technical details supporting this reasoning are provided in the appendices to [115]. The CNSC has accepted the arguments in [115] to exclude internal fires, internal floods and seismic events from the scope of Bruce Power's outage PRA [116].

Type of PRA	Document References	Values of Safety Parameter(s) [per reactor year]	Notes
Levels 1&2 Outage Seismic	Not Available	Not Available	The January 2014 CNSC Submission [115] provides justification why outage PRA for internal fires, seismic events and internal floods does not need to be performed for S-294 compliance.[8]
Levels 1&2 At-Power High Wind	[72]	SCDF=4.80E-06 LRF<4.80E-06	PRA including EME in the Level 1 Event Tree Logic
Levels 1&2 External Flooding (and other External Hazards)	[74] [75] [76] [77] [78]	Not Available	PRAs have not been done for these external hazards. But Hazards Assessments have been performed in accordance with the External Hazards Screening and Disposition Guide [79] and documented in the references [74]. Several of the hazards were not screened out in the Phase 1 assessment and hence analyzed further in Phase 2 assessments, in particular in [75] and [78].

5.6. Sufficiency of Scope and Application of PSA in Assessing Proposed Improvement Options

The existing scope and application of the PSA were reviewed to determine whether this is sufficient for its use to assist the ISR global assessment, for example, to compare proposed improvement options.

In laying out general recommendations for a Periodic Safety Assessment, IAEA SSG-25 states in Clause 2.17 that "in order to integrate the results of the reviews of individual Safety Factors, the operating organization should perform a global assessment of safety at the plant. The global assessment should consider all findings and proposed improvements from the Safety Factor reviews and interfaces between different Safety Factors". It is further stated in Clause 4.22 that "the level of plant safety should be determined by a global assessment reflecting, among other things, the combined effects of all Safety Factors. It is possible that a negative finding (deviation) in one Safety Factor can be compensated for by a positive finding (strength) in another Safety Factor".

In this context, one of the important features of a PRA indicating its sufficiency to assist a Global Assessment Review (GAR) is the degree to which the PRA facilitates clear interfaces with safety aspects assessed in Safety Factors other than the current one. The interfaces discussed in Section 6 indicate that the contents of the Bruce A PRA should incorporate information on actual state of the plant (which may include design, reliability program and effects of ageing), should be consistent with and supported by results of deterministic safety analyses and hazard assessments. The extent to which these aspects are reflected in the Bruce A PRA is discussed in more detail in Sections 5.3 and 5.5.2.

According to the Bruce A ISR Basis Document [1], the findings of the Safety Factor reviews will be consolidated and integrated in a GAR to arrive at overall conclusions regarding the continued safe operation and major component replacement in Bruce A. The GAR will also identify potential improvement opportunities that would address gaps between the current plant design and operation and modern codes, standards and practices, and describes how these opportunities are consolidated, ranked, and prioritized.

An implementation of plant improvements identified and prioritized in a GAR would be used in developing an optimized multi-faceted approach to decision making at the plant. Therefore, the Bruce A PRA is sufficient for this use.

The requirements considered within the scope of this review task are assessed to be met.

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 2: Actual Condition of SSCs" in Section 4.0, verifies that programs exist which ensures that reliability data is collected, integrated and made available to the design basis management program, including the probabilistic risk assessment process. In addition, risk analysis requires a database of reliability (unavailability) data from the station which can be assembled from the monitoring of SSCs as explained in Section 5.7.
- "Safety Factor 3: Equipment Qualification" in Sections 4 and 5.2, verifies that programs exist which identify and categorize equipment to monitor and maintain it appropriately for the life of the plant.
- "Safety Factor 4: Ageing" in Section 4, verifies that a link between ageing management and safety analysis is established through procedure [117]. This procedure describes how fitness for service inspection/monitoring and safety analysis activities are coordinated to ensure that safety margins are adequate and ageing management issues are addressed.

- "Safety Factor 5: Deterministic Safety Analysis" in Section 5.1, reviews analysis methods and computer codes used for deterministic safety analysis in comparison with current standards and requirements including CSA N286.7-99. In Section 5.2, this Safety Factor Report also addresses the classification of abnormal events and identification of postulated initiating events as required by CNSC REGDOC-2.4.1.
- "Safety Factor 7: Hazards Analysis" in Sections 5.1 and 5.2, respectively, assesses the systematic identification of external and internal hazards, some of which are PRA's Postulated Initiating Events (PIEs).

7. Program Assessment 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 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.

A review of audits and inspections that could potentially be relevant to this Safety Factor revealed that there have not been any PRA-related Focus Area Self Assessments (FASAs) in the last five years.

7.2. Internal and External Audits and Reviews

The objective of the audit process as stated in BP-PROG-15.01 [118] is threefold:

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

The objective is achieved by providing a prescribed method for evaluating established requirements against plant documentation, field conditions and work practices. The process describes the activities associated with audit planning, conducting, reporting, and closing-out. The results of the independent assessments are documented and reported to the level of management having sufficient breadth of responsibility for resolving any identified problems (as stated in Section 5.14.2 of [23]).

There have not been any audits or reviews in the last five years relevant to this Safety Factor.

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 all items are quickly corrected.

The CNSC conducted a Type || compliance inspection of the Bruce Power Probabilistic Safety Assessment in September 2014. The objective of the inspection was to verify that the submitted PSA followed the accepted methodologies in accordance with S-294 [119].

Based on the inspection sample reviewed, Bruce Power has followed the methodology for producing the PSA reports, specifically in the areas of Initiating Events, Event Trees, Uncertainty, Sensitivity and Importance Analysis in Level 1 PSA as well as for Level 2 PSA. Gaps have been identified for Fault Trees and data analysis which did not follow the methodology. For human reliability analysis, deficiencies were found in the consistent application of the methodology.

As a result of this inspection, 8 Action Notices and 11 Recommendations have been raised which are documented in BRPD-AB-2014-012 – Probabilistic Safety Assessment Inspection [119]. As documented in the response letter [92], Bruce Power has developed and is currently pursuing specific corrective action plans that address all of the findings of the inspection.

The action notices and recommendations made in the CNSC inspection [90] have been reviewed in light of the assessments performed as part of this Safety Factor Review to ensure that these findings do not result in gaps in addition to those listed in Table 7. Namely, according to the definitions given in the CNSC Inspection Report [90], a Recommendation is less consequential than an Action Notice, with the latter being defined as “a written request that the licensee…take action to correct a non-compliance that is not a direct contravention of the NSCA, the applicable regulations, licence conditions, codes or standards, but that can compromise safety…and that may lead to a direct non-compliance if not corrected”. Since the definition states that an Action Notice does not reflect a direct non-compliance with codes and standards, it is therefore concluded that, for the purposes of the present report, the findings of the CNSC Inspection [90] do not result in additional gaps. This conclusion is consistent with the general finding of the Inspection that Bruce Power “meets the regulatory requirements, with the exception of the above-noted non-compliances with Bruce PRA procedures. CNSC staff did not find evidence of unsafe operation that would result in undue risk to the health and safety of persons, the environment, or that would compromise respect for Canada’s international obligations”.

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.

There are no specific performance indicators associated with probabilistic safety assessment that are currently used.

The "CNSC Staff Integrated Safety Assessment of Canadian Nuclear Power Plants for 2013", issued in September 2014 [120], summarizes the 2013 ratings for Canada's NPPs in each of the 14 CNSC Safety and Control Areas (SCA), including safety analysis (which itself includes PSA). For 2013, the Bruce A rating for the safety analysis SCA was "satisfactory".

8. Summary and Conclusions

The overall objective of the Bruce A ISR is to conduct a safety review of Bruce A 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 objectives of the review of this Safety Factor are to determine:

- The extent to which the existing PSA remains valid as a representative model of the nuclear power plant;
- Whether the results of the PSA show that the risks are sufficiently low and well balanced for all postulated initiating events and operational states;
- Whether the scope (which should include all operational states and identified internal and external hazards), methodologies and extent (i.e., Level 1, 2 or 3) of the PSA are in accordance with current national and international standards and good practices; and
- Whether the existing scope and application of PSA are sufficient.

These specific objectives have been met by the completion of the review tasks specific to probabilistic safety analysis.

One strength was identified in the Integrated Safety Review of Safety Factor 6, as follows:

- Bruce Power has developed and implemented a process of continuous maintenance of the PRA model to ensure that the model is representative of the actual plant configuration and operation and testing at the station. This exceeds the requirement of CNSC REGDOC-2.4.2 (Clause 4.4) that the PRA models be updated every five years.

Table 7 summarizes the key issues arising from the Integrated Safety Review of Safety Factor 6.

Table 7: Key Issues

Issue Number	Gap Description	Source(s)
SF6-1	Although the result of each separate PRA meets the safety goal limits set up for Bruce A PRAs, their aggregates obtained by summation across all available PRA types, do not meet the more stringent quantitative safety goal targets set forth in the requirement clause.	Section 5.5.1 Micro-gaps against requirement clauses: REGDOC-2.5.2 – Clause 4.2.2
SF6-2	The proposed safety goal that the contribution to the large release frequency from all sequences involving failure to shut down be below 10^{-7}/yr events per reactor per year is not met.	Section 5.5.3 Micro-gaps against guidance clauses: REGDOC-2.5.2 – Clause 8.4.2

The overall conclusion is that, with the exceptions noted in Table 7, Bruce Power's programs meet the requirements of the Safety Factor related to Probabilistic Safety Analysis.

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, IAEA, March 2013.

