Periodic Safety Review - Final Document Review Traveler

Bruce Power Document #:	Revision:	Information Classification	Usage Classification
NK21-SFR-09701-00005	R000	Internal Use Only	Information

Bruce Power Document Title:
Safety Factor 5 – Deterministic Safety Analysis

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

Supplier's Name:	Supplier Document #:	Revision:
CANDESCO	K-421231-00015	R00

Supplier Document Title:
Safety Factor 5 – Deterministic 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 3

Bruce Power Document #:	NK21-SFR-09701-00005	Rev #: R000	Information Classification: Internal Use Only	Usage Classification: Information
Bruce Power Document Title:	Safety Factor 5 – Deterministic Safety Analysis	Suppliers Name:	CANDESCO	
Bruce Power Contract/ Purchase Order:	00193829	Supplier Document Title:	Safety Factor 5 – Deterministic Safety Analysis	
Bruce Power Project #:	38180	Supplier Document:	K-421231-00015	Rev #: R00

Reviewed By:

Name	Title	Department	Signature	Date
Ken Chuong	Sr. Technical Specialist	Nuclear Safety Analysis & Support		July 27, 2015
Joan Higgs	Technical Advisor, Engineering	Nuclear Safety Analysis & Support		JULY 27, 2015
Rob McLean	Sr. Technical Engineer	Nuclear Safety Analysis & Support		30 JUL 2015.
Neman Ali	Sr. Technical Engineer	Nuclear Safety Analysis & Support		July 28, 2015
Vlad Costiuc	Sr. Design Engineer	Nuclear Safety Analysis & Support		Jul 28, 2015
Patrick Ta	Sr. Technical Specialist	Nuclear Safety Analysis & Support	Patrick Ta	Jul 28, 2015
Hassan Albasha	Technical Advisor, Engineering	Nuclear Safety Analysis & Support		July 28, 2015

Recommended for Use By:

Name	Title	Department	Signature	Date
Phil Hunt	Division Manager	Reactor Safety Engineering	P. Hunt	Aug 12, 2015

Periodic Safety Review - Final Document Review Traveler

Sheet # 3 of 3

Bruce Power Document #:	NK21-SFR-09701-00005	Rev #: R000	**Information Classification:** Internal Use Only	**Usage Classification:** Information
Bruce Power Document Title:	Safety Factor 5 – Deterministic Safety Analysis	Suppliers Name:	CANDESCO	
Bruce Power Contract/ Purchase Order:	00193829	Supplier Document Title:	Safety Factor 5 – Deterministic Safety Analysis	
Bruce Power Project #:	38180	Supplier Document:	K-421231-00015	Rev #: R00

Reviewed By:

Name	Title	Department	Signature	Date
Susan Brissette	Dept. Manager	Management Systems	S Brissette	31 JUL 15

Recommended for Use By:

Name	Title	Department	Signature	Date
Susan Brissette	Dept. Manager	Management Systems	S Brissette	31 JUL 15

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**

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 5 - Deterministic Safety Analysis

File: K-421231-00015-R00

NK21-SFR-09701-00005

A Report Submitted to Bruce Power

July 10, 2015

Issue	Reason for Issue:				
R00D0	For first internal Candesco review				
	Author: A. Abdul-Razzak	Verifier:	Reviewer: G. Archinoff T. Kapaklili M. Gold	Approver:	Date: Nov 27, 2014
Issue R00D1	**Reason for Issue:** For harmonization, which incorporates internal Candesco review comments				
	Author: A. Abdul-Razzak	Verifier:	Reviewer: G. Archinoff T. Kapaklili	Approver:	Date: Jan 20, 2015
Issue R00D2	**Reason for Issue:** For final internal Candesco review				
	Author: A. Abdul-Razzak	Verifier:	Reviewer: G. Archinoff L. Watt	Approver:	Date: Feb 20, 2015
Issue R00D3	**Reason for Issue:** Issued to Bruce Power for review				
	Author: A. Abdul-Razzak	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:
A. Abdul-Razzak</td><td>Verifier:
G. Aldev</td><td>Reviewer:
G. Archinoff
L. Watt</td><td>Approver:</td><td>Date:
June 26, 2015</td></tr>
<tr><td rowspan="2">Issue
R00</td><td colspan="5">Reason for Issue:
For use</td></tr>
<tr><td>Author:
A. Abdul-Razzak</td><td>Verifier:
G. Aldev
C. Stallman</td><td>Reviewer:
G. Archinoff
L. Watt</td><td>Approver:
L. Watt</td><td>Date:
July 10, 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

AI	Action Item
AIM	Abnormal Incidents Manual
AOO	Anticipated Operational Occurrence
AOR	Analysis of Record
BEAU	Best Estimate Analysis and Uncertainty
BDBA	Beyond Design Basis Accident
BP	Bruce Power
CANDU	Canada Deuterium Uranium
CM	Configuration Management
CMF	Common Mode Failure
CNSC	Canadian Nuclear Safety Commission
COG	CANDU Owners Group
CSA	Canadian Standards Association
CSI	CANDU Safety Issue
DAC	Derived Acceptance Criteria
DBA	Design Basis Accident
DF	Dual Failure
DSA	Deterministic Safety Analysis
EA	Environmental Assessment
EFPD	Effective Full Power Days
EFPH	Equivalent Full Power Hours
F&FCI	Fuel and Fuel Channel Integrity
FE-FE Contact	Fuel Element – Fuel Element Contact
FFSG	Fitness for Service Guidelines
HT	Heat Transport
HTS	Heat Transport System
IAEA	International Atomic Energy Agency
ISR	Integrated Safety Review

IST	Industry Standard Toolset
ITP	Independent Technical Panel
IUC	Instrument Uncertainty Calculations
LCH	Licence Conditions Handbook
LCMP	Life Cycle Management Plan
LLOCA	Large Loss-of-Coolant Accident
LOCA	Loss-of-Coolant Accident
LOE	Limit of Operating Envelope
LOECI	Loss of Emergency Coolant Injection
LOF	Loss of Flow
LRF	Large Release Frequency
LTEP	Long Term Energy Plan
MCR	Major Component Replacement
NERP	Nuclear Emergency Response Plan
NPP	Nuclear Power Plant
NSA	Nuclear Safety Assessment
NSAS	Nuclear Safety Analysis and Support
NSASD	Nuclear Safety Analysis and Support Department
NSCA	Nuclear Safety and Control Act
OFI	Opportunities for Improvement
OLC	Operating Limits and Conditions
OP&Ps	Operating Policies and Principles
OPEX	Operating Experience
OPG	Ontario Power Generation
OSRs	Operational Safety Requirements
P&G	Principles and Guidelines
PIE	Postulated Initiating Event
PRA	Probabilistic Risk Assessment
PROL	Power Reactor Operating Licence
PSR	Periodic Safety Review
QA	Quality Assurance

RDS	Reference Data Sets
RIDM	Risk-Informed Decision Making
ROE	Realistic Operating Envelope
RRS	Reactor Regulating System
SAI	Safety Analysis Improvement
SAIRP	Safety Analysis Issue Review Panel
SAMG	Severe Accident Management Guidance
SAS	Safety Analysis Software
SBR	Safety Basis Report
SCA	Safety and Control Areas
SCDF	Severe Core Damage Frequency
SCR	Station Condition Records
SDS	Shutdown System
SF	Single Failure
SFR	Safety Factor Report
SLOCA	Small Loss-of-Coolant Accident
SME	Subject Matter Expert
SOE	Safe Operating Envelope
SR	Safety Report
SRI	Safety Report Improvement
SRU	Safety Report Update
SSCs	Structures, Systems, and Components
TBA	Technical Basis Assessment
TDF	Task Definition Form
V&V	Verification and Validation

1. Objective and Description

Bruce Power (BP), as an essential part of its operating strategy, is planning to continue operation of Units 3 and 4 as part of its contribution to the Long Term Energy Plan (LTEP) (http://www.energy.gov.on.ca/en/ltep/). Bruce Power has developed plant life integration management plans in support of operation to 247,000 Equivalent Full Power Hours (EFPH). A more intensive Asset Management program is under development, which includes a Major Component Replacement (MCR) approach to replace pressure tubes, feeders and steam generators, so that the units are maintained in a fit for service state over their lifetime. However, due to the unusually long outage and de-fuelled state during pressure tube replacement, there is an opportunity to conduct other work, and some component replacements that could not be done reasonably in a maintenance outage will be scheduled concurrently.

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

1.1. Objective

The overall objective of the Bruce A ISR is to conduct a review of Bruce A against modern codes and standards and international safety expectations and provide input to a practicable set of improvements to be conducted during the Major Component Replacement in Units 3 and 4, and during asset management activities to support ongoing operation of all four units, including U0A, that will enhance safety to support long term operation. The look-ahead period will be longer than that in the interim PSR performed for Units 1-8 [2]. It will cover a 10-year period, since there is an expectation that a PSR will be performed on approximately a 10-year cycle, given that all units are expected to be operated well into the future. Nuclear Safety is a primary consideration for Bruce Power and the management system must support the enhancement and improvement of safety culture and the achievement of high levels of safety, as well as reliable and economic performance.

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

The specific objective of the review of this Safety Factor is to determine to what extent the existing safety analysis remains valid when the following aspects have been taken into account: actual plant design; the actual condition of SSCs (Structures, Systems and Components) and their predicted state at the end of the period covered by the ISR; current deterministic methods; and current safety standards and knowledge. In addition, the review should also identify any gaps relating to the application of the defence-in-depth concept.

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. Review of the application of analytical methods, guidelines and computer codes used in the existing deterministic safety analysis and comparison with current standards and requirements;
2. Review of the current state of the deterministic safety analysis (original analysis and updated analysis) for the completeness of the set of postulated initiating events forming the design basis, with consideration given to feedback of operating experience from plants of a similar design, in Canada;
3. Evaluation of whether the assumptions made in performing the deterministic safety analysis remain valid given the actual condition of the plant;
4. Evaluation of whether the actual operational conditions of the plant meet the acceptance criteria for the design basis;
5. Evaluation of whether the assumptions used in the deterministic safety analysis are in accordance with current regulations and standards;
6. Review of the application of the concept of defence-in-depth;
7. Evaluation of whether appropriate deterministic methods have been used for development and validation of emergency operating procedures and the accident management program at the plant;
8. Evaluation of whether calculated radiation doses and releases of radioactive material in normal and accident conditions meet regulatory requirements and expectations; and
9. Analysis of the functional adequacy and reliability of systems and components, the impact on safety of internal and external events, equipment failures and human errors, the adequacy and effectiveness of engineering and administrative measures to prevent and mitigate accidents.

2. Methodology of Review

As discussed in the Bruce A ISR Basis Document [1], the methodology for an ISR should include making use of safety reviews that have already been performed for other reasons. Accordingly, the Bruce A ISR makes use of previous reviews that were conducted for the following purposes:

- Return to service of Bruce Units 3 and 4 (circa 2001) [7];
- Life extension of Bruce Units 1 and 2 (circa 2006) [8] [9];
- Proposed refurbishments of Bruce Units 3 and 4 (circa 2008) [10] [11] [12]; and
- Safety Basis Report (SBR) and 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 considered in the 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 ageing 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[2]. The edition dates referenced in the third column of the table are the modern versions used for comparison.

The following Licence conditions are applicable to deterministic safety analysis:

- Licence Condition 3.1 [16] states that, the licensee shall maintain a documented set of operating policies and principles. The operating policies and principles shall provide direction for operating the nuclear facility safely and shall, as a minimum, reflect a safety analysis that has been previously submitted to the Commission, or a person authorized by the Commission. Operating limits, as well as procedural and administrative limitations for safety systems and safety-related systems, shall be specified in the operating policies and principles. Operation in states not considered in, or bounded by the safety analysis is not permitted.

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

- Licence Condition 5.2 [16] states that, the licensee shall not make any change to the design of the facility, facility operation, equipment or procedure that would change the operational limits referred to in condition 3.1, or introduce hazards different in nature or greater in probability than those considered by the Final Safety Analysis Report and Probabilistic Safety Assessment, without the prior written consent of the Commission, or a person authorized by the Commission.
- Licence Condition 5.4 [16] states, the licensee shall ensure that design and analysis computer codes and software used to support the safe operation of the nuclear facility are in accordance with CSA standard N286.7: Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants.

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 RD-310	Safety Analysis for Nuclear Power Plants	CNSC REGDOC-2.4.1 [19]	CBC
CNSC RD-360	Life Extension of Nuclear Power Plants	CNSC RD-360 (2008) [4]	NR
CSA N286-05	Management System Requirements for Nuclear Power Plants	CSA N286-12 [20]	NR
CSA N286.7	Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants	CSA N286.7-99 (R2012) [21]	NR
CSA N290.13-05	Environmental Qualification of Equipment for CANDU Nuclear Power Plants	CSA N290.13-05 (R2010) [22]	NR
CSA N290.15-10	Requirements for the Safe Operating Envelope of Nuclear Power Plants	CSA N290.15-10 [23]	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 REGDOC-2.4.1: CNSC REGDOC-2.4.1 [19] sets out requirements and guidance for the preparation and presentation of a safety analysis that demonstrates the safety of a nuclear facility. The document is presented in two parts: Part I applies to nuclear power plants, and Part II addresses small reactor facilities. This document supersedes the following regulatory documents: CNSC RD-310, Safety Analysis for Nuclear Power Plants; GD-310, Guidance on Safety Analysis for Nuclear Power Plants; and CNSC RD-308, Deterministic Safety Assessment for Small Reactor Facilities. Table C-1 of the ISR Basis Document [1] calls for a code-to-code assessment of differences between CNSC REGDOC-2.4.1 [19] and CNSC RD-310, followed by a clause-by-clause assessment against only those CNSC REGDOC-2.4.1 clauses without corresponding equivalent CNSC RD-310 clauses. However, CNSC REGDOC-2.4.1 is the most relevant regulatory document to Safety Factor 5 and accordingly, a clause-by-clause review is performed 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 CNSC RD-360, Life Extension for Nuclear Power Plants, issued February 2008. Therefore, CNSC RD-360 [4] *de facto* continues to provide guidance on how this review should be conducted. However, CNSC 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 Document [1] calls for a code-to-code review against CSA N286-05. CNSC staff have stated that in their view the CSA N286-12 version of CSA N286 "does not represent a fundamental change to the current Bruce Power Management System" and have acknowledged that "the new requirements in CSA N286-12 are already addressed in Bruce Power's program and procedure documentation" [24].

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 [25]. This timeframe will facilitate the implementation of CSA 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 [26]. 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: The use of computer software for deterministic safety analysis makes CSA N286.7-99 (R2012) [21] relevant in that it provides quality assurance requirements for the design, development, maintenance, modification, and use of computer programs that are used in nuclear power plant applications. Some of the safety analyses in Part 3 of the Bruce A Safety Report were performed using legacy tools that predate 1999 and do not meet the requirement of CSA N286.7-99; however, all new analyses are performed with the Industry Standard Toolset (IST) that are qualified according to CSA N286.7-99 requirements. The Safety Analysis Improvement (SAI) task team of the Canadian Deuterium Uranium (CANDU) industry has established guidelines for performing Deterministic Safety Analysis (DSA) [27], for conduct of computer code validation [28], and for computer code accuracy assessment [29]. CSA N286.7-99 is in the current licence and accordingly no further assessment against its requirements is performed in this Safety Factor report.

CSA N290.13-05: CSA N290.13-05 [22] provides environmental qualification requirements for the design of CANDU Nuclear Power Plants (NPPs). It is of relevance to deterministic safety analysis, since assumed system credits in safety analysis are supported by environmental qualification. The safety analysis of Design Basis Accidents (DBAs) only credits equipment qualified to withstand the harsh environment resulting from such accidents. This standard that was used for the Bruce 1 and 2 ISR has not been revised and the standard is in the licence. Table C-1 of the ISR Basis Document [1] calls for the confirmation of validity of previous assessment. However, CSA N290.13-05 is currently listed in the licence, and thus no further assessment is required.

CSA N290.15-10: CSA N290.15 [23] is the first edition of the CSA standard for the 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 CANDU nuclear power plants is provided in Annex A to support the requirements. This standard addresses one of the main objectives of deterministic safety analysis to derive or confirm operational limits and conditions that are consistent with the design and safety requirements for the nuclear power plant. This standard will be introduced in the next Licence where Bruce Power is moving from Operating Polices and Principles (OP&Ps) towards the implementation of a Safe Operating Envelope (SOE) program, which will provide the comprehensive identification of all operating limits and conditions in compliance with the requirements of CSA N290.15. The initial SOE objectives were to comply with COG-02-901 [30], which predates CSA N290.15. However, the requirements of CSA N290.15 were considered in the development of the Bruce Power SOE program. The expectation is that Bruce Power will be compliant by September 2015 [31] with N290.15. The implementation and status update of the SOE program is further discussed in review task 4 of this Safety Factor report.

3.3. Regulatory Documents

In addition to those identified in the Bruce Power PROL [15] and 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 R-10	The Use of Two Shutdown Systems in Reactors	[32]	NR
CNSC R-77	Overpressure Protection Requirements for Primary Heat Transport Systems in CANDU Power Reactors Fitted with Two Shutdown Systems	[33]	CV
CNSC REGDOC-2.3.2	Accident Management Severe Accident Management Programs for Nuclear Reactors	[34]	CBC
CNSC REGDOC-2.5.2	Design of Reactor Facilities: Nuclear Power Plants	[35]	CBC
CNSC G-144 (2006)	Trip Parameter Acceptance Criteria for the Safety Analysis of CANDU Nuclear Power Plants	[36]	HL
CNSC G-149 (2000)	Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors	[37]	HL
Assessment type: Clause-by-Clause (CBC); Code-to-Code (CTC); High Level (HL); No Assessment Required (NR); Confirm Validity of Previous Assessments (CV)			

CNSC R-10: CNSC R-10 [32] provides requirements for the shutdown systems in reactors. Section 3 of this regulatory document identifies the design requirements for the use of two shutdown systems for reactors and thus is relevant to design. The CNSC has recently reviewed and reorganized its regulatory framework program in order to develop a more robust, manageable and up-to-date regulatory requirements framework. A key objective of the review was ensuring that CNSC regulatory requirements are well defined and supported by additional guidance, as necessary. CNSC staff has been working with the CSA Group to develop amendments to CSA N290.1 Requirements for the Shutdown Systems of CANDU Nuclear Plants to incorporate all necessary existing requirements currently available in R-10. With the publication of this standard, R-10 is no longer reflecting the current regulatory environment and as such during FY 2012-13 [38] it was identified that it is not necessary to maintain R-10 and it can be withdrawn and archived. Table C-1 of the ISR Basis Document [1] calls for the confirmation of validity of previous assessments of this code to be performed. However, since a clause-by-clause assessment of the latest edition (i.e., 2013) of CSA N290.1 standard is performed and documented in Safety Factor 1, review against CNSC R-10 is not necessary.

CNSC R-77: CNSC R-77 [33] provides overpressure protection requirements for primary heat transport systems in CANDU power reactors fitted with two shutdown systems. This regulatory document provides analysis rules that are used to judge the acceptability of design features, and thus is relevant to deterministic safety analysis. R-77 was issued in 1987 and was reviewed for the Bruce 1 and 2 ISR in 2006, where it was demonstrated that Bruce A design fully meets the requirements and these results remain applicable.

CNSC REGDOC-2.3.2: CNSC REGDOC-2.3.2 [34] sets out the expectations and guidance of the CNSC with respect to severe accident management programs. Relevant clauses to Safety Factor 5 are reviewed in Appendix B (B.3), while a more detailed assessment is performed in “Safety Factor 13: Emergency Planning”.

CNSC REGDOC-2.5.2: Table C-1 of the ISR Basis Document [1] calls for a code-to-code assessment of 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 CNSC RD-337 clauses. It was instead decided to do a clause-by-clause assessment against all clauses of CNSC REGDOC-2.5.2. Relevant clauses to Safety Factor 5 are assessed in Appendix B (B.2), while a more detailed assessment is performed in “Safety Factor 1: Plant Design”.

CNSC G-144: CNSC G-144 [36] provides trip parameter acceptance criteria for the safety analysis of CANDU NPPs. A high-level review of this guidance document is provided in Appendix A (A.1).

CNSC G-149: CNSC G-149 [37] provides requirements for computer programs used in design and safety analysis of NPPs and research reactors. A high-level review of this guidance document is given in Appendix A (A.2).

3.4. CSA Standards

Additional CSA standards which are considered for application to review tasks of this Safety Factor are included in Table 3. These CSA standards are identical to those identified in Table C-1 of the ISR Basis Document [1].

Table 3: CSA Standards

Document Number	Document Title	Reference	Type of Review
CSA N288.2-M91	Guidelines for Calculating Radiation Doses to the Public from a Release under Airborne Radioactive Material Under Hypothetical Accident Conditions in Nuclear Reactors	[39]	NR
CSA N290.1-13	Requirements for Shutdown Systems of CANDU Nuclear Power Plants	[40]	CBC
CSA N290.4-11	Requirements for Reactor Control Systems of Nuclear Power Plants	[41]	CV
CSA N290.5-06 (R2011)	Requirements for Electrical Power and Instrument Air Systems of CANDU Nuclear Power Plants	[42]	CV
CSA N290.6-09 (R2014)	Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of an Accident	[43]	CV
Assessment type: Clause-by-Clause (CBC); Code-to-Code (CTC); High Level (HL); No Assessment Required (NR); Confirm Validity of Previous Assessments (CV)			

CSA N288.2-M91: CSA N288.2-91 [39] provides guidelines for calculating radiation doses to the public from a release of airborne radioactive material under hypothetical accident conditions in nuclear reactors. Table C-1 of the ISR Basis Document [1] calls for the confirmation of validity of the previous assessment. This is a 1991 standard so is not “modern”. It was superseded after the code effective date for this ISR. Dose calculations are known to be generally consistent with the intent of this standard. For these reasons, no detailed assessment against this standard is performed.

CSA N290.1-13: CSA N290.1-M80 was reviewed during the 2001 ISR. This standard was revised in 2013 [40]. Table C-1 of the ISR Basis Document [1] calls for a code-to-code assessment of differences between the 1980 version and 2013 version of CSA N290.1 followed by a clause-by-clause assessment against only those CSA N290.1-13 clauses without corresponding equivalent CSA N290.1-80 clauses. It was decided to instead do a clause-by-clause assessment against all clauses of CSA N290.1-13 with relevance to this Safety Factor. The relevant clauses of this new revision to Safety Factor 5 are assessed in Appendix B (B.4), while the assessment for all clauses is performed in “Safety Factor 1: Plant Design”.

CSA N290.4-11: CSA N290.4-11 [41] was reviewed clause-by-clause during the 2013 interim PSR where no gaps were identified. There have been no revisions or updates to the standard and no change in the BP programmatic aspects or the design of the control systems that would impact this recent assessment. Accordingly, the clause-by-clause assessment for CSA N290.4-11 during the 2013 interim PSR remains applicable.

CSA N290.5-06: CSA N290.5-06 (R2011) [42] covers the design, procurement, qualification, construction, installation, inspection, and documentation of CANDU NPP electrical power and instrument air systems. This standard was reviewed clause-by-clause in the 2013 interim PSR. This assessment did not identify any gaps. There have been no revisions or updates to the standard and no change in the Bruce Power programmatic aspects or the design of the electrical power and instrument air systems that would impact this recent assessment. Accordingly, the clause-by-clause assessment for CSA N290.5 performed in the 2013 interim PSR remains applicable.

CSA N290.6-09: CSA N290.6-09 (R2014) [43] provides requirements for the design, testing, installation, and qualification of equipment for the display of NPP safety functions in the event of an accident. A code-by-code comparison of the 1982 and 2009 edition was conducted in the 2013 interim PSR. This assessment did not identify any gaps. There have been no revisions or updates to the standard and no change in the Bruce Power programmatic aspects or the design of the equipment for the display of the plant safety functions that would impact this recent assessment. Accordingly, the assessment for CSA N290.6 during the 2013 interim PSR remains applicable.

3.5. International Standards

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, deterministic safety analysis falls under the broader function of Nuclear Safety Assessment (NSA), which also covers activities such as probabilistic safety assessment and criticality safety assessment. The Nuclear Safety Assessment function, together with the Design Management Function, falls under Bruce Power's BP-PROG-10.01 Plant Design Basis Management Program [44]. Nuclear safety is addressed at the highest level of the hierarchy in the Management System Manual [45], which presents a road map that defines how all of Bruce Power business aspects fit together in an integrated manner. This high level manual governs the Plant Design Basis Management program [44] with objectives and principles specified as:

- Define, document, and control changes to the Design Basis to maintain the Design Basis within approved safety margins and regulatory requirements.
- Perform such Safety Analysis as is required to ensure that plant operation conforms to the Design Basis and licensing assumptions, and remains within the bounds of analyzed conditions encompassed by the SOE.

The Plant Design Basis Management program [44] is implemented through the following procedures:

- BP-PROC-00363 on Nuclear Safety Assessment [46];
- BP-PROC-00335 on Design Management [47].
- DIV-ENG-00009, Design Authority [48];
- BP-PROC-00582, Engineering Fundamentals [49]; and
- BP-PROC-00502, Resolution of Differing Professional Opinions [50].

The Nuclear Safety Assessment procedure, documented in BP-PROC-00363, defines the elements, functional requirements, implementing procedures and key responsibilities associated with the NSA process. The objective of NSA is to ensure that all necessary nuclear safety requirements are defined for the actual or proposed design of the plant throughout the design modification process or in addressing emergent issues (e.g., plant ageing) that may affect the Design Basis or the Safety Report Basis.

The Management System Manual [45] assigns responsibility for the Plant Design Basis Management Program [44] to the Engineering Division. The Design Authority Procedure [48] in turn, delegates the responsibility for the implementation and execution of the Nuclear Safety Assessment Procedure (BP-PROC-00363) [46] to the Nuclear Safety Analysis and Support (NSAS) Department. The organization of the Reactor Safety Engineering Division, and specific accountabilities of the NSAS Department, are described within the approved reference chart authorities and responsibilities manual [51].

Within NSAS, the implementation of BP-PROC-00363 [46] on Nuclear Safety Assessment is supported by a variety of divisional and departmental procedures. Key amongst these is DPT-NSAS-00015 [52] on the Execution of Safety Analysis, which interfaces with the following related procedures:

- DIV-ENG-00012 [53], which defines the processes that will initiate Nuclear Safety Assessment (NSA) and the processes for review of NSA;
- DIV-ENG-00013 [54], which establishes the Quality Assurance (QA) process for planning internal work related to nuclear safety analyses;
- DPT-NSAS-00008 [55], which describes the process for performing work through an external contractor/consultant related to nuclear safety analysis and component fitness for service;
- DPT-NSAS-00011 [56], which establishes the Configuration Management (CM) process for Safety Analysis Software (SAS);
- DPT-NSAS-00012 [57], which describes the process, roles and responsibilities of associated personnel for the preparation and revision of Operational Safety Requirements (OSRs), which document those aspects of the SOE that are derived from or confirmed by the nuclear safety analysis;

- DPT-NSAS-00013 [58], which describes the process for preparing, maintaining and using Reference Data Sets (RDS) that are used with Safety Analysis Software;
- DPT-NSAS-00016 [59], which 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;
- DPT-NSAS-00007 [60], which describes the process to be followed in processing reports made pursuant to CNSC S-99[3], Section 6.3.2.3 when safety issues are discovered by the staff of NSAS;
- DPT-NSAS-00002 [61], which describes the overall process, and the responsibilities of associated personnel, for the Safety Report analysis update. It is supported by:
    - DPT-NSAS-00003 [62], which describes the process and the responsibilities of associated personnel for the step pertaining to the evaluation and prioritization of Safety Report analysis issues.
- DPT-RS-00015 [63], which provides guidance on how to assess whether station design, operation and maintenance are in compliance with the requirements imposed by the licensing safety analysis as documented in the OSRs and supporting Instrument Uncertainty Calculations (IUC) and outlines the roles and responsibilities associated with sustaining SOE compliance.

This whole system of procedures is supported and integrated through DPT-NSAS-00001 on the Quality Assurance of Nuclear Safety Assessment [64].

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

[3]Reporting is performed under S-99 up to the end of 2014, and under CNSC REGDOC-3.1.1 for periods thereafter.

[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.

Table 5: Key Implementing Documents

First Tier Documents	Second Tier Documents	Third Tier Documents	Fourth Tier Documents	Fifth Tier Documents
BP-MSM-1: Management System Manual [45]	BP-PROG-10.01: Plant Design Basis Management [44]	DIV-ENG-00009: Design Authority [48]		
		BP-PROC-00335: Design Management [47]		
		BP-PROC-00363: Nuclear Safety Assessment [46]	DIV-ENG-00012: Nuclear Safety Assessment and Review [53]	
			DIV-ENG-00013: Planning of Internal Work for Nuclear Safety Analysis [54]	
			DPT-NSAS-00015: Planning and Execution of Nuclear Safety Assessments [52]	
			DPT-NSAS-00007: Processing of S-99 Reportable Conditions Arising from Safety Analysis [60]	
			DPT-NSAS-00008: Management of External Work for Nuclear Safety Analysis and Support [55]	

First Tier Documents	Second Tier Documents	Third Tier Documents	Fourth Tier Documents	Fifth Tier Documents
			DPT-NSAS-00011: Configuration Management of Safety Analysis Software [56]	
			DPT-NSAS-00012: Preparation and Maintenance of Operational Safety Requirements [57]	
			DPT-NSAS-00013: Guidelines for Managing Reference Data Sets [58]	
			DPT-NSAS-00016: Integrated Ageing Management for Safety Assessment [59]	
			DPT-NSAS-00002: Safety Report Analysis Update Process Overview [61]	DPT-NSAS-00003: Guidelines for Evaluating and Prioritizing Safety Report Issues [62]
			DPT-RS-00015: Safe Operating Envelope Gap Assessment [63]	
			DPT-NSAS-00001: Quality Assurance of Nuclear Safety Assessment [64]	

Given that the Bruce A Safety Report is referenced in the plant's Operating Licence, the Safety Report is implicitly part of the outcome of the programs and procedures above.