[4] CNSC RD-360, Life Extension of Nuclear Power Plants, CNSC, February 2008.

[5] NK21-CORR-00531-03839, Bruce A Environmental Assessment Study Report, Bruce Power, 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 Operation: 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 15.00/2014), 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.

[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 S-98 Rev. 1, Reliability Programs for Nuclear Power Plants, CNSC, July 2005 (Superseded by RD/GD-98).

[20] CNSC RD/GD-98, Reliability Programs for Nuclear Power Plants, CNSC, June 2012.

[21] CNSC S-294, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, CNSC, April 2005.

[22] CNSC REGDOC-2.4.2, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, CNSC, May 2014.

[23] CAN/CSA N286-05, Management System Requirements for Nuclear Facilities, CSA, 2007.

[24] CAN/CSA N286-12, Management System Requirements for Nuclear Facilities, CSA, 2012.

[25] CSA N286.7-99, Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants, CSA, March 1999, R2012.

[26] CAN/CSA N290.15, Requirements for the Safe Operating Envelope of Nuclear Power Plants, CSA, August 2010.

[27] NK21-CORR-00531-10762/NK29-CORR-00531-11144, Action Item 090711: Bruce Power Reliability Program, Bruce Power Letter, F. Saunders to R. Lojk, October 10, 2013.

[28] NK21-CORR-00531-10448/NK29-CORR-00531-10849, Subject: Notification of Major Change to LCH Document: Revision 003 of BP-PROG-11.01, R003, Equipment Reliability, Bruce Power Email, A. Maksymyk to R. Lojk et al., January 25, 2013 (Verified by M. Poole, September 9, 2013).

[29] NK21-CORR-00531-11494/NK29-CORR-00531-11881, CSA N286-12 - Management System Requirements for Nuclear Facilities, Action Item 1307-4697, CNSC Letter, K. Lafrenière to F. Saunders, July 24, 2014.

[30] 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.

[31] NK21-CORR-00531-11563/NK29-CORR-00531-11946, CSA N286-12 - Management System Requirements for Nuclear Facilities, Action Item 1307-4697, Bruce Power Letter, F. Saunders to K. Lafrenière, September 9, 2014.

[32] DPT-NSAS-00001-R006, Quality Assurance of Safety Analysis, Bruce Power, August 2014.

[33] DPT-NSAS-00008-R004, Management of External Work for Nuclear Safety Analysis and Support, Bruce Power, September 14, 2011.

[34] NK21-CORR-00531-11728/NK29-CORR-00531-12117, Bruce A and Bruce B CSA N290.15 Compliance Update, Bruce Power Letter, F. Saunders to K. Lafrenière, December 9, 2014.

[35] CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants, CNSC, May 2014.

[36] CAN/CSA N288.6-12, Environmental Risk Assessments at Class I Nuclear Facilities and Uranium Mines and Mills, CSA, June 2012.

[37] BP-MSM-1-R012, Management System Manual, Bruce Power, June 23, 2014.

[38] BP-PROG-10.01-R009, Plant Design Basis Management, Bruce Power, December 4, 2014.

[39] BP-OPP-00002-R012, Operating Policies and Principles – Bruce A, Bruce Power, July 24, 2013.

[40] BP-PROC-00363-R003, Nuclear Safety Assessment, Bruce Power, January 24, 2013.

[41] BP-PROC-00335-R006, Design Management, Bruce Power, May 24, 2013.

[42] BP-PROC-00582-R003, Engineering Fundamentals, Bruce Power, July 25, 2014.

[43] BP-PROC-00502-R002, Resolution of Differing Professional Opinions, Bruce Power, October 12, 2010.

[44] DIV-ENG-00009-R005, Design Authority, Bruce Power, November 1, 2013.

[45] DIV-ENG-00010-R000, Probabilistic Risk Assessment Process, Bruce Power, December 15, 2006.

[46] DPT-RS-00012-R001, Systems Important to Safety (SIS) Decision Methodology, Bruce Power, September 24, 2013.

[47] DPT-RS-00008-R000, Preparation and Maintenance of Unavailability Models, Bruce Power, February 2, 2007.

[48] DPT-RS-00004-R001, Risk Assessment of Proposed Changes to Engineering, Operations, Surveillance and Maintenance, Bruce Power, October 4, 2011.

[49] DPT-RS-00003-R001, Evaluation of Risk Outside the Scope of the Probabilistic Risk Assessment, Bruce Power, January 26, 2007.

[50] DPT-RS-00007-R001, Preparation and Maintenance of Probabilistic Risk Assessments, Bruce Power, February 15, 2007.

[51] DPT-RS-00002-R000, Risk Assessment of Operational Events, Bruce Power, January 31, 2007.

[52] DPT-RS-00006-R001, Outage and Inage Risk Management, Bruce Power, January 28, 2011.

[53] DIV-ENG-00013-R001, Planning of Internal Work for Nuclear Safety Analysis, Bruce Power, March 2, 2009.

[54] BP-PROG-11.01-R004, Equipment Reliability, Bruce Power, October 8, 2013.

[55] BP-PROC-00778-R001, Scoping and Identification of Critical SSCs, Bruce Power, April 11, 2013.

[56] DIV-OD-00028, Probabilistic Risk Assessment, Bruce Power, (Superseded by DIV-ENG-00010).

[57] DPT-NSAS-00009-R000, Assessment Guidelines in Using PRA, Bruce Power, March 18, 2002 (Superseded by DIV-ENG-00010).

[58] C6798/TR/005-R04, Bruce A Nuclear Generating Station Probabilistic Risk Assessment (BAPRA) NNC Canada Limited, March 2003.

[59] NK21-CORR-00531-11324/NK29-CORR-00531-11729, Enclosure 10, Submission of S-294 Probabilistic Risk Assessment Final Reports (2014 Bruce A Probabilistic Risk Assessment (BAPRA) Level 1 At-Power PRA Model Integration Report (including Emergency Mitigating Equipment (EME)), NK21-03611.1 P NSAS), Bruce Power Letter, F. Saunders to K. Lafrenière, July 31, 2014.

[60] B-REP-03611-00005-R001, Level 1 At-Power Internal Events Probabilistic Risk Assessment (PRA) Guide, Bruce Power, June 2011.

[61] NK21-CORR-00531-11324/NK29-CORR-00531-11729, Enclosure 1, Submission of S-294 Probabilistic Risk Assessment Final Reports (2014 Bruce A Probabilistic Risk Assessment (BAPRA) Level 1 Outage PRA Model Summary Report, Bruce Power, NK21-03611.1 P NSAS), Bruce Power Letter, F. Saunders to K. Lafrenière, July 31, 2014.

[62] B-REP-03611-00006-R00, Level 1 Outage Internal Events Probabilistic Risk Assessment (PRA) Guide, Bruce Power, July 2010.

[63] NK21-CORR-00531-10958/NK29-CORR-00531-11342, Enclosure 3, Submission of S-294 Probabilistic Risk Assessment Deliverables (Bruce Nuclear Generating Station A Internal Flood Probabilistic Risk Assessment (PRA) Summary Report, Bruce Power, NK21-03611.1 P NSAS), Bruce Power Letter, F. Saunders to R. Lojk, December 24, 2013.

[64] B-REP-03611-00010-R01, Level 2 At-Power Internal Events Probabilistic Risk Assessment (PRA) Guide, Bruce Power, October 2012.

[65] NK21-CORR-00531-11091/NK29-CORR-00531-11491, Attachment A, S-294 Probabilistic Risk Assessment Confirmatory Activities, Bruce Power Letter, Letter, F. Saunders to K. Lafrenière, March 31, 2014.

[66] NK21-CORR-00531-11324/NK29-CORR-00531-11729, Enclosure 5, Submission of S-294 Probabilistic Risk Assessment Final Reports (Bruce Nuclear Generating Station A Fire Probabilistic Risk Assessment, Bruce Power, NK21-03611.1 P NSAS), Bruce Power Letter, F. Saunders to K. Lafrenière, July 31, 2014.

[67] B-REP-03611-00008-R00, Bruce Power Probabilistic Risk Assessment (PRA) Guide – Internal Fire, Bruce Power, January 2011.

[68] NK21-CORR-00531-10958/NK29-CORR-00531-11342, Enclosure 12, Submission of S-294 Probabilistic Risk Assessment Deliverables (Bruce Nuclear Generating Station A Internal Flood Probabilistic Risk Assessment (PRA) Summary Report, Bruce Power, NK21-03611.1 P NSAS), Bruce Power Letter, F. Saunders to R. Lojk, December 24, 2013.

[69] B-REP-03611-00007-R00, Bruce Power Probabilistic Risk Assessment (PRA) Guide – Internal Flood, Bruce Power, November 2010.

[70] NK21-CORR-00531-11324/NK29-CORR-00531-11729, Enclosure 3, Submission of S-294 Probabilistic Risk Assessment Final Reports (Bruce Nuclear Generating Station A Seismic Probabilistic Risk Assessment Summary Report, NK21-03611.5 P NSAS), Bruce Power Letter, F. Saunders to K. Lafrenière, July 31, 2014.

[71] B-REP-03611-00009-R00, Bruce Power Seismic PRA Guide, Bruce Power, November 2010.

[72] NK21-CORR-00531-11324/NK29-CORR-00531-11729, Enclosure 8, Submission of S-294 Probabilistic Risk Assessment Final Reports (2014 Bruce A Probabilistic Risk Assessment (BAPRA) High Wind PRA Model Report, NK21-03611.7 P NSAS), Bruce Power Letter, F. Saunders to K. Lafrenière, July 31, 2014.