Note that the listed governance programs and procedures were also used in the Bruce 3 and 4 ISR; however, they have been recently revised to consider CNSC RD-310 requirements (recently superseded by CNSC REGDOC-2.4.1) in preparation for CNSC REGDOC-2.4.1 implementation within the Safety Report Improvement (SRI) program.

5. Results of Review Tasks

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 been changed from those listed in Section 1.2.

5.1. Review of Analysis Methods and Computer Codes and Comparison with Current Standards and Requirements

This review task includes the review of the application of analytical methods, guidelines and computer codes used in the existing deterministic safety analysis and comparison with current standards and requirements.

CNSC REGDOC-2.4.1 [19], which supersedes CNSC RD-310, sets out requirements and guidance for the preparation and presentation of a safety analysis that demonstrates the safety of a nuclear facility. A clause-by-clause assessment against this standard was performed for this ISR and is documented in Appendix B (B.1). Of particular relevance to this review task are the clauses under 4.4.2 Method for deterministic safety analysis, 4.4.5 Computer Codes, and 4.4.6 Conservatism in deterministic safety analysis.

Part 3 of the Safety Report includes analysis originally performed at Ontario Hydro/Ontario Power Generation (OPG) using older procedures and computer codes. All newer analyses that have been included in the current Safety Reports and/or the Analysis of Record (AOR) since the implementation of improved analysis procedures are in compliance with quality assurance requirements of CSA N286.7-99 [21]. The continuous improvement in the safety analysis procedures is evident by further modification to the analysis procedures currently being implemented to introduce CNSC REGDOC-2.4.1 requirements, in preparation for phasing in CNSC REGDOC-2.4.1 implementation in the SRI program. New safety analysis (discussed in Section 5.3), at projected aged core conditions corresponding to 2019, has been performed for the main events impacted by ageing to meet REGDOC-2.4.1 requirements.

Bruce Power CNSC REGDOC-2.4.1 implementation and SRI activities are being tracked under Action Item 090739 [65]. The SRI program was initiated in 2010 to address Safety Report (SR) concerns identified by the CNSC, after their review of the Bruce 1 and 2 ISR as outlined in [66] and [67]. CNSC concerns were focused on the following four main areas:

- Validated tools to perform safety analysis;
- Consistency and conservatism in analysis methodologies and assumptions;

- Treatment and specification of uncertainties; and
- General compliance with CSA N286.7-99 QA Standards.

In addressing CNSC concerns, several activities have been completed by the industry Safety Analysis Improvement (SAI) task team. This includes completion of the development of an Industry Deterministic Safety Analysis Principles and Guidelines (P&G) document [27], the development of the Limit of Operating Envelope/Realistic Operating Envelope (LOE/ROE) guidelines (COG-11-9023) [68] and establishment of guidelines for the conduct of code validation [28] and computer code accuracy assessments [29]. Consistent with CNSC REGDOC-2.4.1 requirements, the P&G for DSA [27] recommends the methodologies to be used in the analysis of the various event classes. Level 2 defence-in-depth for the Anticipated Operational Occurrences (AOOs) and Level 4 defence-in-depth for the Beyond Design Basis Accidents (BDBAs) are to be analyzed with the ROE methodology, which has been incorporated in the latest revision (Rev 1) of COG-11-9023 [68]. DBAs are to be analyzed more conservatively using the LOE methodology or alternatively using the Best Estimate Analysis and Uncertainty (BEAU) methodology [69]. CNSC REGDOC 2.4.1 Clause 4.4.2 requires performing sensitivity analysis and identifying, where necessary, margins to cliff-edge effects. Cliff edge-effects are inherently covered in the assessment of trip coverage; however, they are not consistently addressed for quantitative acceptance criteria beyond reactor trip. Conservative assumptions are used in the analysis presented in Part 3 of the Safety Report. However, there is no demonstration that the conservatism of the analysis would cover modeling uncertainties.

Recently, the CNSC closed Action Item 110701 “CANDU Safety Issue AA3 – Computer Codes and Plant Model Validation – TUF Validation Work” [70] based on Bruce Power's request [71] after CNSC staff was satisfied with the action plan for the TUF validation basis and meeting the closure criteria for the action item. Bruce Power also provided the CNSC with a post closure update [72] on Bruce Power progress and activities related to TUF validation, which identified the completion of the following two actions that were targeted for Q2 of 2014:

- Conceptual Model Assessment - Documentation of work previously completed under Integrated Implementation Plan (IIP) Verification and Validation (V&V) Project; and
- TUF Accuracy Document where TUF accuracy values for key safety related parameters and their basis are identified [73].

Three gaps relevant to this review task are identified as follows:

- The Safety Report includes old analyses using computer codes that are not qualified to current safety standards;
- There is no demonstration that the conservatism of the analysis would cover modeling uncertainties; and
- Cliff edge-effects are not consistently addressed for quantitative acceptance criteria beyond reactor trip.

These gaps are listed as SF5-1, SF5-9 and SF5-10, respectively, in Table 8.

5.2. Review of Current State of Deterministic Safety Analysis for Completeness

This review task includes a review of the current state of the deterministic safety analysis (original analysis and updated analysis) for completeness of the set of postulated initiating events forming the design basis, with consideration given to feedback of operating experience from plants of a similar design in Canada.

Requirement 4.2.1 of CNSC REGDOC-2.4.1 [19] prescribes the use of a systematic process to identify events that can potentially challenge the safety or control functions of the NPP. This process shall be based on regulatory requirements and guidance, past licensing precedents, operational experience, engineering judgment, results of deterministic and probabilistic assessments, and any other systematic reviews of the design. It also requires that the identification of events shall account for all operating modes including normal operation.

Similarly, Requirement 9.1 of CNSC REGDOC-2.5.2 [35] specifies that: "…the first step of each part of the safety analysis shall be to systematically identify postulated initiating events. This shall be done in a systematic manner such as that defined by the failure modes and effects analysis methodology. Postulated Initiating Event (PIE) identification shall consider both direct and indirect events".

These requirements are more appropriate for a new plant design than for an older plant like Bruce A. When the conceptual design for a new plant is first produced and there is not sufficient detail to undertake a Probabilistic Risk Assessment (PRA), a systematic method needs to be adopted to determine what PIEs need to be considered. This was done for example for Darlington NGS and when the Darlington PRA was available it was used to confirm that the list of PIEs was complete.

In subsequent years, an extensive analysis program was undertaken by Ontario Hydro, the owner of Bruce A and B, to update the Safety Reports of its other CANDU plants, since the methods used in the analyses and the extent of sequences had changed since their original Safety Reports were written. The ground rules used in those updated analyses were that the sequences considered and the methods presented in the Darlington Safety Report be used on all of the older plants. The only difference in these older Safety Report updates was that the results of these new analyses be reported against the Siting Guide [74] rather than newer regulatory guidance, since the former was used as the basis for their licensing.

Section 2.1 of Part 3 of the Safety Report consequently addresses the identification of initiating events and states that all systems and components are reviewed to identify those containing significant quantities of radioactive materials. For each source of radioactive material, it is possible to determine ways in which unplanned release of this material can occur, based on the knowledge of the plant processes and past experience in selecting initiating events. This process leads to a comprehensive list of internal initiating events. To complete the list of abnormal events, all combinations of initiating events and compounding failures in the special safety systems and other mitigating systems are identified. This process is based on the knowledge of the plant processes and past experience in selecting initiating events.

The main Bruce Power database "SCR Viewer" is an Operating Experience (OPEX) database where Bruce Power Station Condition Records (SCRs) are generated and stored. The database is also recognized to be one of the main sources to be used in confirming the comprehensiveness and completeness of a systematic event identification process to be used in the implementation of SRI plan [73]. The CANDU Owners Group (COG) database is also available to Bruce Power and other nuclear industry utilities associated with COG. These databases are regularly assessed to confirm that any new relevant occurrence is covered in the Safety Report and PRA. Requirement 4.2.2 of CNSC REGDOC-2.4.1 [19] states that the list of events identified for the safety analysis shall include all credible:

- Component and system failures or malfunctions;
- Operator errors; and
- Common cause internally and externally initiated events.

The list of PIEs provided in Table 2.1 of Part 3 of the Safety Report [75] addresses mainly component and system failures or malfunctions. Although some of these events on the list may be attributable to operator errors, this category of PIEs has not been explicitly identified. Also, natural common cause events are not analyzed in the Safety Report.

The scope and identification of PIEs, as prescribed in Sections 4.2.1 and 4.2.2 of CNSC REGDOC-2.4.1 [19] and their classification, as prescribed in Section 4.2.3, are interdependent and cannot be dealt with in isolation. These considerations are therefore part of the updated CNSC RD-310 implementation plan and now identified as the CNSC REGDOC-2.4.1 implementation plan. The updated Bruce Power CNSC REGDOC-2.4.1 implementation plan is integrated with the Safety Report Improvement program [73]. One of the early activities of the CNSC REGDOC-2.4.1 implementation plan is identification and classification of the various events. This will be performed based on the guidance provided in the industry P&G for DSA [27] and the lessons learned during prototype applications. The main issue with the current Part 3 of the Safety Report is that the comprehensiveness of the considered events is not demonstrated by a systematic process as required by CNSC REGDOC-2.4.1.

Although AOOs are considered within the analyzed events, they are not currently classified or analyzed as such in the Safety Report. CNSC REGDOC-2.4.1 establishes new expectations for the analysis of AOOs, which can impact on scope and methodology of analyses incorporated in the Safety Report. Industry prototype applications, including the Bruce Power Loss of Flow (LOF) application [76], addressed in particular the treatment of AOOs following the recommended applicable roles for Level 2 and 3 defence-in-depth, as recommended by the industry P&G for DSA [27]. The lessons learned from these exercises will be utilized in performing the analysis of AOOs for the various event categories during the CNSC REGDOC-2.4.1 implementation phase as outlined in the SRI plan [73].

The gap for this review task is listed as SF5-2 in Table 8, and is related to the scope and process of event identification and classification. The sources of the gap were identified as a result of the assessment against the requirements and guidance of the modern codes CNSC REGDOC-2.4.1 and CNSC REGDOC-2.5.2. The use of a systematic approach for the event identification and classification is one of the earliest activities of the SRI plan [73].

5.3. Evaluation of Existing Safety Analysis and Validity of Assumptions Given Actual Condition of Plant

This review task evaluates whether the assumptions made in performing the deterministic safety analysis remain valid given the actual condition of the plant. This review task is extended to cover the current status of Category 3 CANDU Safety Issues (CSIs) and Safety Report Improvement program.

The compilation of deterministic safety analysis for Bruce A consists of the accident analyses contained in the SR and, more generally, the AOR, which are submitted to the CNSC in support of safe operation and the operating licence. The Safety Report currently consists of:

- Part 1: Plant and Site Description (NK21-SR-01320-00001 [77]);
- Part 2: Plant Components and Systems (NK21-SR-01320-00002 [78]); and
- Part 3: Accident Analysis (NK21-SR-01320-00003 [75]).

The current revision of Part 3 of Bruce A Safety Report includes all the relevant analyses as of the freeze date of August 31, 2011. The same revision of the Bruce A Safety Report was reviewed in 2012 on an accident-by-accident basis. This was performed as part of the CNSC RD-310 implementation plan and SR improvement activities being tracked under Action Item (AI) 090739. The review assessed the main elements of the safety analysis for each event category that included:

- Identification and classification of the SR events;
- Mapping of the above events to CNSC RD-310 event categorization;
- Relevant acceptance criteria;
- Status of the analysis (Obsolete, Design Changes, Ageing Impact);
- Safety analysis methodology; and
- Main conservative assumptions related to modeling and plant parameters.

The identified gaps are covered by the identified gaps in various review tasks of this Safety Factor Report and were considered in developing the SRI plan [73].

The SRI plan [73] is designed to upgrade the SR analysis at Bruce A and B as part of the CNSC RD-310 implementation plan (now revised to be REGDOG 2.4.1 implementation plan) and SR improvement activities being tracked under Action Item 090739 [65]. The plan reflects achievements to date in addressing SR concerns identified by the CNSC, and builds upon the preliminary SRI plan originally submitted by Bruce Power [79]. These achievements include:

- completion of a number of analyses at Bruce A and B to reflect enhanced methodologies and utilize the modern ISTs for safety analysis,
- completion of an CNSC RD-310 compliant pilot analysis for Bruce A Loss of Flow Events, and

- development of an Industry Deterministic Safety Analysis Principles and Guidelines (P&G) document [27].

The planning basis furthermore takes into account the findings of detailed accident-specific gap assessment work conducted with respect to CNSC RD-310 for Bruce A and B [80]. The SRI plan is established based on Bruce Power's strategy to integrate the existing SR Update program with SRI activities while managing emerging safety concerns. The SRI plan [73] consists of the following two main elements:

- A three-year Safety Report Improvement Project that will be undertaken to align the Bruce A and B Safety Reports with an RD-310 (now CNSC REGDOC-2.4.1) framework. Additionally, a new appendix on Common Mode Failures (CMFs) will be introduced into both the Bruce A and B SRs. This new appendix will be structured as per the CNSC REGDOC-2.4.1 framework, with new CNSC REGDOC-2.4.1 compliant analyses. The project is scheduled to be completed by the end of 2017.
- A Safety Report Improvement Program will be undertaken to perform RD-310 (now CNSC REGDOC-2.4.1) compliant analyses over a nine-year period from 2014 to 2022. The analysis schedule will be guided by gap assessments undertaken by Bruce Power along with business drivers and operational needs.

The current Safety Report of Bruce A incorporates the consequences of changes in actual plant configuration into the analyses of events that are most impacted by ageing. This includes the impact of ageing to the number of Effective Full Power Days (EFPD) covering to at least 2019.

A suite of safety analysis was performed for design basis accidents that are most impacted by ageing incorporating the impacts of ageing to 2019. This suite of safety analysis was submitted to CNSC in support of the Bruce Power licence renewal process [81]. This includes re-analysis for:

- Loss of regulation (Neutron Overpower (NOP) trip setpoint calculations) for Units 1&2 [82] and Units 3&4 [83]
- Small Loss-of-Coolant Accident (SLOCA) for Units 1&2 [84] and Units 3&4 [85]
- LOF for Units 1&2 [76] and Units 3&4 [86], and
- Large LOCA (LLOCA) for Units 1&2 [87] and Units 3&4 [88].