[73] B-REP-03611-00012-R00, Bruce Power Probabilistic Risk Assessment Guide – High Wind Hazard, Bruce Power, November 2012.

[74] NK21-CORR-00531-11324/NK29-CORR-00531-11729, Enclosure 7, Submission of S-294 Probabilistic Risk Assessment Final Reports (External Hazards Assessment – Task 7 – Final Report, NK21-03611.7 P NSAS), Bruce Power Letter, F. Saunders to K. Lafrenière, July 31, 2014.

[75] NK21-CORR-00531-09809/NK29-CORR-00531-10287, Bruce A and B External Hazards Assessment, Bruce Power Letter, F. Saunders to R. Lojk, September 28, 2012.

[76] NK21-CORR-00531-10848/NK29-CORR-00531-11226, Bruce A and B External Hazards Assessment, Bruce Power Letter, F. Saunders to R. Lojk, December 12, 2013.

[77] B-03611.7 P NSAS, External Hazards Assessment, Phase 2c – (W03) External Flooding, Bruce Power, July 24, 2014.

[78] K-449958-REPT-0017-R01, External Hazards Assessment, Phase 2d, W03 – External Flooding, July 24, 2014.

[79] NK21-CORR-00531-09253/NK29-CORR-00531-09881, Submission of Revised Bruce Power Probabilistic Risk Assessment (PRA) Guide – Screening and Disposition of External Hazards, Bruce Power Letter, F. Saunders to R. Lojk, March 9, 2012.

[80] NK21-CORR-00531-08908/NK29-CORR-00531-09623, Bruce Power Level 1 At-Power and Outage Internal Events Probabilistic Risk Assessment Guides, CNSC Letter, Letter, K. Lafrenière to F. Saunders, August 31, 2011.

[81] NK21-CORR-00531-10191/NK29-CORR-00531-10595, Action Item 091411: Acceptance of Bruce Power Level 2 At-Power Internal Events Probabilistic Assessment (PRA) Guide, Rev. 1, CNSC Letter, Letter, R. Lojk to F. Saunders, January 21, 2013.

[82] NK21-CORR-00531-10193/NK29-CORR-00531-10599, Action Item 091411: Acceptance of Bruce Power Probabilistic Assessment (PRA) Guide – Internal Fire, Revision 1, CNSC Letter, R. Lojk to F. Saunders, January 21, 2013.

[83] NK21-CORR-00531-10638/NK29-CORR-00531-11030, Acceptance of Bruce Power's Level 1 Seismic Probabilistic Risk Assessment Guide, CNSC Letter, R. Lojk to F. Saunders, July 8, 2013.

[84] NK21-CORR-00531-10212/NK29-CORR-00531-10614, Action Item 091411: Acceptance of Bruce Power Probabilistic Risk Assessment (PRA) Guide – Internal Flood at Power, Revision 2, CNSC Letter, R. Lojk to F. Saunders, January 28, 2013.

[85] NK21-CORR-00531-10263/NK29-CORR-00531-10672, Acceptance of Bruce Power Probabilistic Risk Assessment Guide – High Wind Hazard, CNSC Letter, R. Lojk to F. Saunders, February 20, 2013.

[86] NK21-CORR-00531-11691/NK29-CORR-00531-12082 Bruce A and B External Hazard Assessment, CNSC Letter, K. Lafrenière to F. Saunders, October 31, 2014.

[87] NK21-03611.1 P NSAS, AMEC NSS document number B1294/RP/003-R01, 2013 Bruce A Probabilistic Risk Assessment Level 1 At-Power Summary Report, Bruce Power, August 30, 2013.

[88] NK21-03611.4 P NSAS, AMEC NSS document number B1130/RP/004-R01, Bruce A Probabilistic Risk Assessment Level 1 At-Power Event Tree Analysis (Appendix E), Bruce Power, June 28, 2013.

[89] NK21-CORR-00531-09019/NK29-CORR-00531-09699, Submission of Bruce Power – Probabilistic Risk Assessment Common Cause Failure Methodology, Bruce Power Letter, F. Saunders to R. Lojk, November 24, 2011.

[90] NK21-CORR-00531-11710/NK29-CORR-00531-12099, Action Item 2014-07-5551: CNSC Type II Compliance Inspection Report: BRPD-AB-2014-012 – Probabilistic Safety Assessment Inspection, CNSC, November 6, 2014.

[91] NK21-CORR-00531-10341/NK29-CORR-00531-10750, Bruce Power Irradiated Fuel Bay Structural Integrity Analysis, Bruce Power Letter, F. Saunders to R. Lojk, March 26, 2013.

[92] NK21-CORR-00531-11721/NK29-CORR-00531-12110, Action Item 2014-07-5551: CNSC Type II Compliance Inspection Report: BRPD-AB-2014-012 – Probabilistic Safety Assessment, Bruce Power Letter, F. Saunders to K. Lafrenière, January 16, 2015.

[93] BP-PROC-00659-R02, Severe Accident Management, Bruce Power, February, 2014.

[94] NK21-REP-00701-09DEC2013-060, Summary of Bruce Power Fukushima Action Items for the 2014 Interim Periodic Safety Review, Bruce Power, December 11, 2013.

[95] BP-SAM-00001-R00, Technical Support Group User's Guide, Bruce Power, October 2009.

[96] BP-SAM-10003-R001, Bruce A – Diagnostic Flow Chart (DFC), Bruce Power, May, 2010.

[97] BP-SAM-10001-R00, Bruce A – SACRG-1: Initial Response, Bruce Power, June 21, 2010.

[98] BP-SAM-10002-R000, Bruce A – SACRG-2: Technical Support Group Functional, Bruce Power, June 2010.

[99] BP-SAM-10004-R001, Bruce A – Severe Challenge Status Tree, Bruce Power, May 2010.

[100] NK21-CORR-00531-10565/NK29-CORR-00531-10965, CNSC Review of Bruce Power's Irradiated Fuel Bay Structural Integrity Analysis (Fukushima Action Items 1.5.1, 1.6.1 and 1.6.2), CNSC Letter, R. Lojk to F. Saunders, June 3, 2013.

[101] NK21-REP-09051.1-00011-R00, Confidential – Bruce A Annual Reliability Report – 2013, Bruce Power, April 25, 2014.

[102] COG-13-9034-R0, Development of a Whole-Site PSA Methodology, CANDU Owners Group Report, February 2014.

[103] COG-JP-4499-001-R0 CANDU Whole-Site Probabilistic Safety Assessment Project Execution Plan, CANDU Owners Group Report, December 2014.

[104] NK21-CORR-00531-10364/NK29-CORR-00531-10776, Acceptance of Bruce Power Probabilistic Risk Assessment Common Cause Failure (CCF) Methodology, CNSC Letter, R. Lojk to F. Saunders, March 25, 2013.

[105] NK21-CORR-00531-08531/NK29-CORR-00531-09287, Bruce A & B Risk Assessment Action Plan – Computer Codes Documentation, CNSC Letter, K. Lafrenière to F. Saunders, February 28, 2011.

[106] NK21-CORR-00531-10877/NK29-CORR-00531-11258, Acceptance of Bruce Power Probabilistic Risk Assessment Computer Codes, CNSC Letter, K. Lafrenière to F. Saunders, October 29, 2013.

[107] NK21-CORR-00531-11043/NK29-CORR-00531-11439, Bruce Power Probabilistic Risk Assessment – Additional Computer Code Information, Bruce Power Letter, F. Saunders to K. Lafrenière, February 24, 2014.

[108] NK21-CORR-00531-11206/NK29-CORR-00531-11609, Acceptance of Bruce Power Probabilistic Risk Assessment Computer Code – WINDFAIL, CNSC Letter, K. Lafrenière to F. Saunders, March 19, 2014.

[109] NK21-CORR-00531-10451/NK29-CORR-00531-10851, Bruce Power Probabilistic Risk Assessment Computer Codes, Bruce Power Letter, F. Saunders to R. Lojk, July 9, 2013.

[110] NK21-CORR-00531-10877/NK29-CORR-00531-11258, Acceptance of Bruce Power Probabilistic Risk Assessment Computer Codes, CNSC Letter, R. Lojk to F. Saunders, October 29, 2013.

[111] COG-05-9011, Interim Implementation Guidelines for CANDU Nuclear Plant Reliability Programs, CANDU Owners Group, April 2006.

[112] NK21-CORR-00531-11181, Bruce Power Response to CNSC Review of the Bruce A Annual Reliability Report 2012, Bruce Power Letter, F. Saunders to K. Lafrenière, March 21, 2014.

[113] NK21-CORR-00531-11324/NK29-CORR-00531-11729, Submission of S-294 Probabilistic Risk Assessment Final Reports, Bruce Power Letter, F. Saunders to K. Lafrenière, July 31, 2014.

[114] B1538/005/000001, "RE: Bruce A and Bruce B Level 2 At-Power PRA Results Including Emergency Mitigating Equipment", November 20, 2014.

[115] NK21-CORR-00531-11017/NK29-CORR-00531-11413, Outage Probabilistic Risk Assessment (PRA) for Internal Fires, Seismic Events and Internal Floods, Bruce Power Letter, F. Saunders to R. Lojk, January 22, 2014.

[116] NK21-CORR-00531-11284/NK29-CORR-00531-11692, Outage Probabilistic Risk Assessment (PRA) for Internal Fires, Seismic Events and Internal Floods, CNSC Letter, K. Lafrenière, April 29, 2014.