This re-analysis demonstrates that the units are safe to operate now, and processes are in place to ensure safe operation to at least 2019. The other events of Part 3 of the Safety Report are not reflective of the current condition of the plant.

A CNSC report on the application of the CNSC Risk-Informed Decision Making (RIDM) process to Category 3 CANDU Safety Issues (CSIs) identified 16 Category 3[5] issues in 2009 [89]. Three of those issues were later reclassified to Category 2. Four of the remaining thirteen Category 3 issues are related to LLOCA. They are:

AA9 – Analysis for void reactivity coefficient

PF9 – Fuel behaviour in high temperatures

PF10 – Fuel behaviour in power pulse transients

PF12 – Channel voiding during a LLOCA

These four CSIs are addressed through the LLOCA Industry Joint Project COG-JP-4367 final report submitted to CNSC [90]. As part of COG-JP-4367, PF 12 has been reclassified to Category II [91], and Bruce Power has requested reclassification of AA9, PF9 and PF10 in [90]. This issue remains in progress [92].

Significant progress has been made on the nine Category 3 non-LOCA (Loss-of-Coolant Accident) CSIs and their status is shown in Table 6. As shown in this table, five CSIs, namely GL3, SS5, IH6, PF19, and PSA3 were recently reclassified to Category 2. A request for reclassification of three CSIs (CI1, AA3, and PF20) has already made but has not been approved yet by CNSC and BP request to re-classifying PF18 is pending. Bruce Power is following up on CNSC's request for additional support to justify re-classifying the above mentioned CSIs and preparing for the request of re-classifying PF18. For PF18, Bruce Power is leading a COG team to develop the recommendations of the Independent Technical Panel (ITP) [93] into a set of Derived Acceptance Criteria (DAC) acceptable to the CNSC for future deterministic safety analysis performed to support safe operation and CNSC RD-310 implementation. The first revision of a report (COG-13-9035) documenting the derived acceptance criteria to be applied to deterministic safety analysis of postulated accidents is issued [94].

[5] Category 1: The issue has been satisfactorily addressed in Canada.
Category 2: The issue is a concern in Canada - appropriate measures are in place to maintain safety margins.
Category 3: The issue is a concern in Canada - measures are in place to maintain safety margins, but the adequacy of these measures needs to be confirmed.

Table 6: Status of Non-LOCA Category 3 CSIs for Bruce A and B Stations

CSI	Status
GL3 (Ageing of equipment and structures)	Reclassified to Category 2 April 2014
CI1 (Fuel channel integrity and effect on core internals)	Applied for reclassification December 2012
SS5 (Hydrogen control measures during accidents)	Reclassified to Category 2 September 2012
AA3 Computer code and plan model validation	Applied for reclassification February 2013
PF19 (Impact of ageing on safe plant operation)	Reclassified to Category 2 April 2013
PF20 (Analysis methodology for NOP / ROP trips)	Applied for reclassification June 2012
IH6 (Need for systematic assessment of high energy line break effects)	Reclassified to Category 2 August 2012
PSA3 (Open design of the balance of plant - steam protection)	Reclassified to Category 2 October 2014
PF18 (Fuel bundle/element behaviour under post dryout conditions)	Target date is contingent on CNSC review of the ITP and CNSC review of COG 13-9035 “Derived Acceptance Criteria for Deterministic Safety Analysis” [94]

Bruce Power design modifications that are being planned or are being implemented to enhance the safety basis include:

- The introduction of modified 37 element fuel to further mitigate ageing impacts; and

- New neutronic trips for both Shutdown System 1 (SDS1) and Shutdown System 2 (SDS2) to improve the safety margins for large LOCA; and

As part of Bruce Power's Process and Document Enhancement Project, undertaken since the preparation of the Bruce 3&4 ISR, all of the implementing procedures that are relevant to deterministic safety analysis were revised. These include:

- BP-PROC-00363 Nuclear Safety Assessment [46];
- DPT-NSAS-00001 Quality Assurance of Nuclear Safety Assessment [64];
- DPT-NSAS-00002 Safety Report Analysis Update Process Overview [61];
    - DPT-NSAS-00003 Evaluating and Prioritizing Safety Report Issues [62];
- DPT-NSAS-00007 Processing of S-99 Reportable Conditions Arising from Safety Analysis [60];
- DPT-NSAS-00008 Management of External Work For Nuclear Safety Analysis and Support [55];
- DPT-NSAS-00011 Configuration Management of Safety Analysis Software [56];
- DPT-NSAS-00012 Preparation and Maintenance of Operational Safety Requirements [57];
- DPT-NSAS-00013 Guidelines for Managing Reference Data Sets [58];
- DPT-NSAS-00016 Integrated Ageing Management for Safety Assessment [59];
- DPT-NSAS-00015 Execution of Safety Analysis [52];
- DIV-ENG-00012 Nuclear Safety Assessment Initiation and Review [53]; and
- DIV-ENG-00013 Planning of Internal Work for Nuclear Safety Assessment [54].

These procedures ensure that at any given time, the Analysis of Record, which includes Part 3 of the Safety Report, reflects the safety analysis basis and all known issues related thereto for the facility. A more recent revision to the DSA procedures is made specifically to align them with RD-310 (now CNSC REGDOC-2.4.1) requirements. In particular, DPT-NSAS-00015 [52] has been revised extensively to include detailed requirements for the analysis plan that covers RD-310 analysis requirements and provides clear guidance on the framework of the safety analysis process. Updates are being made on procedure DPT-NSAS-00002 to allow it become the overall driver of the SRI Program. DPT-NSAS-00003 is also being updated to conduct risk-based prioritization of the various demands for new Safety Analysis. Further updates and improvements are also being made on procedures DPT-NSAS-00013 and DPT-NSAS-00015. The new revisions of these procedures are expected by the end of 2015. The updated deterministic safety analysis process and procedures are to ensure consistency and reproducibility of safety analyses performed by NSAS or by external organizations. The updated DSA process is intended to be applied to future safety analyses in general and to the anticipated analysis to address gaps in meeting CNSC REGDOC-2.4.1 requirements, in particular. Addressing CNSC REGDOC-2.4.1 gaps in new analyses, as well as any other required analysis, will be based on the guidance provided in the Industry DSA Principles and Guidelines (P&G) document [27], which is specifically prepared for the implementation of SRI programs. This guidance document addresses RD-310 (now CNSC REGDOC-2.4.1) requirements.

The only identified issue relevant to this review task is that not all the analyses within Part 3 of the Safety Report have been kept up with the condition of the plant. This issue is identified as SF5-8 and its source is a gap against CNSC REGDOC-2.4.1 Clause 4.6.2, as shown in Table 8.

5.4. Review of Actual Operational Conditions and Design Basis Acceptance Criteria

This review task evaluates whether the actual operational conditions of the plant meet the acceptance criteria for the design basis. This covers an assessment of the status of the SOE program, and the acceptance criteria used in the analysis of Part 3 of the Safety Report.

Bruce A has recently completed its baseline SOE project which consisted of documenting the limits and conditions derived from the safety analysis in OSRs, completing the corresponding Instrument Uncertainty Calculations (IUCs), and performing Gap Assessments to verify that the requirements are completely and accurately reflected in the station operating documentation. The baseline project and subsequent programmatic SOE activities aim to ensure that the operating limits and conditions in station operating documentation remain aligned with safety analysis upon which the station is licensed. This is required by the relevant codes and standards, in particular CSA N290.15-10, "Requirements for the safe operating envelope of nuclear power plants" [23], which is expected to be incorporated into the new PROL.

One aspect of the SOE program is the production and implementation of OSRs. The OSRs contain analysis and design limits, and required surveillance to ensure that operation is within these limits, and conditions of operability that identify impact of the reduction of barriers up to the safety limit. The OSRs also identify the unit operating conditions under which the limits and conditions apply. The process of producing the OSRs ensures that the operating limits established in safety analysis are consistent with those implemented in actual operation and vice-versa. DPT-NSAS-00015 Execution of Safety Analysis [52] states *“The relevant sections of the Safety Report (SR) and/or Operational Safety Requirements (OSR) and/or Fitness for Service Guidelines (FFSG) and/or Life Cycle Management Plan/Technical Basis Assessment (LCMP/TBA) and/or PRA reports shall be consulted during the preparation of an Analysis Plan or TDF [Task Definition Form] to ensure that input values to be used in the analysis do not inadvertently contradict any safety limits already established. Deviations from these limits should be justified and the basis for the new limit explained.”*

The codes and standards, the Bruce Power governance and implementation procedures that are relevant to the SOE are shown in Table 7.

Table 7: Codes and Standards, BP Governance and Implementation Procedures Relevant to SOE

Relevant Codes and Standards	Relevant SOE Governance	Relevant Implementation Procedures
Bruce A PROL and LCH, "identify requirements for the establishment and maintenance of SOE. COG-02-901 P&G, "the definition, Implementation and maintenance of SOE" CSA N290.15-10, "Requirements for SOE of Nuclear Power Plants"	BP-MSM-1, " Management System Manual" BP-PROG-10.01, "Plant Design Management" BP-PROG-10.02, "Engineering Change Control" BP-PROG-10.03, "Configuration Management" BP-PROG-11.01, "Equipment Reliability" BP-PROG-11.04, "Plant Maintenance" BP-PROG-12.01, "Conduct of Plant Operations" BP-PROG-12.02, "Plant Chemistry Management" BP-PROG-12.03, "Fuel Management"	BP-PROC-00363, "Nuclear Safety Assessment" DPT-NSAS-00012, "Preparation and Maintenance of SOE Requirements" DPT-RS-00015, "Safe Operating Envelope Gap Assessment"

The objective of BP-PROC-00363 [46] is to ensure that all necessary nuclear safety requirements are defined for the actual or proposed design of the plant throughout the design modification process as governed by the Engineering Change Control (ECC) process or in addressing emergent issues (e.g., ageing) that may affect the design basis or the Safety Report basis.

DPT-NSAS-00012 [57] takes authority from the BP-PROC-00363, Nuclear Safety Assessment to provide guidance on the preparation and maintenance of OSRs and identifies requirements for the preparation of IUCs, which are required for a system if the associated OSR identifies safety analysis limits that rely upon the operation of instrumentation either to perform functions post-accident or to verify availability of functions during surveillance. The procedure considers the guidance provided in the CSA standard on safe operating envelope of nuclear power plants [21] and COG Principles and Guidelines on SOE definition and implementation at CANDU Power Plants in Canada [95].

DPT-RS-00015 [96] is the implementation procedure to assess whether station design, operation, and maintenance is in compliance with the requirements imposed by the licensing safety analysis as documented in the OSRs and supporting IUCs, and outlines the roles and responsibilities associated with sustaining SOE compliance. The OSRs and IUCs are living documents that are updated as required to address changes to the design and safety analyses of the station.

The implementing documents of the SOE program are OSRs, IUCs, and gap assessments which are subject to controlled document life cycle management as defined in the Bruce Power Procedure BP-PROC-00068 [97].

In 2012, the CNSC conducted a pilot Type I Inspection of the implementation of the SOE program at Bruce B [98]. CNSC staff observed or identified areas of strengths, as well as areas where improvements are needed, in order for Bruce Power to meet the intent of CSA standard N290.15-10 [23]. CNSC staff has made recommendations to improve the implementation of the SOE program at Bruce Power. The Bruce Power response to CNSC recommendations on SOE was documented in Attachment A of NK29-CORR-00531-10884 [99]. The response included modifications that are being implemented. Bruce Power has issued AR 28404125 on their commitment to complete and track work to resolve gaps in the governance and implementation of CSA N290.15. The identified corrective action is to ensure implementation of CSA N290.15-10 into the hierachy of design documentation. In addressing the identified gaps in governance, BP-PROG-10.01, BP-PROG-10.02 and BP-PROG-10.03 programs and procedures listed below have been, or are to be, revised. Those underlined/italicized below have already been revised, while the revision of the rest of the list are in progress.

- BP-PROC-00539 - Design Change Package
- *BP-PROC-00786 - Margin Management* [100]
- *BP-PROC-00638 - Temporary Configuration Change Management* [101]
- *DPT-PDE-00006 - Design Plan* [102]
- *DPT-PDE-00024 – Preparation and Revision of Overpressure Protection Reports* [103]
- *DPT-PDE-00034 - Preparation and Revision of System Design Manuals, Design Requirements and Design Description* [104]
- DPT-PDE-00013 - Human Factors Engineering Program Plan
- BP-PROC-00014 - Technical Operability Evaluation
- *BP-PROC-00375 - Software Development* [105]
- *DIV-ENG-00005 - Engineering Calculations* [106]
- DPT-PDE-00044 - Preparation and Maintenance of Instrument Uncertainty Calculations
- *DPT-PDE-00040 - Preparation of Instrument Calibration Specifications* [107]
- *SEC-RSA-00001 - Preparation of the EQ Room Conditions Manual* [108]

- BP-PROC-00542 - Configuration Information Change
- BP-PROG-10.01 - Plant Design Basis Management [44]
- BP-PROG-10.02 - Engineering Change Control [109]
- BP-PROG-10.03 - Configuration Management [110]

In all cases, statements are added to describe how each procedure/program relates to the Safe Operating Envelope. A reference to the CSA N290.15 standard was also added to the requirements listed in Section 5.1 of BP-PROC-00786 [100], DPT-PDE-00006 [102], DPT-PDE-00024 [103], BP-PROC-00375 [105], DIV-ENG-00005 [106], DPT-PDE-00040 [107] and SEC-RSA-00001 [108]. As applicable for some of these governance documents, specific steps were also added to address impacts to the Safe Operating Envelope. Furthermore, all impacted administrative document changes for compliance sustainability in PROGs 12.02, 12.03 and 11.01 were planned to be completed by September 30, 2015.

In summary, the completion of the SOE project and subsequent programmatic activities has established a good basis for compliance with CSA N290.15, which includes the preparation of all OSRs, IUCs requirements which are consistent with the Operating Limits and Conditions (OLCs) and their basis derived from safety analysis. Gaps in continuous compliance and areas for improvement in programmatic aspects identified in the self-assessment and pilot inspection are being addressed for the introduction of CSA N290.15 in the next licensing period.

Another aspect considered for this review task is the extent to which the acceptance criteria used in the Bruce A Safety Report meet the relevant requirements of modern codes and standards. Section 1.5, Acceptance Criteria, of Part 3 of the Safety Report addresses radiological doses and derived acceptance criteria for the various design basis events. The events are not categorized as AOOs, DBAs and BDBAs. Accordingly, AOOs are not considered explicitly and their dose limit is currently taken to be the same as for Single Failure (SF) events. Single Failure and Dual Failure (DF) limits of 5 mSv and 250 mSv, respectively, are used in Part 3 of the Safety Report. All dose limits and derived acceptance criteria are met in Part 3 of the Safety Report.