[117] DPT-NSAS-00016, R000, Integrated Aging Management for Safety Assessment, Bruce Power, June 21, 2013.

[118] BP-PROG-15.01-R004, Nuclear Oversight Management, Bruce Power, December 18, 2013.

[119] NK21-CORR-00531-11710/NK29-CORR-00531-12099, Action Item 2014-07-5551: CNSC Type II Compliance Inspection Report: BRPD-AB-2014-012 – Probabilistic Safety Assessment Inspection, CNSC, 6 Nov 2014.

[120] CC171-11/2013E, CNSC Staff Integrated Safety Assessment of Canadian Nuclear Power Plants for 2013, ISSN 1926-1705, September 2014.

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

No codes or standards relevant to Safety Factor 6 were subjected to high-level assessment. This Appendix is retained only for consistency with the Appendix numbering scheme in all other Safety Factor Reports.

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 particular clause provides requirements that are less strenuous than clauses of another standard that has already been assessed;
- 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.

B.1. CNSC REGDOC-2.4.2, Probabilistic Safety Analysis

In support of the review tasks listed in Section 5, a detailed assessment of CNSC REGDOC-2.4.2 has been performed in Table B1.

Table B1: CNSC REGDOC-2.4.2, Probabilistic Safety Analysis

Article No.	Clause Requirement	Assessment	Compliance Category
4.1	Perform a level 1 and level 2 PSA for each NPP. Considerations shall include the reactor core and other radioactive sources such as the spent fuel pool (also called irradiated fuel bay). Multi-unit impacts, if applicable, shall be included. For radioactive sources outside the reactor core, the licensee may, with the agreement of persons authorized by the Commission, choose an alternate analysis method to conduct the assessment.	The Bruce A Probabilistic Risk Assessment (synonymous with Probabilistic Safety Assessment), 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 current Level 1 and Level 2 Bruce A PRAs are plant specific. They also take into consideration applicable multi-unit impacts (see assessment of Clause 4.3 for more details). The main results of the Level 1 PRAs are frequencies of core damage states that can result from various accident sequences. The core damage states are defined based on their severity, time of progression and other features using insight from deterministic analyses. The frequencies of most consequential core damage states are summed up to obtain the safety goal of severe core damage frequency (SCDF). Bruce Power has developed PRAs for at-power and outage plant states, with contributions from internal initiating events (IEs), from internal hazards and from external hazards. The Level 2 PRAs further develop accident sequences from the	C

Article No.	Clause Requirement	Assessment	Compliance Category
		Level 1 analyses, to obtain estimates of frequencies of radioactive releases outside of the reactor containment system. Release categories are defined based on their radioactive contents, duration and location of release, using deterministic analyses. The frequencies of specific release categories are summed up to obtain estimates of the two safety goals associated with Level 2 PRA: Large Release Frequency (LRF) and Small Release Frequency (SRF). The preparation of the Level 1 and Level 2 PRAs has been based on the Bruce Power PRA guides for specific plant states and types of initiating events considered. For example, the Level 1 and Level 2 At-Power Internal Events PRAs are prepared in accordance with the PRA guides B-REP-03611-00005 Ver1 and B-REP-03611-00010 Ver0, respectively. Safety assessment of the irradiated fuel bay has been conducted outside the scope of PRA, as documented in NK21-CORR-00531-10341 Ver. This analysis was reviewed by CNSC and found acceptable as per their response letter NK21-CORR-00531-10565 Ver. The set of current Bruce A PRAs and corresponding PRA Guides includes the following: 1a) Level 1 At-Power Internal Events PRA NK21-03611.1 P NSAS (E10) - B1401/RP/005 Ver01 1b) Level 1 At-Power Internal Events PRA Guide: B-REP-03611-00005 Ver1	

Article No.	Clause Requirement	Assessment	Compliance Category
		2a) Level 1 Outage Internal Events PRA NK21-03611.1 P NSAS (E1) - B1401-RP-003-R01 Ver 2b) Level 1 Outage Internal Events PRA Guide: B-REP-03611-00006 Ver00 3a) Level 2 At-Power Internal Events PRA: NK21-03611.5 P NSAS Ver1 3b) Level 2 At-Power Internal Events PRA Guide: B-REP-03611-00010 Ver0 4a) Level 2 Outage Internal Events PRA: B-03611.5 P NSAS Ver01 NK21-CORR-00531-11091/NK29-CORR-00531-11491 states that there is no need to complete a detailed Level 2 Outage Internal Events PRA, justifying this by the acceptably low SCDF from the Level 1 Outage Internal Events PRA and by a limited Level 2 Outage study. 5a) At-Power Internal Fire PRA: NK21-03611.1 P NSAS (E5) - K-410003-REPT-0036 Ver01 5b) Internal Fire PRA Guide: B-REP-03611-00008 Ver0	

Article No.	Clause Requirement	Assessment	Compliance Category
		6a) At-Power Internal Flood PRA: NK21-CORR-00531-10958 Ver 6b) Internal Flood PRA Guide: B-REP-03611-00007 Ver0 7a) At-Power Seismic PRA: K21-03611.5 P NSAS (E3) - K-410003-REPT-0073 Ver01 7b) Seismic PRA Guide: B-REP-03611-00009 Ver0 8a) At-Power High Wind PRA: NK21-03611.7 P NSAS (E8) B1401/RP/001 R01 Ver1 8b) High Wind PRA Guide: B-REP-03611-00012 Ver00 The PRA guides used for the preparation of the Bruce A PRAs have been accepted for use by CNSC, as documented in their letters NK21-CORR-00531-08908 Ver, NK21-CORR-00531-10191 Ver, NK21-CORR-00531-10193 Ver, NK21-CORR-00531-10638 Ver, NK21-CORR-00531-10212 Ver and NK21-CORR-00531-10263 Ver0. Note that the January 2014 submission to CNSC NK21-CORR-00531-11017 Ver provides justification why outage PRAs for internal fires, seismic events and internal floods do not need to be performed for S-294 compliance (whose clause 9 in Section 5.0 lays out the same requirement regarding at-power and shutdown states as the present clause of CNSCREGDOC-2.4.2). The CNSC	

Article No.	Clause Requirement	Assessment	Compliance Category
		has accepted the arguments in [NK21-CORR-00531-11017/NK29-CORR-00531-11413] to exclude internal fires, internal floods and seismic events from the scope of Bruce Power's outage PRA in NK21-CORR-00531-11284/NK29-CORR-00531-11692. Note also that PRAs have not been done for external flooding and other external hazards (except seismic and high wind). However, hazards assessments have been performed in NK21-CORR-00531-11324 Ver (Enclosure 7), NK21-CORR-00531-09809/NK29-CORR-00531-10287, NK21-CORR-00531-10848/NK29-CORR-00531-11226, B-03611.7 P NSAS, K-449958-REPT-0017-R01 for many external hazards, in accordance with the guide for screening and disposition of external hazards B-REP-03611-00011 Ver0. Several of the hazards were not screened out in the Phase 1 assessment and hence analyzed further in Phase 2 assessments, in particular in K-449958-REPT-0012 Ver02 and K-449958-REPT-0017 Ver01 for external flooding.	
4.2	Conduct the PSA under the management system or quality assurance program established in the licensing basis. Guidance: The CSA N286 management system requirements standard and CSA N286.7, Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants, are referenced in the licensing basis of operating nuclear power plants. The PSA should be developed in a manner that is consistent with the management system.	Bruce Power PRA is performed in accordance with the Quality Assurance (QA) process of Bruce Power and its subcontractors, AMEC/NSS (Nuclear Safety Solutions) and Kinectrics. In preparation of the PRA models, Bruce Power follows quality-related procedures DPT-NSAS-00001 Ver005, DPT-NSAS-00008 Ver004 and DPT-NSAS-00011 Ver003 to ensure quality, configuration management of software and data sets, and software qualification. The procedure DPT-NSAS-00001 Ver005 establishes the QA process for performing safety analysis work in support of nuclear safety assessment, with the intent to satisfy relevant requirements specified in CSA N286-05 Ver2007. The procedure DPT-NSAS-00008 Ver004 describes the process for performing work through an external contractor/consultant related to nuclear safety analysis, as required in Sections 6.1, 6.2, 6.3, 6.4, Annex A & Annex F of CSA N286-05 Ver2007. The procedure DPT-NSAS-00011 Ver003 establishes the configuration management process for safety analysis software, including PRA-related analysis, applications, scripts and utility codes. This procedure is intended to satisfy the requirements of CSA N286.7-99 Ver1999, in addition to the relevant requirements of CSA N286-05 Ver2007.	C

Article No.	Clause Requirement	Assessment	Compliance Category
		CNSC acknowledged in their letter NK21-CORR-00531-10877 Ver that CSA N286.7-99 Ver1999 or equivalent QA computer code requirements are being followed by Bruce Power. Bruce Power is cognizant of the fact that CSA N286-05 Ver2007 has been recently superseded by an expanded edition CSA N286-12 Ver2012. However, as explained in Section 3.4, CNSC staff have stated that "the new requirements in CSA N 286-12 Ver2012 are already addressed in Bruce Power's program and procedure documentation" NK21-CORR-00531-11494 Ver0. 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 Ver2007 version of the code to the CSA N286-12 Ver2012 version, during the next licensing period as specified in letter NK21-CORR-00531-11189 Ver0.	
4.3	The PSA models shall reflect the plant as built and operated (including multi-unit impacts), as closely as reasonably achievable within the limitations of PSA technology, and consistent with the risk impact.	The Bruce A PRA model (BAPRA) NK21-03611.1 P NSAS (E10) - B1401/RP/005 Ver01 adequately reflects specifics of the plant configuration and operation. The model assesses the risk of a representative unit (Unit 3), taking advantage of the similarity of units. The Bruce A systems' design, operation and testing is modelled in BAPRA using a set of system fault trees specific to Bruce A. The plant-specificity of the BAPRA model has been improving in the course of its multiple updates, carried out since its inception under the governance of DPT-RS-00007 Ver1, as summarized in Appendix F of the Level 1 Internal Events PRA NK21-03611.1 P NSAS (E10) - B1401/RP/005 Ver01. In particular, one integrated database was created by combining databases initially developed for the Level 1 At-Power, Level 2 At-Power and Level 1 Outage	AD