The G-144 requirement of no onset of intermittent fuel sheath dryout prior to the primary trip cannot be met for all events. However, this is considered as an acceptable deviation since G-144 requirements are being replaced with new acceptance criteria which are based on the recommendation of a relevant ITP report [93]. The industry has issued the initial version of COG 13-9035 “Derived Acceptance Criteria for Deterministic Safety Analysis” [94]. This initial version of COG 13-9035 focuses on acceptance criteria for slow events, which are intended to replace G-144 requirements. The industry intends to extend the next version of the report to document the derived acceptance criteria to be applied to deterministic safety analysis of postulated AOOs and DBAs. This document is to be used in support of the *Principles and Guidelines for Deterministic Safety Analysis* (COG-09-9030) [27], which provides overall governance and detailed guidance on performance of safety analysis, including implementation of CNSC regulatory document CNSC REGDOC-2.4.1 [19]. It is also to be used in conjunction with *Guidelines for Application of the LOE/ROE Methodologies to Deterministic Safety Analysis* (COG-11-9023) [68].

With the exception of some events that would be classified as BDBA, but are part of the current safety basis, DSA for BDBAs is currently within the scope of PRA and performed to assist in evaluating the plant safety goals. The plant safety goals are 10^{-4}/a for Severe Core Damage Frequency (SCDF) and 10^{-5}/a for Large Release Frequency (LRF). These safety goals are met. See Safety Factor 6 for more details.

The identified issue relevant to this review task is SF5-3 related to gaps in the experimental basis of the acceptance criteria, and the absence of acceptance criteria specific to AOOs. The sources of this issue are micro-gaps against CNSC REGDOC-2.4.1 and CNSC REGDOC-2.5.2 requirements as shown in Table 8. The path forward is to establish detailed acceptance criteria to be applied to deterministic safety analysis of postulated AOOs and DBAs [94] for their use in new analysis and the implementation of the SRI plan [73].

5.5. Evaluation of Assumptions and Current Regulations and Standards

This review task evaluates whether the assumptions used in the deterministic safety analysis are in accordance with current regulations and standards. This review is mainly based on the findings on analysis assumptions from the review of the various appendices of the Bruce A Safety Report discussed in Section 5.3. The intent of the assessment of this review task is primarily to assess the approach to assumptions made in the DSA of the Safety Report and their comparison against new requirements, particularly in CNSC REGDOC-2.4.1.

Plant operating limits and conditions are taken into account in the analysis assumptions and inputs of Part 3 of the Safety Report. Analysis of the main events impacted by ageing are revised to reflect predicted plant conditions applicable to the licence duration. The results of new analysis are consistently used to confirm the validity of the OLCs applicable to the licence duration and if necessary used to derive a more suitable value for use as an operating limit. The analysis assumptions related to credited operator actions are summarized in Section 1.3 of Part 3 of the Safety Report. The allowed times for operator actions do not meet those proposed in CNSC REGDOC-2.5.2 for new plants. However, with the exception of the analysis of accidents involving the irradiated fuel port, the assumed operator actions are in accordance with the corresponding CNSC REGDOC 2.4.1 requirements. For accidents involving the irradiated fuel port, operator action is credited 10 minutes after the incident. This is less than the recommended 15 minutes allowance after unambiguous indication of a problem requiring operator action from inside the main control room. CSA N290.1 [40] guidance on operator action is similar to CNSC REGDOC 2.4.1 requirements, where 15 minutes for actions inside the control room and 30 minutes for actions outside the control room are recommended.

Conservative assumptions for initial and boundary conditions are used in Part 3 of the Safety Report. Level 2 and Level 4 defence-in-depth are not explicitly covered in Part 3 of the Safety Report. New analyses will be based on COG P&G for DSA [27], which is consistent with CNSC REGDOC-2.4.1 guidance for using more realistic assumptions for Level 2 and Level 4 defence-in-depth.

The CNSC REGDOC-2.4.1 requirement on the single failure criterion applies to all safety systems and their support systems. It has not been demonstrated that the safety analysis for all events in Part 3 of the Safety Report complies with this requirement. CNSC REGDOC-2.4.1

recommends that the single failure criterion not be applied to Level 2 and Level 4 defence-in-depth. This is a less restrictive requirement for Level 2 events (AOOs) and Level 4 events (BDBA); however, DSA in the Safety Report does not distinguish between AOO and DBA and does not address BDBAs explicitly.

Another gap against CNSC REGDOC-2.4.1 requirements was also identified that is related to crediting a control system for the analysis of the Safety Report. For example, for SLOCA analysis, Reactor Regulating System (RRS) normal operation was credited while CNSC REGDOC-2.4.1 requires no credit should be taken for the operation of the control systems in mitigating the effects of the initiating event for Level 3 defence-in-depth.

The three gaps relevant to this review task are identified as SF5-4 on the single failure criterion, SF5-5 on credited systems for Level 3 defence-in-depth analysis, and SF5-12 on the allowance of sufficient time for operator action. The sources of these gaps are CNSC REGDOC-2.4.1 requirement clauses as listed in Table 8.

5.6. Review of Application of Concept of Defence-in-Depth

This review task considers the application of the concept of defence-in-depth.

CNSC REGDOC-2.5.2 [35] states that "*The design of an NPP shall incorporate defence in depth. The levels of defence in depth shall be independent to the extent practicable. Defence in depth shall be achieved at the design phase through the application of design provisions specific to the five levels of defence.*"

The aim of the first level of defence-in-depth is to prevent deviations from normal operation, and to prevent failures of SSCs. The first level of defence-in-depth is supported by good engineering practices used in the design and for engineering changes, which assures high quality of modifications and adherence to design principles consistent with the requirements of defence-in-depth. Design changes are managed through Bruce Power's Engineering Change Control program BP-PROG-10.02 [109]. Examples of the Bruce A design features of Level 1 defence-in-depth are that:

- the electrical system and heat transport system provide engineering features to prevent electrical system failures and failures of the Heat Transport (HT) main pumps, or mitigating their consequences;
- common systems are divided into odd and even buses to ensure dual bus redundancy is provided; and
- system connections are such that half of any process is supplied from an odd bus and the other half from an even bus.

In addition, two systems (i.e., shutdown cooling system and maintenance cooling system) are provided for removing reactor shutdown heat. Safety analysis of the effectiveness of the special safety systems and the applicable alternative heat sink systems was performed and is documented in the Safety Report, although stress analysis for the Bruce A shield cooling system is not performed to confirm the design and safety requirement.

The aim of the second level of defence-in-depth is to detect and intercept deviations from normal operation in order to prevent AOOs from escalating to accident conditions, and to allow return of the plant to a state of normal operation. To support the second level of defence-in-depth, AOOs are required to be analyzed to demonstrate the robustness of the control systems in arresting AOOs and in preventing damage to SSCs that are not involved in the initiation of an AOO, to the extent that these SSCs will remain operable following the AOO. Such assessment is not explicitly considered in Part 3 of the Safety Report. Level 2 defence-in-depth for the various events is provided by RRS, Heat Transport System (HTS) pressure and inventory control and secondary side pressure and inventory control systems. Most of the analyzed AOOs are not expected to require safety system initiation (i.e., Level 2 of defence-in-depth can be demonstrated). For some AOOs, it may be necessary to invoke elements of SDS1 or SDS2, which are qualified, reliable and fast acting systems normally considered part of Level 3 defence-in-depth. The specific features of the CANDU reactor, which provides for three independent means of reactor shutdown (RRS setback/stepback and two independent shutdown systems), make it possible in a specific AOO scenario to utilize either SDS1 or SDS2 trip parameters in achieving the objective of Level 2 defence-in-depth, if the normal Level 2 defence-in-depth provisions (i.e., RRS parameters used to initiate protective action) are ineffective. Credit is taken for the SDS trip signal only since, in CANDU designs, stepback is automatically initiated on any SDS trip. Due to the additional defence-in-depth available in the CANDU reactor design, the systems credited in a Level 2 defence-in-depth role may differ in some instances from those credited in other reactor designs. For more details, see COG P&G for DSA [27]. This complies with the guidance clause 4.2.3.1 of CNSC REGDOC-2.4.1, "*Plant design is expected to be sufficiently robust, such that most AOOs would not require the initiation of safety systems to prevent consequential damage to the plant's SSCs. This is part of Level 2 defence in depth, and helps to ensure that events requiring use of safety systems are minimized.*"

The aim of the third level of defence-in-depth is to minimize the consequences of accidents by providing inherent safety features, fail-safe design, additional equipment, and mitigating procedures. Level 3 defence-in-depth is primarily provided by the special safety systems: SDS1 and SDS2, the Emergency Core Cooling system, and the Containment system. In addition, overpressure protection is provided by the HT relief valves for HTS and the steam relief valves for the secondary side.

To support the third level of defence-in-depth, DBAs are analyzed to demonstrate the capabilities of the safety systems to mitigate any resulting radiological consequences, i.e., to demonstrate meeting the prescribed dose limits for DBAs and related derived acceptance criteria for protecting fission product release barriers. The analyses of DBAs are also used to assist in developing Abnormal Incidents Manuals (AIMs) or emergency operating procedures that define actions that should be taken during these events. Part 3 of the Safety Report analyses focuses on Level 3 defence-in-depth. An AOO plus independent failure of Level 2 defence-in-depth would be classified as a DBA, and the dose limit applicable to DBAs applies.

The aim of the fourth level of defence-in-depth is to ensure that radioactive releases caused by severe accidents are kept as low as practicable. Level 4 of defence-in-depth is achieved by providing equipment and procedures to manage accidents and mitigate their consequences. This level of defence is covered in Section 5.7.

The aim of the fifth level of defence-in-depth is to mitigate the radiological consequences of potential releases of radioactive materials that may result from accident conditions. Level 5 defence-in-depth is secured by providing adequately equipped emergency support facilities, and plans that are covered in SFR13 – Emergency Planning.

The only identified gap relevant to this review task is that stress analysis is not performed for the Bruce A shield cooling system to confirm the design and safety requirement. This is identified as SF5-11 in Table 8.

5.7. Review of Development and Validation of Emergency Operating Procedures and Accident Management Program

This review task evaluates whether appropriate deterministic methods have been used for the development and validation of emergency operating procedures and the accident management program at the plant. The scope of this review is extended to review the fourth level defence-in-depth. SFR13 – Emergency Planning covers all emergency management aspects.

The Emergency Management Program BP-PROG-08.01 [111] is developed to enable effective response to all hazards at Bruce Power by considering:

- Design basis accidents;
- Beyond design basis accidents;
- Other emergencies (e.g., conventional) leading to nuclear emergencies; and
- Multi-unit accident scenarios, if applicable.

This review task focuses on the DSA for DBAs and BDBAs used in supporting the emergency procedures and accident management program. The relevant operation-based implementing documents are the AIMs, which include procedures specifically established to mitigate various design basis events, and Severe Accident Management Guidance (SAMG), which is used if the plant has entered, or is going to enter, a severe accident condition. A comprehensive set of Bruce Power specific AIMs and SAMG documents are prepared. The technical basis, entry and exit conditions, and assumptions used in AIM procedures, including credits for operator actions make use of the deterministic analysis of the design basis events, while those used in SAMG technical basis are largely based on the deterministic safety analysis of severe BDBAs analyzed within the PRA Level 2 scope, as well as previous PRA Level 1 and 2 assessments.

SAMG documents are in place and the progress on the resolution of the identified gaps resulting from extensive post-Fukushima reviews and assessments has progressed well [112]. A new Emergency Management Centre is in place and significant improvements have been made on the emergency program. Post-Fukushima design enhancements to prevent and mitigate severe accidents include adding design features to allow external water makeup to the HTS, moderator system, steam generators and the irradiated fuel bay, as well as enhancements to the emergency power supply and providing overpressure protection to the shield tank. These modifications are intended to provide further defence-in-depth against beyond design basis accidents and to support SAMGs by early mitigation of the severe accident progression and protecting containment integrity. These modifications significantly improve the fourth level of defence-in-depth. PRAs, taking into account Emergency Mitigation Equipment, demonstrate significant improvements in SCDF and releases (see SFR6 for details).

The generic COG SAM guidance, and subsequently the Bruce Power guidance, was developed to guide response to a severe accident occurring on a single unit only. For multi-unit sites, SAMG needs to consider the possibility of accidents occurring concurrently on more than one unit. This may require complementary DSA for BDBAs that would be needed for the confirmation of the safety goals and/or to support enhancements to SAM guidance. CNSC REGDOC-2.4.1 guidance clause 4.4.2.6 requires that the analysis should take into account the capacity and limitations of long-term makeup water and electrical power supplies.

The main issue identified for this review task is that the completeness of the considered multi-unit events needs to be confirmed. In particular, this may require complementary DSA for BDBAs, accounting for the capacity and limitations of long-term makeup water and electrical power supplies to confirm meeting the safety goals. This issue is identified as SF5-6 in Table 8.

5.8. Review of Radiation Doses and Releases of Radioactive Material in Normal and Accident Conditions

This review task evaluates whether calculated radiation doses and releases of radioactive material in normal and accident conditions meet regulatory requirements and expectations.

The radiation dose limits for members of the public for releases of radionuclides from Bruce A during normal operation are given in Table 1.2 of Part 1 of the Safety Report [77]. The applicable dose limits are those provided in the Radiation Protection Regulations [113].

The limits on radioactive releases for accident conditions are given in Section 1.5 of Part 3 of the Safety Report [75]. The applicable dose limits are those provided in the original Siting Guide [74]. The Siting Guide dose limits are specified for postulated initiating events involving a single process failure (termed single failures) and for events involving a single process failure in conjunction with failure of one of the special safety systems (termed dual failures).

CNSC REGDOC-2.4.1 [19] addresses dose limits and radiation releases in its Section 4.3 on *Acceptance Criteria.* For normal operation, it requires in Section 4.3.1 that analyses demonstrate that radiological doses to workers and members of the public are within limits acceptable to the CNSC. For AOOs and DBAs it requires in Section 4.3.2 that analyses demonstrate that radiological doses to members of the public do not exceed the established limits. The guidance in Section 4.3.2 of CNSC REGDOC-2.4.1 states that:

"This dose is less than or equal to one of the following dose acceptance criteria:

- *0.5 millisievert for any AOO*
- *20 millisieverts for any DBA*

These dose limits apply to new NPPs. For existing reactors, the dose limits specified in the operating licences must be met."

The specific dose limits specified in Bruce A Safety Report are 5 mSv for single failures and 250 mSv for dual failures. Since the single failure dose limit of 5 mSv is less than the new limit for DBAs of 20 mSv, Bruce A would meet the CNSC REGDOC-2.4.1 limit for DBAs. Dual failures would be classified as BDBAs. AOOs have not been treated separately, and some of them may not meet the new limit of 0.5 mSv. However, those currently analyzed as DBAs have been shown to meet the current single failure limit as required. This is implicit in the issue identified in gap SF5-2 in Table 8.

An issue relevant to CNSC REGDOC-2.4.1 guidance clause 4.4.4.7 was identified. The clause specifies that weather scenarios with probabilities of occurrences higher than 5% and dose calculations for intervals up to 1 year should be considered. This is not demonstrated in Part 3 of the Safety Report. This issue is identified as SF5-7 in Table 8.

5.9. Review of Adequacy and Effectiveness of Engineering and Administrative Measures to Prevent and Mitigate Accidents

This review task includes the analysis of the functional adequacy and reliability of systems and components, the impact on the safety of internal and external events, equipment failures and human errors, the adequacy and effectiveness of engineering and administrative measures to prevent and mitigate accidents.

The purpose of this review task is similar to that on the application of the concept of defence-in-depth discussed in Section 5.6. The effectiveness of engineering and administrative measures is demonstrated through safety analysis of a wide range of accident scenarios, demonstrating that the levels of defence-in-depth have been met, and that all of the regulatory reference dose limits of the current licence are not exceeded.

Preventive strategies are needed to preserve safety functions that are important to prevent or mitigate the consequences of core damage such as maintaining core cooling and containment integrity. SCDF is a measure of the plant's ability to prevent escalation of postulated accidents. The Large Release Frequency is a measure of the plant's accident mitigation capabilities. The plant safety goals are 10^{-4}/a for SCDF and 10^{-5}/a for LRF and both are met. See Safety Factor 6 for more details.

Bruce Power's Equipment Reliability program [114] provides an overall description of the equipment reliability process, and establishes a framework to monitor and maintain Structures, Systems and Components (SSC). DSA and PRA outputs are utilized in establishing this framework and the scope of Emergency Response procedures. The Bruce A Annual Reliability Report is regularly submitted to meet the CNSC annual reporting requirements. The Annual Reliability Report includes assessments of the reliability of Systems Important to Safety (SIS) against their performance targets. SFR1 and SFR6 of the current ISR include an assessment of SIS performance against the relevant requirements of new codes and standards. No gaps relevant to this review task of SFR5 are identified.

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 1: Plant Design" in Appendix B.1 provides a detailed assessment of CSA N290.1-13, Requirements for the Shutdown Systems of CANDU Nuclear Power Plants, and in Appendix B.2 provides a detailed assessment of CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants.
- "Safety Factor 6: Probabilistic Safety Analysis" in Section 5.3, addresses BDBA events which are not currently part of the safety basis, performed to assist in evaluating plant safety goals for SCDF and LRF.
- "Safety Factor 7: Hazards Analysis" in Section 5.1 and 5.2, respectively, assesses the systematic identification of external and internal hazards, which may have to be considered as PIEs for deterministic safety analysis.
- "Safety Factor 13: Emergency Planning" in Section 5.1, addresses Level 5 of defence-in-depth by reviewing the Bruce Power Nuclear Emergency Response Plan and Severe Accident Management Guidance in terms of adequacy which make use of deterministic safety analysis of DBAs and BDBAs.

7. Program Assessments and Adequacy of Implementation

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

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

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

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

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

Among various self-assessments that were carried out since 2009, the NSAS self-assessment, SA-NSAS-2010-01 Safety Report Update Process Effectiveness Review [115], is the most relevant to Safety Factor 5 as discussed below.

The objective of this self-assessment [115] was to ensure the effectiveness of the Safety Report Update (SRU) process in identifying, prioritizing and closing safety analysis issues. The assessment was based on reviewing DPT-NSAS-00002, Safety Report Analysis Update Process Overview [61], DPT-NSAS-00003, Guidelines for Evaluating and Prioritizing Safety Report Issues [62], and DPT-NSAS-00004, Guidelines for Managing the Key Deliverables of the SRU Process [116].

In the assessment, a Safety Analysis Issue Review Panel (SAIRP) meeting was observed, interviews held with SAIRP Subject Matter Experts (SMEs) and the SAIRP chair, and completed questionnaires by SAIRP participants and the SRU process owner were reviewed.

This assessment concluded that the SRU process is reliable; however, opportunities for improvement and corrective actions were identified to improve the effectiveness of the process, which were closed based on the completion of follow-up actions that were performed.
No more recent self-assessments are identified, although there was a CNSC inspection in 2012 (discussed in Section 7.3) that would have obviated the need for a more recent self-assessment.

7.2. Internal and External Audits and Reviews

The objective of the audit process as stated in BP-PROG-15.01 [117] 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 [118]).

No recent independent internal audits or reviews relevant to Safety Factor 5 have been identified.

Relevant regulatory evaluations and reviews are discussed in the next section. No other recent external audits or reviews relevant to Safety Factor 5 have been identified.

7.3. Regulatory Evaluations and Reviews

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

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

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

A CNSC staff review of Bruce Power's Deterministic Safety Analysis [119] was conducted in 2012 in accordance with a CNSC request made in [120]. This CNSC review was conducted by performing the following three activities:

- Reviewing BP quality documents and procedures related to Safety Analysis;
- Conducting interviews with BP managers and staff responsible for safety analysis; and
- Conducting vertical slice detailed reviews for selected analyses to examine work completed and records maintained.

The CNSC review concluded with the following main results:

- Bruce Power has sufficient quality documents related to the conduct of safety analysis;
- These documents are being followed to a large extent by Bruce Power staff;
- Bruce Power has a well-developed training program and Nuclear Safety Analysis and Support Department (NSASD) is developing specialized training for its staff; and
- Bruce Power has good management oversight for planning and conducting safety analysis activities.

No formal actions were placed on Bruce Power as a result of this review. However, Bruce Power had reviewed the recommendations provided in the desktop review report and they are considered for implementation as discussed in Attachment A of the Bruce Power response to CNSC recommendations [121].

In 2012, the CNSC also conducted a pilot Type I Inspection of the implementation of the SOE program at Bruce B [98]. CNSC staff observed or identified areas of strengths, as well as areas where improvements are needed, in order for Bruce Power to meet the intent of CSA N290.15-10 [23]. The Bruce Power response to CNSC recommendations on SOE implementation included modifications and changes that have been implemented, or are to be implemented, in SOE governance. For more details see Section 5.4.

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 Bruce Power specific performance indicators associated with deterministic safety analysis or any of the relevant programs and procedures.

The “CNSC Staff Integrated Safety Assessment of Canadian Nuclear Power Plants for 2013”, issued in September 2014 [122], summarizes the 2013 ratings for Canada’s NPPs in each of the 14 CNSC Safety and Control Areas (SCA), including safety analysis. 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 review of Bruce A against modern codes and standards and international safety expectations and provide input to a practicable set of improvements to be conducted during the Major Component Replacement in Units 3 and 4, and during asset management activities to support ongoing operation of all four units, that will enhance safety to support long term operation. The specific objective of the review of this Safety Factor is to determine to what extent the existing safety analysis remains valid when the following aspects have been taken into account: actual plant design; the actual condition of SSCs and their predicted state at the end of the period covered by the ISR; current deterministic methods; and current safety standards and knowledge. In addition, the review should also identify any gaps relating to the application of the defence-in-depth concept. This specific objective has been met by the completion of the review tasks specific to deterministic safety analysis.

Major improvements relevant to DSA that were identified during this review are:

- Bruce Power has established an integrated strategy to improve the deterministic safety analysis contained in the Safety Reports as part of its objective to reach compliance with CNSC REGDOC-2.4.1 to the maximum practicable extent over a defined transition period. Bruce Power DSA procedures have been revised in consideration of CNSC REGDOC-2.4.1 requirements and the industry P&G for DSA. Industry guidelines for LOE/ROE and BEAU methodologies are established. Moreover, "Derived Acceptance Criteria for Deterministic Safety Analysis" is issued as COG 13-9035 [94]. Bruce Power is leading or actively participating in all SRI activities.
- Bruce Power has implemented or is in the process of adding significant preventive and mitigating design modifications that are intended to provide further defence-in-depth against design basis events and severe accidents and to support SAMGs by mitigating severe accident progression and protecting containment integrity.

Table 8 summarizes the key issues arising from the Integrated Safety Review of Safety Factor 5.

Table 8: Key Issues

Issue Number	Gap Description	Source(s)
SF5-1	A number of the legacy analyses in the Safety Report are performed with codes (including the models and data) that have not been verified and validated to the requirements of CSA N286.7-99. Some key legacy computer codes, such as SOPHT, may not have been formally validated as per CSA N286.7-99, but code	Section 5.1 Micro-gaps against requirement clauses: REGDOC-2.4.1 – Clause 3 (Gap 2) REGDOC-2.4.1 – Clause 4.1 (Gap 1) REGDOC-2.4.1 – Clause 4.4.1 (Gap 1) (Gap 2) (Gap 3) (Gap4)

Issue Number	Gap Description	Source(s)
	prediction has been compared to experimental and station data and benchmarking between SOPHT and TUF was performed. However, the following are not consistently addressed: • Assessment of the applicability of the codes to the analyzed events, and • Consideration of code accuracy in predicting key parameters.	REGDOC-2.4.1 – Clause 4.4.2 (Gap 1) (Gap 2) (Gap 3)(Gap 5) REGDOC-2.4.1 – Clause 4.4.3 (Gap 1) (Gap 2) (Gap 3) (Gap 4) REGDOC-2.4.1 – Clause 4.4.5 (Gap 1) REGDOC-2.4.1 – Clause 4.5 (Gap 1) REGDOC-2.4.1 – Clause 4.7 (Gap 1) REGDOC-2.5.2 – Clause 9.4 (Gap 3) Micro-gaps against guidance clauses: REGDOC-2.4.1 – Clause 4.3.2 (Gap 2) REGDOC-2.4.1 – Clause 4.4.2.9 (Gap 1) REGDOC-2.4.1 – Clause 4.4.4.6 (Gap 1)
SF5-2	A systematic event identification and classification process is not well documented and/or demonstrated. AOOs have been addressed implicitly rather than explicitly in the deterministic safety analysis. Common-mode failure events are not included in Part 3 of the Safety Report. Relevant operational modes are not comprehensively addressed.	Section 5.2 and 5.8 Micro-gaps against requirement clauses: REGDOC-2.4.1 – Clause 4.3 (Gap 1) REGDOC-2.4.1 – Clause 4.2.1 (Gap 1) REGDOC-2.4.1 – Clause 4.2.2 (Gap 1) (Gap 2) (Gap 3) REGDOC-2.4.1 – Clause 4.2.3 (Gap 1) REGDOC-2.5.2 – Clause 4.2.1 (Gap 1) REGDOC-2.5.2 – Clause 4.2.3 (Gap 1) REGDOC-2.5.2 – Clause 6.1 (Gap 1) REGDOC-2.5.2 – Clause 6.4 (Gap 1) (Gap 2) (Gap 3) REGDOC-2.5.2 – Clause 6.6.1 (Gap 1) REGDOC-2.5.2 – Clause 7.4 (Gap 1) REGDOC-2.5.2 – Clause 8.10.4 (Gap 1) REGDOC-2.5.2 – Clause 9.1 (Gap 1) REGDOC-2.5.2 – Clause 9.2 (Gap 1) REGDOC-2.5.2 – Clause 9.4 (Gap 1) Micro-gaps against guidance clauses: REGDOC-2.4.1 – Clause 4.2.1 (Gap 2) (Gap 3)

Issue Number	Gap Description	Source(s)
SF5-3	The acceptance criteria are not systematically supported by experimental data.	Sections 5.4 Micro-gaps against requirement clauses: REGDOC-2.4.1 – Clause 4.3.2 (Gap 1) REGDOC-2.4.1 – Clause 4.3.4 (Gap 1)(Gap 2) REGDOC-2.5.2 – Clause 8.4.1 (Gap 1) REGDOC-2.5.2 – Clause 9.4 (Gap 2) Micro-gaps against guidance clauses: REGDOC-2.4.1 – Clause 4.3.2 (Gap 3) (Gap 4) (Gap 5) REGDOC-2.4.1 – Clause 4.3.4 (Gap 3) (Gap 4)
SF5-4	All analyses documented in the Safety Report were in accordance with the interpretation of the single failure criterion prevalent at the time. However, these analyses do not follow newer, more restrictive, interpretations of the single failure criterion.	Section 5.5 Micro-gaps against requirement clauses: REGDOC-2.4.1 – Clause 4.4.4 (Gap 1)(Gap 2)(Gap 4) REGDOC-2.5.2 – Clause 7.6.2 (Gap 1)
SF5-5	The limiting assumption with respect to RRS working or failed is not demonstrated for Small LOCA and transition breaks.	Section 5.5 Micro-gaps against requirement clauses: REGDOC-2.4.1 – Clause 4.4.4 (Gap 3)
SF5-6	Bruce A station PRA indicates that multi-unit events are considered. The completeness of such consideration needs to be confirmed, in particular, it may require complementary DSA for BDBAs, accounting for the capacity and limitations of long-term makeup water and electrical power supplies to confirm meeting the safety goals. Some of the analyzed events in the Safety Report will be classified as BDBAs and any required revision of their analysis will need to adopt a more realistic analysis methodology consistent with the PRA approach.	Section 5.7 Micro-gaps against requirement clauses: REGDOC-2.5.2 – Clause 4.2.2 (Gap 1) REGDOC-2.3.2 – Clause 3.4 (Gap 1) REGDOC-2.3.2 – Clause 4.2.1 (Gap 1) REGDOC-2.3.2 – Clause 4.2.5 (Gap 1) REGDOC 2.4.1 – Clause 4.4.4 (Gap 6)

Issue Number	Gap Description	Source(s)
SF5-7	It is not demonstrated if weather scenarios with probabilities of occurrences higher than 5% and dose calculations for intervals up to 1 year are considered.	Section 5.8 Micro-gaps against guidance clauses: REGDOC-2.4.1 – Clause 4.4.4.7 (Gap 1)
SF5-8	Part 3 of the Safety Report is not fully reflective of the condition of the plant.	Section 5.3 Micro-gaps against requirement clauses: REGDOC-2.4.1 – Clause 4.6.2 (Gap 1)
SF5-9	Conservative assumptions are used in the analysis. However, there is no demonstration that the conservatism of the analysis covers modeling uncertainties.	Section 5.1 Micro-gaps against requirement clauses: REGDOC-2.4.1 – Clause 4.4.6 (Gap 1)
SF5-10	Cliff edge-effects are inherently covered in the assessment of trip coverage, however, it is not consistently addressed for quantitative acceptance criteria beyond reactor trip.	Section 5.1 Micro-gaps against requirement clauses: REGDOC-2.4.1 – Clause 4.2.3 (Gap 2) REGDOC-2.4.1 – Clause 4.4.2 (Gap 4)
SF5-11	Stress analysis for Bruce A shield cooling system is not performed to confirm the design and safety requirement.	Section 5.6 Micro-gaps against requirement clauses: REGDOC-2.4.1 – Clause 3 (Gap 1)
SF5-12	For accidents involving the irradiated fuel port, operator action is credited 10 minutes after the incident. This is less than the usual 15 minutes allowed from first unambiguous indication of a problem requiring operator action from inside the main control room.	Section 5.5 Micro-gaps against requirement clauses: REGDOC 2.4.1 – Clause 4.4.4 (Gap 5)

The overall conclusion is that, with the exceptions noted in Table 8, Bruce Power's programs meet the requirements of the Safety Factor related to deterministic 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, 2013.