Article No.	Clause Requirement	Assessment	Compliance Category
		PRAs. Other updates included revisions of the component failure rates, addition of probability parameters for maintenance and testing outage events, conditioning events and developed events, and updates of the frequencies of initiating events (IEs). The updates of frequencies of initiating events (IEs) are done using Bayesian techniques whereby distributions of frequencies (extracted from generic industry-wide data) are updated by taking into account CANDU-specific and Bruce A-specific operating experience. This methodology is described in the Level 1 At-Power Internal Events PRA Guide B-REP-03611-00005 Ver1. Application of Bayesian techniques to updating component failure rates is described in the Level 1 At-Power PRA Guide B-REP-03611-00005 Ver1. It has not been fully implemented in the current BAPRA; this work is in progress per Action Request 28295222. The failure rate data update carried out in the 2011 version of BAPRA B0979/RP/001 Ver01 was limited to updating failure rates with generic industry data and did not include a Bayesian update with plant-specific evidence. In addition, Bruce Power has been improving quantification of key screening human interaction (HI) error values based on importance, and completed the qualification of the Bruce A MAAP4-CANDU parameter file for severe accident analysis. BAPRA also takes into account applicable multi-unit impacts. Examples of the latter include modelling of a forebay blockage event and of a large steam-line break in an adjacent unit, included in the Level 1 Internal Events PRA NK21-03611.1 P NSAS (E10) - B1401/RP/005 Ver01. Modeling of multiple unit accidents in the Level 2 Internal Event PRA NK21-03611.5 P NSAS Ver1 is approximated by scaling the common containment volumes by a factor of two or four, such that the containment pressure response	

Article No.	Clause Requirement	Assessment	Compliance Category
		reflects the relative rate of energy generation and absorption from failure of two or four units. Emergency Mitigating Equipment (EME), to be installed under the Fukushima Action Plan, has been modelled, which includes modifications of event trees, incorporation of EME-related fault trees, databases and human interaction events into the following Bruce A PRAs: Level 1 PRAs for At-Power and Outage Internal Events NK21-03611.1 P NSAS (E10) - B1401/RP/005 Ver01, NK21-03611.1 P NSAS (E1) - B1401-RP-003-R01 Ver, Level 2 At-Power Internal Events NK21-03611.5 P NSAS Ver1, and into the PRAs for Fire, Seismic and High Wind Hazards NK21-03611.1 P NSAS (E5) - K-410003-REPT-0036 Ver01, NK21-03611.5 P NSAS (E3) - K-410003-REPT-0073 Ver01, NK21-03611.7 P NSAS (E8) B1401/RP/001 R01 Ver1. The CNSC conducted an inspection NK29-CORR-00531-12099 of the Bruce Power Probabilistic Safety Assessment, whose specific focus was compliance of the Level 1 NK21-03611.1 P NSAS (E10) - B1401/RP/005 Ver01 and Level 2 NK21-03611.5 P NSAS Ver1 At-Power Internal Events PRAs with the requirements of CNSC S-294. The inspection found that Bruce Power followed CNSC accepted methodology on quantification of initiating events and in the event tree analysis. It was further found that Bruce Power has a process for making changes to the PRA models as required by the S-294 standard, that the uncertainty, sensitivity and importance analyses follow the accepted methodology, that the containment analysis in the Level 2 PRA and the interface between the Level 1 and Level 2 analyses are in agreement with the methodology, as are the definitions of the Plant Damage States (PDSs) and Release Categories (RCs). However, the inspection also found several shortcomings in the implementation of the PRA governance. Namely, it was pointed out	

Article No.	Clause Requirement	Assessment	Compliance Category
		that the updates of the fault tree analysis are not sufficiently traceable, and that some assumptions in FT models are not supported by the methodology, that quantification of human interaction (HI) events should be refined and should be applied consistently, and that the treatment of basic event reliability parameters do not fully reflect the plant as built and operated. As a result of these findings, 8 Action Notices and 11 Recommendations from the CNSC inspection were issued, as documented in the inspection report NK29-CORR-00531-12099. Also, Bruce Power has responded to the CNSC inspection and made a number of commitments to address the Action Notices and Recommendations - see NK21-CORR-00531-11721/NK29-CORR-00531-12110. These findings do not constitute a gap for the purposes of this review, because according to the definitions given in the CNSC Inspection Report, an Action Notice is "a written request that the licensee…take action to correct a non-compliance that is <u>not a direct contravention of the NSCA, the applicable regulations, licence conditions, codes or standards</u>, but that can compromise safety…and that may lead to a direct non-compliance if not corrected". Therefore, an acceptable deviation is assessed against this clause.	
4.4	Update the PSA models every five years. The models shall be updated sooner if the facility undergoes major changes. Guidance: Update the PSA models so that they adequately represent the as-operated plant conditions.	Current practice at Bruce Power is to continuously maintain the at-power BAPRA model throughout the year and issue a reference model and summary update document for PSA applications approximately once a year. This follows the procedure described in Section 4.4.2 of DPT-RS-00007, "Preparation and Maintenance of Probabilistic Risk Assessments". Update program, which began in 2004, has been implemented to ensure that the BAPRA model is representative of the actual plant configuration and operation and testing at the station. The development and implementation of the continuous PRA maintenance process constitutes a strength as it exceeds the regulatory requirement. 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 (E10) - B1401/RP/005 Ver01.	C

Article No.	Clause Requirement	Assessment	Compliance Category
		The continuous model development is now viewed as implementation of the concept of "Living PRA", as defined in DIV-ENG-00010 Ver000 and DPT-RS-00007 Ver1: "Living PRA is a PRA/unavailability model that is re-evaluated and updated periodically to reflect plant-specific design, operational and component reliability data changes. Design and operational changes to modeled systems requires revision of the specific PRA/unavailability models. Plant-specific nuclear power plant component reliability data is collected, evaluated and input back into the PRA based unavailability models on a frequent basis (i.e., typically yearly). The routine collection, evaluation and inputting of component reliability data ensures that the PRA/unavailability models are calculating risks/unavailabilities which are representative of changes in component reliability data over the life of the nuclear power plant." Bruce Power intends to continue to maintain and update BAPRA for consistency with NPP testing and configuration management, taking into account the currently pursued asset management initiative and associated with it risk-informed decision making practices	
4.5	Ensure the PSA models are developed using assumptions and data that are realistic and practical and, where required, supported by deterministic safety analysis or engineering assessments.	The original BAPRA model assumptions were made based on the best available plant information and the best judgment of plant engineers prior to the Bruce 3&4 restart (2002). As part of the existing BAPRA maintenance process and updates, summarized in Appendix F of the current Level 1 Internal Events PRA NK21-03611.1 P NSAS (E10) - B1401/RP/005 Ver01, these conservative elements are being replaced by more realistic assumptions as the assumptions are challenged through various plant risk applications. To achieve a realistic and up-to-date plant representation, the component failure database has been regularly revised in the course of BAPRA revisions and updates, incorporating relevant data sources and current testing and maintenance intervals.	C

Article No.	Clause Requirement	Assessment	Compliance Category
		The Bruce PRA Guide B-REP-03611-00005 Ver1 specifies that a realistic approach should be applied to probabilistic analysis, wherein realistic assumptions and data are used and unnecessary conservatism is avoided. Some conservatism may be acceptable where information is lacking or there is a high level of uncertainty, in order to avoid unjustifiable optimism, or where risk insights from sensitivity assessments indicate low impact on results. For determination of plant response and success criteria (both in event tree and fault tree analyses), especially for design basis accidents (DBAs), the existing BP PRAs rely on the conservative safety analyses that are described in the plant-specific Safety Reports. (The current version of the Bruce A Safety Report containing deterministic safety analysis is NK21-SR-01320-00003 Ver004.) However, when a system, structure or component (SSC) is identified as providing a specific mitigating function for a beyond design basis accident (BDBA), the conservative safety analysis should only be used if the assumptions in the safety analysis are not risk important. For risk important assumptions the supporting analysis should be made as realistic as possible. Examples of supporting analyses for PRA include the use of the MAAP-CANDU code in the Level 2 Internal Events PRA NK21-03611.5 P NSAS Ver1 to provide best estimate analysis for determining accident progression and timing. Bruce A PRAs have been supported by deterministic analysis, according to the systematic process defined in the Bruce PRA Guides. For example, the Level 1 At-Power Internal Events PRA Guide B-REP-03611-00005 Ver1 defines a systematic Process for Identifying Initiating Events for PSA, which calls for a review the deterministic safety analysis: "The deterministic accident analyses should be reviewed to ensure that all relevant initiating events have been identified in the PRA.	