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

[5] NK21-CORR-00531-03839, Bruce A Environmental Assessment Study Report, December 7, 2005.

[6] CNSC REGDOC-2.3.3, Operating Performance: Periodic Safety Reviews, CNSC, April 2015.

[7] NK21-CORR-00531-00514, Bruce A: CNSC approval to Restart Units 3 and 4 and Application to Amend PROL 15.01/2003, Bruce Power Letter, F. Saunders to J.H.M. Douglas, November 16, 2001.

[8] NK21-CORR-00531-04059, Bruce A Refurbishment for Life Extension – Systematic Review of Safety: Plant Design, Bruce Power Letter, F. Saunders to P. Webster, March 30, 2006.

[9] NK21-CORR-00531-04339, Bruce A Units 1 and 2 Return to Service – Systematic Review of Safety, Bruce Power Letter, F. Saunders to P. Webster, July 31, 2006.

[10] NK21-CORR-00531-05976, Bruce A Units 3 and 4 Refurbishment for Life Extension and Continued 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 15.00/2015), May 1, 2014.

[16] NK21-CORR-00531-11391, Bruce Nuclear Generating Station A Nuclear Power Reactor Operating Licence: Licence Conditions Handbook (LCH-BNGSA-R8), June 4, 2014.

[17] PROL 18.00/2020, e-Doc 4723908, Nuclear Power Reactor Operating Licence, Bruce Nuclear Generating Station A and Bruce Nuclear Generating Station B, June 1, 2015.

[18] LCH-BNGS-R000, e-Doc 4659316, Bruce Nuclear Generating Station A and Bruce Nuclear Generating Station B Power Reactor Operating Licence, June 1, 2015.

[19] CNSC REGDOC-2.4.1, Deterministic Safety Analysis, May 2014.

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

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

[22] CSA N290.13-05, Environmental Qualification of Equipment for CANDU Nuclear Power Plants, February 2005, R2010.

[23] CAN/CSA N290.15-10, Requirements for the Safe Operating Envelope of Nuclear Power Plants, August 2010.

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

[25] 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.

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

[27] COG-09-9030 R03, Principles & Guidelines for Deterministic Safety Analysis Used in Licensing of Current Nuclear Power Plants Operating in Canada, CANDU Owners Group, November 2014.

[28] ISTR-12-5044-R001, Code Validation Guidelines Document, November 2012.

[29] ISTO-09-5092-R002, Guidelines for Generic Methodology for Estimation of Computer Code Accuracy, September 2012.

[30] COG-02-901, Principles and Guidelines for the Definition, Implementation and Maintenance of the Safe Operating Envelope at CANDU Power Plants in Canada, CANDU Owners Group, March 2003.

[31] NK21-CORR-00531-11728/NK29-CORR-00531-12117, Bruce A and Bruce B CSA N290.15 Compliance Update, December 9, 2014.

[32] CNSC R-10, The Use of Two Shutdown Systems in Reactors, January 1977.

[33] CNSC R-77, Overpressure Protection Requirements for Primary Heat, October 20, 1987.

[34] CNSC REGDOC-2.3.2, Accident Management Severe Accident Management Programs for Nuclear Reactors, October 2014.

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

[36] CNSC G-144, Trip Parameter Acceptance Criteria for the Safety Analysis of CANDU Nuclear Power Plants, May 2006.

[37] CNSC G-149, Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors, October 2000.

[38] 13-M25, Regulatory Framework Program Update, CNSC, May 16, 2013.

[39] CAN/CSA N288.2-M91, Guidelines for Calculating Radiation Doses to the Public from a Release under Airborne Radioactive Material Under Hypothetical Accident Conditions in Nuclear Reactors, 1991.

[40] CAN/CSA N290.1-13, Requirements for Shutdown Systems of Nuclear Power Plants, December 2013.

[41] CAN/CSA N290.4-11, Requirements for Reactor Control Systems of Nuclear Power Plants, October 2011.

[42] CAN/CSA N290.5-06, Requirements for Electrical Power and Instrument Air Systems of CANDU Nuclear Power Plants, December 2006 (Update No. 1, Reaffirmed 2011).

[43] CAN/CSA N290.6-09, Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of an Accident, March 2009 (Reaffirmed 2014).

[44] BP-PROG-10.01-R008, Plant Design Basis Management, Bruce Power, January 6, 2014.

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

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

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

[48] DIV-ENG-00009-R005, Design Authority, November 1, 2013.

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

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

[51] BP-MSM-1 Sheet 0002-R015, MSM - Approved Reference Chart Authorities and Responsibilities, Bruce Power, January 20, 2015.

[52] DPT-NSAS-00015-R004, Execution of Safety Analysis, Bruce Power, October 16, 2013.

[53] DIV-ENG-00012-R001, Nuclear Safety Assessment Initiation and Review, Bruce Power, April 29, 2010.

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

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

[56] DPT-NSAS-00011-R004, Configuration Management of Safety Analysis Software, Bruce Power, October 11, 2013.

[57] DPT-NSAS-00012-R003, Preparation and Maintenance of Operational Safety Requirements, Bruce Power, September 8, 2011.

[58] DPT-NSAS-00013-R003, Guidelines for Managing Reference Data Sets, Bruce Power, September 20, 2011.

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

[60] DPT-NSAS-00007-R004, Processing of S-99 Reportable Conditions Arising from Safety Analysis, Bruce Power, August 30, 2011.

[61] DPT-NSAS-00002-R004, Safety Report Analysis Update Process Overview, Bruce Power, September 14, 2011.

[62] DPT-NSAS-00003-R004, Guidelines for Evaluating and Prioritizing Safety Report Issues, Bruce Power, September 14, 2011.

[63] DPT-RS-00015-R000, Safe Operating Envelope Gap Assessment, Bruce Power, May 31, 2011.

[64] DPT-NSAS-00001-R006, Quality Assurance of Nuclear Safety Assessment, Bruce Power, August 20, 2014.

[65] NK21-CORR-00531-07548/NK29-CORR-00531-08524, Action Item 090739 - Implementation of RD-310/Action Items 070718/071402: Safety Report Improvement Program, CNSC Letter, F. Saunders to K. Lafrenière, December 10, 2009.

[66] NK21-CORR-00531-04994, Bruce Units 1&2 Return to Service and Life Extension - CNSC Staff Review of Bruce Power's Systematic Review of Safety, CNSC Letter, D. Desjardins to F. Saunders, May 18, 2007.

[67] NK21-CORR-00531-05206/e-Doc 3069369, Bruce NGS A Safety Report Update Part 3: Accident Analysis, CNSC Letter, P. Elder to F. Saunders, August 10, 2007.

[68] COG-11-9023-R001, Guidelines for the Application of the LOE/ROE Methodologies to Deterministic Safety Analysis, CANDU Owners Group, November 2014.

[69] COG-06-9012-R001, Guidelines for Application of the Best Estimate Analysis and Uncertainty (BEAU) Methodology to Design Basis Accident (DBA) Licensing Analysis, CANDU Owners Group, April 28, 2008.

[70] NK21-CORR-00531-11218/e-Doc 4405384, Closure of Action Item 110701: CANDU Safety Issue AA3 – Computer Codes and Plant Model Validation – TUF Validation Work, CNSC Letter, K. Lafrenière to F. Saunders, March 26, 2014.

[71] NK21-CORR-00531-11051, Request for Closure of Action Item 110701: CANDU Safety Issue AA3: Computer Codes and Plant Model Validation – TUF Validation Work, Bruce Power Letter, F. Saunders to K. Lafrenière, March 12, 2014.

[72] NK21-CORR-00531-11466, Action Item 110701 Post Closure Progress Update: TUF Code Validation Activities, Bruce Power Letter, F. Saunders to K. Lafrenière, August 1, 2014.

[73] NK21-CORR-00531-10774/NK29-CORR-00531-11155, Action Item 090739: Safety Report Improvement Plan for Bruce A and Bruce B, Bruce Power Letter, F. Saunders to R. Lojk, November 20, 2013.

[74] Paper 72-CNA-102, D.G. Hurst and F.C. Boyd, Reactor Licensing and Safety Requirements, presented at the 12th Annual Conference of the Canadian Nuclear Association, Ottawa, Canada, June 11-14, 1972.

[75] NK21-SR-01320-00003-R004, Bruce A Safety Report, Part 3: Accident Analysis, Bruce Power, January 2012.

[76] NK21-REP-03507.1 P NSAS, RD-310 Pilot Project – Electrical System Failures, December 2013.

[77] NK21-SR-01320-00001-R005, Bruce A Safety Report, Part 1: Plant and Site Description, Bruce Power, February 2013.

[78] NK21-SR-01320-00002-R005, Bruce A Safety Report, Part 2: Plant Components and Systems, Bruce Power, February 2013.

[79] NK21-CORR-00531-08258/NK29-CORR-00531-09070, Action Item 090739: Safety Report Improvement Program, Bruce Power Letter, F. Saunders to K. Lafrenière, November 30, 2010.

[80] NK21-03500 NSAS / NK29-03500 NSAS, RD-310 Gap Prioritization Report, Bruce Power, December 12, 2012.

[81] NK21-CORR-00531-10943/NK29-CORR-00531-11325, Safety Analysis in Support of Operation of Bruce A and B to 2019, Bruce Power Letter, F. Saunders to R. Lojk, December 12, 2013.

[82] NK21-63720/63730 P NSAS, Bruce NGS A Units 1&2: Assessment of NOP Trip Coverage at 2019 Aged Core Conditions, December 11, 2013.

[83] NK21-63720/63780 P NSAS, Bruce NGS A Units 3&4: Assessment of NOP Trip Coverage at 2019 Aged Core Conditions, December 11, 2013.

[84] NK21-03507.1 P NSAS, Bruce NGS A Unit 1&2 Small LOCA Assessment to the End of 2019, November 15, 2013.

[85] NK21-03507.1 P NSAS, Bruce A Units 3&4 Small LOCA Analysis in Support of Operation to 2019, November 26, 2013.

[86] NK21-03507.1 P NSAS, Bruce NGS A Units 3&4 Loss of Flow Analysis in Support of Operation to 9950 EFPD, December 2, 2013.

[87] NK21-03503.7 LOF NSAS, Assessment of Impact of Change in Coolant Void Reactivity on Large Break LOCA Analysis for Bruce A Units 1 and 2, December 6, 2013.

[88] NK21-03503.7 LOF NSAS, Analysis of Large Break Loss of Coolant Accident for Bruce A NGS Units 3 and 4 in Support of Operation to 9950 EFPD, November 25, 2013.

[89] N-REP-03611-0381169/e-Doc 3413831, Application of the CNSC Risk-Informed Decision Making Process to Category 3 CANDU Safety Issues, Canadian Nuclear Safety Commission, August 2009.

[90] NK21-CORR-00531-10787/NK29-CORR-00531-11164, Large Break Loss of Coolant Accident: Composite Analytical Approach, Bruce Power Letter, F. Saunders to G. Rzentkowski, September 26, 2013.

[91] NK21-CORR-00531-10543/NK29-CORR-00531-10942/e-Doc 4136514, Re-categorization of CANDU Safety Issue PF12 - Channel Voiding during a Large Loss of Coolant Accident, CNSC Letter, G. Rzentkowski to F. Saunders, May 17, 2013.

[92] E-Doc 4610151, Large LOCA Safety Margins – Assessment of the Proposed Composite Analytical Approach, CNSC Letter, G. Rzentkowski to F. Saunders, January 7, 2015.

[93] COG-10-2010, ITP Recommendations for the CANDU Trip Effectiveness Acceptance Criteria, CANDU Owners Group Report, November 2011.

[94] COG-13-9035-R00, Derived Acceptance Criteria for Deterministic Safety Analysis, November 2014.

[95] COG-02-901, Principles and Guidelines for the Definition and Implementation of the Safe Operating Envelope at CANDU Power Plants in Canada, CANDU Owners Group, March 2003.

[96] DPT-RS-00015-R000, Safe Operating Envelope Gap Assessment, Bruce Power, May 31, 2011.

[97] BP-PROC-00068-R021, Controlled Document Life Cycle Management, Bruce Power, August 22, 2014.

[98] NK29-CORR-00531-10306/e-Doc 3978429, Bruce B: Pilot Type I Inspection of the Bruce Power Safe Operating Envelope, CNSC Letter, R. Lojk to F. Saunders, September 2012.

[99] NK29-CORR-00531-10884, Response to the CNSC Inspection of the Safe Operating Envelope Implementation Program at Bruce B, Bruce Power Letter, F. Saunders to R. Lojk, June 6, 2013.

[100] BP-PROC-00786-R003, Margin Management, Bruce Power, August 5, 2014.

[101] BP-PROC-00638-R012, Temporary Configuration Change Management, Bruce Power, May 7, 2014.

[102] DPT-PDE-00006-R013, Design Plan, Bruce Power, June 26, 2014.

[103] DPT-PDE-00024-R006, Preparation and Revision of Overpressure Protection Reports, Bruce Power, May 6, 2014.

[104] DPT-PDE-00034-R001, Preparation and Revision of System Design Manuals, Bruce Power, June 21, 2007.

[105] BP-PROC-00375-R001, Software Development, Bruce Power, October 7, 2014.

[106] DIV-ENG-00005-R009, Engineering Calculations, Bruce Power, July 30, 2014.

[107] DPT-PDE-00040-R001, Preparation of Instrument Calibration Specifications, Bruce Power, July 29, 2014.

[108] SEC-RSA-00001-R002, Preparation of the EQ Room Conditions Manual, Bruce Power, July 30, 2014.

[109] BP-PROG-10.02-R009, Engineering Change Control, Bruce Power, December 13, 2013.

[110] BP-PROG-10.03-R005, Configuration Management, Bruce Power, January 10, 2014.

[111] BP-PROG-08.01-R007, Emergency Management Program, Bruce Power, December 16, 2013.

[112] NK21-CORR-00531-11379, Bruce Power Progress Report No. 5 on CNSC Action Plan – Fukushima Action Items, Bruce Power Letter, F. Saunders to K. Lafrenière, July 15, 2014.

[113] SOR/2000-203, Radiation Protection Regulations, May 31, 2000.

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

[115] SA-NSAS-2010-01, Safety Report Update Process Effectiveness Review, Bruce Power, 2010.

[116] DPT-NSAS-00004-R004, Guidelines for Managing the Key Deliverables of the Safety Report Analysis Update Process, Bruce Power, September 13, 2011.

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

[118] CAN/CSA N286-05, Management System Requirements for Nuclear Power Plants, February 2005.

[119] NK21-CORR-00531-09689/NK29-CORR-00531-10202/NK37-CORR-00531-01915/e-Doc 3969838, CNSC Desktop Review of Bruce Power's Deterministic Safety Analysis Program, CNSC Letter, R. Lojk to F. Saunders, July 13, 2012.