Article No.	Clause Requirement	Assessment	Compliance Category
		Sources of information include the plant-specific Safety Report, as well as other safety analysis documentation" The initiating events selected in BAPRA are plant-specific, regularly updated, and based on realistic assumptions. The PRA Guide B-REP-03611-00005 Ver1 also provides for the use of expert judgement to support the preparation of a PRA when there is a lack of information or analytical methods for resolving a specific technical issue. For example, engineering judgement is used in the Level 1 Internal Events PRA NK21-03611.1 P NSAS (E10) - B1401/RP/005 Ver01, where subjective failure probabilities are assigned to undeveloped events present in the fault trees. Also, engineering assessment is part of defining the scope of and interfaces between different fault trees (by identifying failures that should be included in fault trees for different, and thus related, systems). Bruce Power performed the actions to verify key BAPRA assumptions, as committed to the CNSC in the Bruce Power letters NK21-CORR-00531-05517 Ver and NK21-CORR-00531-08069 Ver0. These verification actions addressed the CNSC's request to "review BAPRA assumptions and perform sensitivity studies to identify, validate and communicate the assumptions that have a significant impact on the risk posed by the plant operation."	
4.6	The level of detail of the PSA shall be consistent with the facility testing, maintenance and configuration management programs, and should be consistent with the intended uses of the PSA.	The current level of detail in BAPRA is consistent with Bruce A testing and configuration management for the operating Bruce A units. Bruce A PRAs are prepared under the general process described in the BP governing document DIV-ENG-00010 Ver000, which establishes the requirements for the use of PRA at BP nuclear facilities. Within this framework, department procedure DPT-RS-00007 Ver1 provides instructions for the preparation and maintenance of plant-specific PRAs, defines the process for	C

Article No.	Clause Requirement	Assessment	Compliance Category
		preparing a PRA as well as the systematic process of updating the PRA in order to maintain it as a "Living PRA". In particular, the regular updates of the BAPRA model incorporate accumulated significant changes stemming from design, operational, maintenance, analysis and PRA applications experience, as required to keep the PRA consistent with the as built and as operated state of the plant. The process of periodic risk reassessment in PRA, as defined in the procedure DPT-RS-00007 Ver1, is based on changes from significant operational events, or changes to engineering, operations, surveillance and maintenance, evaluations of risk outside the scope of the existing PRA, design changes and component reliability updates (based on the Annual Reliability Report NK21-REP-09051.1-00011 Ver000, issues from operating experience, etc. A full summary of updates of the BAPRA model is given in Appendix F of the current Level 1 Internal Events PRA NK21-03611.1 P NSAS (E10) - B1401/RP/005 Ver01. Bruce Power intends to continue to maintain and update BAPRA for consistency with NPP testing and configuration management, taking into account the currently pursued asset management initiative and associated with it risk-informed decision making practices.	
4.7	Seek CNSC acceptance of the methodology and computer codes to be used for the PSA before using them for the purposes of this document. Guidance: The methodology should be suitable to support the objectives of the PSA (set forth in section 3 of this document) and to support the intended PSA applications.	The current BAPRA models employ standard fault tree and event tree methodologies, implemented through the use of the Computer Assisted Fault Tree Analysis (CAFTA) software that is commonly used in nuclear industry for probabilistic risk modelling. Original version of BAPRA were based using the Windows Risk Spectrum code, and a full migration of the model to the CAFTA platform was completed in 2012, and subsequent model developments have been continued using CAFTA. Modular Accident Analysis Program MAAP4-CANDU is used to perform consequence analysis for severe accidents. Documentation on computer codes used in PRA (MAAP4-CANDU and CAFTA) has been completed, as described in the letter regarding Action Item 091411 NK21-CORR-00531-08069 Ver0.	C

Article No.	Clause Requirement	Assessment	Compliance Category
	Acceptance of the methodology prior to actual PSA development aims to help ensure the methodology can support the PSA's objectives. For example, the computer codes that support the analytical methods should be adequate for the purpose and scope of the analysis. Note: At the time of publication, the CNSC was reviewing the methodology for developing multi- unit PSA to evaluate the site integrated risk. The CNSC will establish the safety goals for site-wide PSA, which may consider: • interactions between the units, due to an initiating event (single-unit events and common-mode events), or as a result of the accident progression • aggregation of risk from internal events, internal hazards, and external hazards during all operating modes for all units at a site • radioactive sources other than the reactor cores (noting that alternate analysis methods may be used if accepted by the CNSC)	Bruce Power has obtained CNSC acceptance of the PRA methodologies described in the Level 1 Internal Events At-Power and Outage guides, B-REP-03611-00005 Ver1, B-REP-03611-00006 Ver00, respectively (acceptance document NK21-CORR-00531-08908 Ver), and in the Level 2 Internal Events At-Power Guide B-REP-03611-00010 Ver0 (acceptance document in NK21-CORR-00531-10191 Ver). In addition, acceptance has been received of the methodologies for External Hazards Screening B-REP-03611-00011 Ver0 (CNSC comments are documented in NK21-CORR-00531-10753 Ver0), for Fire PRA B-REP-03611-00008 Ver0 (acceptance document NK21-CORR-00531-10193 Ver), for Seismic PRA B-REP-03611-00009 Ver0 (acceptance document NK21-CORR-00531-10638 Ver), for Internal Flooding PRA B-REP-03611-00007 Ver0 (acceptance document NK21-CORR-00531-10212 Ver), and for High Wind Hazard PRA B-REP-03611-00012 Ver00 (acceptance document NK21-CORR-00531-10263 Ver0). CNSC acceptance of the computer codes used for BAPRA is documented in NK21-CORR-00531-08531 Ver and NK21-CORR-00531-10877 Ver. Bruce Power intends to update the governance document DIV-ENG-00010 Ver000 to reflect the newly issued suite of methodology guidance documents. Development of a whole-site PSA methodology for CANDU reactors is the subject of COG-JP-4499. Although Bruce Power considers simple aggregation of risk from internal events, internal hazards and external hazards as an inaccurate method to determine risk due to the potential for double counting in some areas, results of a simple addition of SCDFs and LRFs from the existing PRAs for internal and external events was reported in the July 2014 submission from BP to CNCS NK21-CORR-00531-11324 Ver. This estimate demonstrates that, when the PRA model credits recent and ongoing plant improvement (such as the installation of the Fukushima-related EME, automatic isolation of the Shield Tank Expansion line and containment enhancements), the risk aggregation results meet the single unit	

Article No.	Clause Requirement	Assessment	Compliance Category
		SCDF and LRF limits of 1.0E-4/yr and 1.0E-5/yr respectively. Safety assessment of the irradiated fuel bay (which is a source of radiation other than the reactor core) has been conducted outside the scope of PRA, as documented in NK21-CORR-00531-10341 Ver. This analysis was reviewed by CNSC and found acceptable NK21-CORR-00531-10565 Ver.	
4.8	Include all potential site-specific initiating events and potential hazards, namely: • internal initiating events and internal hazards • external hazards, both natural and human-induced, but non-malevolent Include potential combinations of the external hazards. The screening criteria of hazards shall be acceptable to the CNSC. The licensee may, with the agreement of “persons authorized” by the Commission, choose an alternate analysis method to conduct the assessment of internal hazards and external hazards. Guidance: Examples of external hazards are seismic hazards, external fires (e.g. fires affecting the site and originating from nearby forest fires), external floods, high winds, off-site transportation accidents, releases of toxic substances from off-site storage facilities, severe	The IEs included in these PRAs are plant-specific. Their selection and quantification was based on the procedure described in the Level 1 PRA Guides for the at-power and outage states, B-REP-03611-00005 Ver1 and B-REP-03611-00006 Ver00, respectively, and in the Level 2 Internal Events PRA Guide B-REP-03611-00010 Ver0. The Bruce A PRAs for internal hazards include: 1) At-Power Internal Fire PRA: NK21-03611.1 P NSAS (E5) - K-410003-REPT-0036 Ver01 2) At-Power Internal Flood PRA: NK29-03611.1 P NSAS (E6) - Attachment 4 K-410003-REPT-0012 Ver0 The PRAs for external hazards include: 1) At-Power Seismic PRA: NK21-03611.5 P NSAS (E3) - K-410003-REPT-0073 Ver01	C

Article No.	Clause Requirement	Assessment	Compliance Category
	weather conditions. Examples of internal hazards are internal fires, internal floods, turbine missiles, onsite transportation accidents, and releases of toxic substances from onsite storage facilities.	2) At-Power High Wind PRA: NK21-03611.7 P NSAS (E8) B1401/RP/001 R01 Ver1 The preparation of the Bruce hazard PRAs was based on the following PRA guides: 1) Internal Fire PRA Guide: B-REP-03611-00008 Ver0 2) Internal Flood PRA Guide: B-REP-03611-00007 Ver0 3) Seismic PRA Guide: B-REP-03611-00009 Ver0 4) High Wind PRA Guide: B-REP-03611-00012 Ver00 These guides have been accepted for use by CNSC, as documented in the letters NK21-CORR-00531-08908 Ver, NK21-CORR-00531-10191 Ver, NK21-CORR-00531-10193 Ver, NK21-CORR-00531-10638 Ver, NK21-CORR-00531-10212 Ver and NK21-CORR-00531-10263 Ver0. Note that The January 2014 submission to CNSC NK21-CORR-	

Article No.	Clause Requirement	Assessment	Compliance Category
		00531-11017 Ver provides justification why outage PRAs for internal fires, seismic events and internal floods do not need to be performed for S-294 compliance. Note also that PRAs have not been done for external flooding and other external hazards (except seismic and high wind). However, hazards assessments have been performed in B-03611.7 P NSAS (E7) - K-449958-REPT-0007 R03 Ver for many external hazards, including 23 airborne and extra-terrestrial hazards, 23 water-based hazards, and 24 ground-based hazards. This constituted Phase 1 of the hazards assessment, in accordance with the guide for screening and disposition of external hazards B-REP-03611-00011 Ver0 (note that this guide also includes a methodology applicable to internal hazards screening). The CNSC has accepted the arguments in NK21-CORR-00531-11017 to exclude internal fires, internal floods and seismic events from the scope of Bruce Power's outage PRA NK21-CORR-00531-11284. Hazards assessments have been performed in NK21-CORR-00531-11324 Ver (Enclosure 7), NK21-CORR-00531-09809/NK29-CORR-00531-10287, NK21-CORR-00531-10848/NK29-CORR-00531-11226, B-03611.7 P NSAS, K-449958-REPT-0017-R01 for many external hazards, in accordance with the guide for screening and disposition of external hazards B-REP-03611-00011 Ver0. Several of the hazards were not screened out in the Phase 1 assessment and hence analyzed further in Phase 2 assessments. These included the following Phase 2 hazard assessments: 1) High air temperature, Low air temperature and Turbine-generated missiles: all three addressed in Bruce Power External Hazards Assessment, Phase 2a, A05 - High Air Temperature, A09 - Low Air Temperature, G24 - Turbine-Generated Missiles, K-449958-REPT-0009 Ver02	

Article No.	Clause Requirement	Assessment	Compliance Category
		2) Lightning: addressed in Bruce Power External Hazards Assessment, Phase 2b - A08 Lightning, K-449958-REPT-0011 Ver0 3) Toxic gas/chemical release/radioactive release: addressed in Bruce Power External Hazard Assessment, Phase 2b - (A23) Toxic Gas/Chemical Release, K-449958-REPT-0011 Ver0 4) External Flooding, Other extraordinary waves, and Seiche: all three addressed in Bruce Power External Hazard Assessment, Phase 2c - (W03) External Flooding, K-449958-REPT-0012 Ver02 and K-449958-REPT-0017 Ver01, and Bruce Power External Hazard. Multiple combinations of the external hazards were considered in the Phase 1 and Phase 2 assessments; the justification of screening these combinations out are documented in Appendix A of the hazard assessment B-03611.7 P NSAS (E7) - K-449958-REPT-0007 R03 Ver. The preparation of the Bruce hazard assessments was done in accordance with the external hazards screening guide B-REP-03611-00011 Ver0. The CNSC responses to the submission of the external hazards screening guide are contained in the letter NK21-CORR-00531-10753 Ver0, which states, in particular, that the method for flood hazard assessment is acceptable.	
4.9	Include at-power and shutdown states. A PSA shall also be performed for other states where the reactor is expected to operate for extended periods of time and that are not covered by the at-power and shutdown PSAs.	Bruce A Level 1 Internal Events PRAs cover both at-power and shutdown (outage) states: NK21-03611.1 P NSAS (E10) - B1401/RP/005 Ver01 and NK21-03611.1 P NSAS (E1) - B1401-RP-003-R01 Ver, respectively.	C

Article No.	Clause Requirement	Assessment	Compliance Category
		These Level 1 models have been integrated with the Level 2 At-Power Internal Events PRA NK21-03611.5 P NSAS Ver1. Within the scope of Level 2 Internal Events Outage PRA, there exists a limited consequence assessment for a Unit Loss-of-Heat Sinks (ULHS) event and for a Small Loss-of-Coolant Accident (SLOCA) caused by ice plug failure on a low-elevation feeder, which was prepared using the methodology of the Level 2 At-Power Internal Events Guide B-REP-03611-00010 Ver0. The March 2014 submission to CNSC NK21-CORR-00531-11091 Ver explains the BP's position that there is no need to complete a detailed Level 2 Outage Internal Events PRA, justifying this by the acceptably low SCDF from the Level 1 Outage Internal Events PRA and by the results of the limited Level 2 Outage study B-03611.5 P NSAS Ver01. BP has issued the following hazards PRAs for at-power operation: 1) At-Power Internal Fire PRA: NK21-03611.1 P NSAS (E5) - K-410003-REPT-0036 Ver01 2) At-Power Internal Flood PRA: NK21-CORR-00531-10958 Ver 3) At-Power Seismic PRA: NK21-03611.5 P NSAS (E3) - K-410003-REPT-0073 Ver01 4) At-Power High Wind PRA: NK21-03611.7 P NSAS (E8) B1401/RP/001 R01 Ver1	

Article No.	Clause Requirement	Assessment	Compliance Category
		The January 2014 submission from BP to CNSC NK21-CORR-00531-11017 Ver provides justification why outage PRAs for internal fires, seismic events and internal floods do not need to be performed for S-294 compliance (whose clause 9 in Section 5.0 lays out the same requirement regarding at-power and shutdown states as the present clause of CNSC REGDOC-2.4.2). Hazards assessments have been performed in NK21-CORR-00531-11324 Ver (Enclosure 7), NK21-CORR-00531-09809/NK29-CORR-00531-10287, NK21-CORR-00531-10848/NK29-CORR-00531-11226, B-03611.7 P NSAS, K-449958-REPT-0017-R01 for many external hazards, in accordance with the guide for screening and disposition of external hazards B-REP-03611-00011 Ver0. The CNSC has accepted the arguments in NK21-CORR-00531-11017 to exclude internal fires, internal floods and seismic events from the scope of Bruce Power's outage PRA NK21-CORR-00531-11284.	
4.10	Include sensitivity analysis, uncertainty analysis and importance measures in the PSA.	The sensitivity analyses performed within the Level 1 BAPRA models NK21-03611.1 P NSAS (E10) - B1401/RP/005 Ver01 and NK21-03611.1 P NSAS (E1) - B1401-RP-003-R01 Ver assess the sensitivities of the selected modelling methods, model parameters, assumptions, approximations and simplifications that are likely to have a significant impact on the SCDF. The methodology for sensitivity analysis is specified in the Level 1 PRA Guides B-REP-03611-00005 Ver1 and B-REP-03611-00006 Ver00. Both at-power and outage Level 1 Bruce A PRAs include sensitivity analyses. Within the Level 1 At-Power PRA, the investigated model methodologies and assumptions included modelling of Common Cause Failures (CCFs) (a CCF Methodology for PRA has been issued NK21-CORR-00531-09019 Ver0, accepted by CNSC NK21-CORR-00531-10364 Ver0 and is implemented in BAPRA), Non-Occurrence of Gland Seal LOCA, Impact of ECI Header Pressurization and Impact of Crediting IBIF Heat Sink. Within the Level 1 Outage PRA, sensitivity analyses included parameter changes describing Event Tree Human interaction (HI)	C

Article No.	Clause Requirement	Assessment	Compliance Category
		dependencies, Moderator firewater addition, CCF events, etc. The sensitivity analyses performed within the Level 2 At-Power PRA NK21-03611.5 P NSAS Ver1 include two kinds of studies: effects of parameter changes on LRF, and effects of parameter changes on deterministic consequence modelling done by MAAP-CANDU. The Bruce A Level 1 and Level 2 PRAs (NK21-03611.1 P NSAS (E10) - B1401/RP/005 Ver01, NK21-03611.1 P NSAS (E1) - B1401-RP-003-R01 Ver and NK21-03611.5 P NSAS Ver1) include uncertainty analyses, where the Monte Carlo method was used to develop uncertainty distribution for the SCDF and LRF from the uncertainties associated with the basic events quantification. The resulting distributions of SCDF and LRF provide additional information about confidence with which the point estimates of these measures are known. (An uncertainty analysis was not performed for SRF since its point estimate is almost an order of magnitude below the Safety Goal limit.) The UNCERT utility of CAFTA software was used for the Monte-Carlo sampling. The Level 2 PRA NK21-03611.5 P NSAS Ver1 also includes a consequence uncertainty analysis, performed using MAAP-CANDU. Importance measures are used in the Level 1 and Level 2 BAPRA models to establish the significance of the events and systems in the fault trees in terms of their quantitative contribution to SCDF and LRF. Basic component failures and HI events were mapped to the corresponding systems, and lists of most important systems, components and HI events were created based on calculations of two standards importance measures: Fussell-Vesely (FV) and Risk-Worth Achievement (RAW).	

B.2. CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants

In support of the review tasks listed in Section 5 relevant clauses of REGDOC-2.5.2 have been assessed in Table B2. A more detailed assessment is performed in “Safety Factor 1 – Plant Design”.

Table B2: CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants

Article No.	Clause Requirement	Assessment	Compliance Category
4.2.2	Qualitative safety goals A limit is placed on the societal risks posed by NPP operation. For this purpose, the following two qualitative safety goals have been established: 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. 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. Quantitative application of the safety goals For practical application, quantitative safety goals have been established, so as to achieve the intent of the qualitative safety	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: - for the severe core damage frequency to be less than 10^{-4} per reactor year; - for the small release frequency to be less than 10^{-4} per reactor year; - for the large release frequency to be less than 10^{-5} per reactor year. 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 and in B1538/005/000001: Severe Core Damage Frequency (SCDF) for At-Power Internal Events:	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	goals. The three quantitative safety goals are: 1. core damage frequency 2. small release frequency 3. large release frequency 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. 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. Core damage frequency The sum of frequencies of all event sequences that can lead to significant core degradation shall be less than 10^{-5} per reactor year. Small release frequency The sum of frequencies of all event sequences that can lead to a release to the environment of more than 10^{15} becquerels of iodine-	3.82E-6 per reactor year (if Emergency Mitigating Equipment (EME) installed for Fukushima-related improvements are credited) or 2.07E-5 per reactor year (without crediting the Fukushima-related EME, as obtained in the Level 1 At-Power Internal Events PRA NK21-03611.1 P NSAS) SCDF for Outage Internal Events: 1.28E-5 per reactor year SCDF for Internal Flood: 5.5E-7 per reactor year (with the Fukushima-related EME credited) SCDF for Fire Hazard: 8.72E-6 per reactor year (with the Fukushima-related EME credited) SCDF for Seismic Hazard: 1.7E-6 per reactor year (crediting the Fukushima-related EME) SCDF for High Wind Hazard: 4.8E-6 per reactor year (crediting the Fukushima-related EME) Aggregated SCDF obtained by summation of the above SCDFs:	

Article No.	Clause Requirement	Assessment	Compliance Category
	131 shall be less than 10^{-5} per reactor year. A greater release may require temporary evacuation of the local population. Large release frequency The sum of frequencies of all event sequences that can lead to a release to the environment of more than 10^{14} becquerels of cesium-137 shall be less than 10^{-6} per reactor year. A greater release may require long term relocation of the local population Guidance 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 sufficiency low (i.e., less than the large release frequency limit). Calculations of the safety goals include all internal and external events as per REGDOC-2.4.2, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants. However, aggregation of internal event and other hazard risk metrics performed through simple addition to demonstrate that the risk metrics (core damage frequency, small release frequency and large release frequency) are not exceeded might not be appropriate. It is recognized that when	3.24E-5 per reactor year (with the Fukushima-related EME credited) Large Release Frequency (LRF) for At-Power Internal Events: 1.47E-6 per reactor year (if Emergency Mitigating Equipment (EME) installed for Fukushima-related improvements are credited, as reported in the document “RE: Bruce A and Bruce B Level 2 At-Power PRA Results Including Emergency Mitigating Equipment” B1538/005/000001, November 20, 2014) or 9.9E-6 per reactor year (without crediting the Fukushima-related EME, as obtained in the Level 1 At-Power Internal Events PRA NK21-03611.1 P NSAS) LRF for Fire Hazard: 7.32E-6 per reactor year (with the Fukushima-related EME credited) LRF for Seismic Hazard: 1.7E-6 per reactor year (with the Fukushima-related EME credited) LRF for High Wind Hazard: 4.8E-6 per reactor year (crediting the Fukushima-related EME)	

Article No.	Clause Requirement	Assessment	Compliance Category
	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. Further details on PSAs are contained in section 9.5 of this document and REGDOC-2.4.2, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants.	Aggregated LRF obtained by summation of the above LRFs: 1.53E-5 per reactor year (with the Fukushima-related EME credited) Small Release Frequency (SRF) for At-Power Internal Events: 1.47E-6 per reactor year (if Emergency Mitigating Equipment (EME) installed for Fukushima-related improvements are credited, as reported in the document “RE: Bruce A and Bruce B Level 2 At-Power PRA Results Including Emergency Mitigating Equipment” B1538/005/000001, November 20, 2014) 9.95E-6 per reactor year (without crediting the Fukushima-related EME, as obtained in the Level 1 At-Power Internal Events PRA NK21-03611.1 P NSAS) Gap 1 - Although the result of each separate PRA meets the safety goal limits set up for Bruce A PRAs, their aggregates obtained by respective summation of SCDFs, SRFs and LRFs and across all available PRA types, do not meet the more stringent quantitative safety goal targets set up in the requirement clause. Therefore, a gap is assessed against this clause.	
4.2.3	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. The safety analyses shall examine plant performance for:	The part of this clause regarding probabilistic safety assessment is covered in detail in the assessment of CNSC REGDOC-2.4.2	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	1. normal operation 2. AOOs 3. DBAs 4. BDBAs, including DECs (DECs could include severe accident conditions) 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. The safety analyses are discussed in further detail in section 9.0.		
5.6	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. 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.	The part of this clause regarding probabilistic safety assessment is covered in detail in the assessment of CNSC REGDOC-2.4.2	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	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. 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. 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. Guidance As per IAEA GSR Part 4, Safety Assessment for Facilities and Activities, aspects considered in the safety assessment should include: • 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, and use of operating experience • radiation risks		

Article No.	Clause Requirement	Assessment	Compliance Category
	• safety functions • site characteristics • radiation protection • engineering aspects • human factors • long-term safety The independent peer review should be performed by suitably qualified and experienced individuals. Additional information Additional information may be found in: • IAEA, GSR Part 4, Safety Assessment for Facilities and Activities, Vienna, 2009.		
7.4	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. 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.	The part of this clause regarding probabilistic safety assessment is covered in detail in the assessment of CNSC REGDOC-2.4.2	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	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. Guidance 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. 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. 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). 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. CNSC REGDOC-2.4.1, Deterministic Safety Analysis and CNSC		

Article No.	Clause Requirement	Assessment	Compliance Category
	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. For further information on the safety analysis for the identified PIEs, refer to section 9.0 of this document. Additional information Additional information may be found in: • CNSC, REGDOC-2.4.1, Deterministic Safety Analysis, Ottawa, Canada, 2014.		
7.6	All SSCs important to safety shall be designed with sufficient quality and reliability to meet the design limits. A reliability analysis shall be performed for each of these SSCs. Where possible, the design shall provide for testing to demonstrate that the reliability requirements will be met during operation. 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 10^{-3}. 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.	Bruce A uses the reliability program described in BP-PROG-11.01 and in the hierarchy of its implementing procedures (listed in Appendix B of BP-PROG-11.01). The implementing procedures deal with scoping and identification of Critical SSCs, continuing equipment reliability improvement, preventive maintenance implementation, performance monitoring, equipment reliability problem identification and resolution, long-term planning and life-cycle management. 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;	AD

Article No.	Clause Requirement	Assessment	Compliance Category
	Design for reliability shall take account of mission times for SSCs important to safety. 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. Guidance The design for reliability is based on meeting applicable regulatory requirements and industry standards. The design should provide assurance that the requirements of CNSC RD/GD-98, Reliability Programs for Nuclear Power Plants, will be met during operation. Not all SSCs important to safety identified in the design phase will necessarily be included in the reliability program. The following principles are applied for SSCs important to safety: • 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	for others, CANDU Owner's Group guidance COG-05-9011 is followed, where the applicable initiating events frequencies are used as system monitoring parameters. 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. 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 validating the modelling assumptions, updating the Class 3 unavailability model if required and optimizing the testing program to reduce the unavailability. 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.	

Article No.	Clause Requirement	Assessment	Compliance Category
	The reliability of SSCs assumed in the design stage needs to be realistic and achievable. Deterministic analysis or other methods may be used if the PSA lacks effective models or data to evaluate the reliability of SSCs.		
7.6.1	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. Guidance 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. Additional information Additional information may be found in: • United States Nuclear Regulatory Commission (U.S.	The part of this clause regarding probabilistic safety assessment is covered in detail in the assessment of CNSC REGDOC-2.4.2	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	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, Washington, D.C., 2007. • U.S. NRC, NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, Washington, D.C., 1994.		
8.4.2	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. Periodic testing of the systems and their components shall be scheduled at a frequency commensurate with applicable requirements. Guidance 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. The reliability of the shutdown function should be such that the cumulative frequency of failure to shutdown on demand is less than 10-5 failures per demand, and the contribution of all sequences involving failure to shutdown to the large release frequency of the	Only the Guidance portion of this clause is relevant to probabilistic safety analysis assessment (SF6). The Level 1 Internal Events At-Power 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 10^{-5} is demonstrated by the fuel damage category FDC1 in the Level 1 PSA. Gap 1 - 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 shut down is about 2.3E-7 occurrences per reactor per year. Accordingly, the proposed safety goal of 10^{-7}/yr is not met, which constitutes a gap with respect to the guidance portion of this clause.	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	safety goals is less than 10-7/yr. This considers the likelihood of the initiating event and recognizes that the two shutdown means may not be completely independent. 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.		
9.1	A safety analysis of the plant design shall include hazard analysis, deterministic safety analysis, and probabilistic safety assessment (PSA) techniques. The safety analysis shall demonstrate achievement of all levels of defence in depth, and confirm that the design is capable of meeting the applicable expectations, dose acceptance criteria and safety goals. 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. 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.	The requirements of this clause relevant to probabilistic safety analysis is covered in detail in the assessment of CNSC REGDOC-2.4.2	RNA
9.2	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.	The requirements of this clause relevant to probabilistic safety analysis is covered in detail in the assessment of CNSC REGDOC-2.4.2	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	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. The final safety analysis shall: 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 respond to identified PIEs 4. demonstrate the effectiveness of the safety systems and safety support systems 5. derive the OLCs for the plant, including: a. operational limits and set points important to safety b. allowable operating configurations, and constraints for operational procedures 6. establish requirements for emergency response and accident management		

Article No.	Clause Requirement	Assessment	Compliance Category
	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 8. demonstrate that the design incorporates sufficient safety margins 9. confirm that the dose and derived acceptance criteria are met for all AOOs and DBAs 10. demonstrate that all safety goals have been met Guidance 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.		
9.5	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. Additional information Additional information may be found in: • ASME/ANS, RA-Sa-2009, Standard for Level 1/Large	This clause is covered in detail in the assessment of CNSC REGDOC-2.4.2.	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	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 Hazards in Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 1995. • IAEA, Safety Report Series No.10, Treatment of Internal Fires in Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 1998.		