[120] NK21-CORR-00531-08288/NK29-CORR-00531-09104/NK37-CORR-00531-01629/e-Doc 3630734, Desktop Review of Bruce Power's Deterministic Safety Analysis Program, CNSC Letter, K. Lafrenière to F. Saunders, November 10, 2010.

[121] NK21-CORR-00531-09932/NK29-CORR-00531-10377, CNSC Desktop Review of Bruce Power’s Deterministic Safety Analysis Program, Bruce Power Letter, F. Saunders to R. Lojk, November 29, 2012.

[122] 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

A.1. CNSC G-144, Trip Parameter Acceptance Criteria for the Safety Analysis of CANDU Nuclear Power Plants

This CNSC guideline [36] proposed trip parameter acceptance criteria applicable to slow transients to demonstrate that direct or consequential failures of reactor pressure tube failures due to any fuel failures are precluded. Slow transient events encompass accidents where trip is typically on a process parameter and maintenance of fuel/pressure tube (PT) integrity is based on derived acceptance criteria that limit dryout of the fuel, such as SBLOCA, LOF, and LORC events. The G-144 trip parameter acceptance criteria were:

1. The primary trip parameter predefined limit on each shutdown system should be selected so as to prevent the onset of intermittent fuel sheath dryout; and
2. The backup trip parameters predefined limit on each shutdown system should be selected so as to prevent:
   a) fuel sheath temperature from exceeding 600°C, and
   b) the duration of post-dryout operation from exceeding 60 seconds.

Since this CNSC guidance document was issued, the industry position was that the avoidance of fuel sheath dryout is not a necessary criterion to avoid fuel and pressure tube failures. As a result of this, an Independent Technical Panel (ITP) was established to review the experimental database and provide recommendations on Fuel and Fuel Channel Integrity (F&FCI) acceptance criteria for application to accidents associated with regulatory guide G-144. The recommendations of the ITP for acceptance criteria and for additional experiments that would further support the proposed criteria were documented in the ITP report [93]. Based on the ITP recommendation and a follow-up work, the Safety Analysis Improvement (SAI) Task Team has recently issued the initial version of COG-13-9035 R00 Derived Acceptance Criteria for Deterministic Safety Analysis [94]. This initial version focuses on the acceptance criteria for slow events and intended to replace the requirements of G-144. The derived acceptance criteria for slow events are proposed to be implemented as follows [94]:

1) Pressure tube incremental local or circumferential strain shall not exceed 1%
2) Fuel sheath overstrain shall not exceed 5%
3) The analysis sheath maximum temperature shall not exceed 700°C AND the temperature required to cause local PT strain > 1% on a FE-PT contact.
4) Sheath incremental increase in oxide layer shall not exceed 3 microns
5) $t_{FCM} - t_{DO} \geq (60 + t_{SD})$ seconds

   where,
   i. t_{DO} = time to fuel sheath dryout in seconds
   ii. t_{FCM} = time to fuel centerline melting in seconds
   iii. t_{SD} = required SDS insertion time in seconds.

The proposed maximum sheath temperature of 700°C is to preclude exceeding the 800°C limit on contact between fuel elements, since a bounding value of 100°C was assumed as a potential increase in sheath temperature as a result of such FE-FE contact (Fuel Element – Fuel Element Contact).

In conclusion, the G-144 requirement of no onset of intermittent fuel sheath dryout prior to the primary trip cannot be met for all events. However, this is considered as an acceptable deviation, since G144 requirements are being replaced with new acceptance criteria [94], which are based on the recommendation of a relevant ITP report [93].

A.2. CNSC G-149, Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors

CNSC G-149 [36] provides guidance to licensees in the development, maintenance and use of computer programs used in the design and safety analysis of nuclear power plants and research reactors. This guidance addresses the entire framework of developing a computer code program from code coding, verification, validation, maintenance and documentation.

The current review of G-149 is a high level assessment of G-149 requirements and in particular whether they are covered by CSA 286.7-99 [21]. This high level assessment concludes that all G-149 requirements are encompassed by those of CSA 286.7-99, which is in the operating licence. Accordingly, meeting CSA 286.7-99 requirements will satisfy the intent of G-149 guidance.

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

- BP-PROG-10.01, Plant Design Basis Management [44];
- BP-PROC-00363, Nuclear Safety Assessment, Bruce Power [46];
- DPT-NSAS-00011 Configuration Management on Safety Analysis Software [56]; and
- DPT-NSAS-00013, Guidelines for Managing Reference Data Sets [58].

Moreover, DPT-NSAS-00011, Configuration Management on Safety Analysis Software [56] also indicates its consideration to CNSC G-149 guidance.

The SAI task team of the CANDU industry has established guidelines for performing DSA [27], for conduct of computer code validation [28], and for computer code accuracy assessment [29]. These guidelines were established in compliance with the relevant requirements of CSA N286.7-99 and in consideration with the relevant guidance of CNSC G-149. The Bruce A and Bruce B SRI plan [73] is based on the use of these guidelines.

Appendix B – Clause-by-Clause Assessments Against Relevant Codes and Standards

This appendix presents the clause-by-clause assessments that are performed for this Safety Factor. The ISR Basis Document provides the following compliance categories and definitions for clause-by-clause assessments:

- Compliant (C) – compliance has been demonstrated with the applicable clause;
- Indirect Compliance (IC) – Compliance has been demonstrated with the intent of the applicable clause;
- Acceptable Deviation (AD) – Compliance with the applicable clause cannot be demonstrated; however, a technical assessment has determined that the deviation is acceptable. For this case a detailed discussion and explanation shall be included in the ISR documentation;
- Gap – system design and/or operational improvements may be necessary;
- Guidance: A potential programmatic, engineering, analytical or effectiveness gap found against non-mandatory guidance;
- Relevant but not Assessed (RNA) – The ISR Basis Document defines RNA as "the particular clause provides requirements that are less strenuous than clauses of another standard that has already been assessed". The definition has been broadened to include the guidance portion of clauses in which a gap has already been identified against the requirement;
- Not Relevant (NR) – The topic addressed in the specific clause is not relevant to the safety factor under consideration but may well be assessed under a different Safety Factor; and
- Not Applicable (NA) – The text is not a clause that provides requirements or guidance. Also used if the clause does not apply to the specific facility.

B.1. CNSC REGDOC-2.4.1, Deterministic Safety Analysis

In support of the review tasks listed in Section 5, a detailed assessment of CNSC REGDOC-2.4.1 has been performed in Table B1. This assessment considers the event-specific RD-310 gap analysis submitted to the CNSC (NK21-CORR-00531-10774/NK29-CORR-00531-11155) and addresses differences between RD-310 and CNSC REGDOC 2.4.1 clauses.

Table B1: CNSC REGDOC-2.4.1, Deterministic Safety Analysis

Article No.	Clause Requirement	Assessment	Compliance Category
3	Safety analysis is an essential element of a safety assessment. It is an analytical study used to demonstrate how safety requirements are met for a broad range of operating conditions and various initiating events. Safety analysis involves deterministic and probabilistic analyses in support of the siting, design, commissioning, operation or decommissioning of an NPP. This document focuses on the deterministic safety analysis used in the evaluation of event consequences. PSA and hazard analysis are outside the scope of this document – the requirements for probabilistic safety assessments for NPPs are provided in regulatory document REGDOC-2.4.2, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants* (formerly S-294). The objectives of deterministic analysis are to: 1. confirm that the design of an NPP meets design and safety requirements 2. derive or confirm operational limits and conditions that are consistent with the design and safety requirements for the NPP 3. assist in establishing and validating accident	1. Safety analysis of the effectiveness of the special safety systems and the applicable alternative heat sink systems was performed and is documented in the SR. Some other analyses in support of design and operation would be documented external to the SR, however, stress analysis for Bruce A shield cooling system is not performed to confirm the design and safety requirement (Gap 1). 2. Analyses of some events establishing OLCs were done pre-2001 using legacy codes (Gap 2). 3. Credited operator actions are identified and accident management procedures are not in the SR but documented in the operating manuals. 4. The SR analysis demonstrates that dose limits for DBAs are met and the PRA demonstrates that the plat safety goals are met.	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	management procedures and guidelines 4. assist in demonstrating that safety goals, which may be established to limit the risks posed by the NPP, are met This document identifies high-level requirements for conducting and presenting a safety analysis, taking into account best national and international practices.		
4.	Requirements for Deterministic Safety Analysis	This is not a requirement/guidance clause (this is a title only).	NA
4.1	The licensee is responsible for ensuring that the safety analysis meets all regulatory requirements. The licensee shall: 1. maintain adequate capability to perform or procure safety analysis 2. establish a formal process to assess and update safety analysis, which takes into account operational experience, research findings and identified safety issues	The Management System Manual [BP-MSM-1] assigns responsibility for the Plant Design Basis Management Program [BP-PROG-10-01] to the Engineering Division. The Engineering Division Organizational Manual [DOM-ENG-00001] in turn, delegates the responsibility for the implementation and execution of the Nuclear Safety Assessment Procedure [BP-PROC-00363] to the Nuclear Safety Analysis and Support (NSAS) Department. The organization of NSAS is described in its organization manual [DPM-NSAS-00001]. This manual describes the responsibilities of the functionaries of the department. Section 4.3 of the Quality Assurance of Safety Analysis [DPT-NSAS-00001] specifies the required personnel capability as Staff assigned with the authority and responsibility for NSA will have adequate education, training, experience, supervision and capability to perform their assigned tasks effectively and to understand the importance of assuring nuclear safety. Staff capability records will be maintained. This procedure on Nuclear Safety Assessment (NSA) [BP-PROC-00363], defines the elements, functional requirements, implementing procedures and key responsibilities associated with the NSA process. It states that the objective of NSA is to ensure that all necessary nuclear safety requirements are defined for the actual or proposed design of the plant throughout the design modification process or in addressing emergent issues (e.g., plant ageing) that may affect the design basis or the Safety Report	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	3. establish and apply a formal quality assurance (QA) process that meets the QA standards established for safety analysis in CSA Group N286.7-99, Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants Guidance As stated in this regulatory document, the licensee must maintain adequate capability to perform or procure safety analysis in order to: • resolve technical issues that arise over the life of the plant • ensure the safety analysis requirements are met for the safety analysis developed by the operating organization or procured from a third party A formal process should be established to assess and update the safety analysis to ensure that the safety analysis reflects: • current plant configuration (for existing plants) • current operating limits and conditions (for existing plants) • operating experience, including the experience from similar	basis. [DIV-ENG-00012] procedure defines the processes for initiation and review of NSA to address proposed or planned changes, and emergent issues concerning plant design or operation, or the adequacy of applicable nuclear safety assessments. [BP-PROG-10.01] policy on Plant Design Basis Management was prepared to facilitate satisfaction of N286.7-99 requirements. [DPT-NSAS-00001] states that it satisfies CSA N286-05, Management System Requirements for Nuclear Power Plants. [DPT-NSAS-00011] on Configuration Management of Safety Analysis Software was prepared in consideration of N286.7-99. Although Bruce Power does not perform development or maintenance activities of the safety analysis software, it has acquired the right to use these computer codes from the Hosting Organizations by multiparty or bilateral agreements. As such, this procedure is limited to the description of the processes for use of safety analysis software, requesting software changes to the owner organizations and modification to scripts and utility codes. However, a number of the legacy analyses in the Safety Report are performed with codes (including the models and data) that have not been verified and validated to the requirements of CSA N286.7-99 and therefore is considered a gap against this requirement (Gap 1) Guidance section of this clause: With respect to maintaining adequate capability to perform or procure safety analysis, see discussion on [DPT-NSAS-00001] above. On the formal process to assess and update the safety analysis, Bruce Power procedure [DPT-NSAS-00002] established the Safety Report update process and [DPT-NSAS-00003] documents the guidelines for evaluating and prioritizing Safety Report issues. On execution of safety analysis, DPT-NSAS-00015 states that *"The relevant sections of the Safety Report (SR) and/or Operational Safety Requirements (OSR) and/or Fitness for Service*	

Article No.	Clause Requirement	Assessment	Compliance Category
	facilities • results available from experimental research, improved theoretical understanding or new modelling capabilities to assess potential impacts on the conclusions of safety analyses • human factors considerations, to ensure that credible estimates of human performance are used in the analysis	*Guidelines (FFSG) and/or Life Cycle Management Plan/Technical Basis Assessment (LCMP/TBA) and/or PRA reports shall be consulted during the preparation of an Analysis Plan or TDF to ensure that input values to be used in the analysis do not inadvertently contradict any safety limits already established. Deviations from these limits should be justified and the basis for the new limit explained.”*	
4.2	Events to be Analyzed	This is not a requirement/guidance clause (this is a title only).	NA
4.2.1	The licensee shall use a systematic process to identify events, event sequences, and event combinations (“events” hereafter in this document) that can potentially challenge the safety or control functions of the NPP. The licensee shall also identify events that may lead to fission product releases, including those related to spent fuel pools (also called irradiated fuel bays) and fuel-handling systems. This process shall be based on regulatory requirements and guidance, past licensing precedents, operational experience, engineering judgment, results of deterministic and probabilistic assessments, and any other systematic reviews of the design. The identification of events will include at-power and shutdown states. The deterministic analysis should 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 analysis. Common-cause events affecting multiple reactor units on a site shall be considered. The list of identified events shall be reviewed for completeness during the design and analysis process and modified as necessary. In addition to events that could challenge the safety or control functions of the NPP, safety analysis shall be performed for normal operation.	Section 2.1, Identification of Initiating Events, of Part 3 of the Safety Reports states that all systems and components are reviewed to identify those containing significant quantities of radioactive materials. For each source of radioactive material, it is possible to determine ways in which unplanned release of this material can occur, based on knowledge of the plant processes and past experience in selecting initiating events. This process leads to a comprehensive list of internal initiating events. To complete the list of abnormal events, all combinations of initiating events and compounding failures in the special safety systems and other mitigating systems are identified. However, a systematic event identification process is not well documented and/or demonstrated. Safety analysis for normal operation of operating plant is required only if significant design change or a new operational state is considered (see guidance clause 4.2.2.1). In comparison to [RD-310] corresponding requirement, this requirement of REGDOC-2.4.1 is more specific in including; - Events for spent fuel pools and fuel-handling systems, and - Events for states where the reactor is expected to operate for extended periods of time and that are not covered by the at-power and shutdown analysis. - Common-cause events affecting multiple reactor units on a site. For the first bullet above, spent fuel pool and fuel handling system	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	Guidance The safety analysis is performed for a set of events that could lead to challenges related to the NPP's safety or control functions. These include events caused by SSC failures or human error, as well as human-induced or natural common-cause events. The events considered in safety analysis could be single PIEs, sequences of several consequential events, or combinations of independent events. The set of events to be considered in safety analysis is identified using a systematic process and by taking into account: • reviews of the plant design using such methods as hazard and operability analysis, failure mode and effects analysis, and master logic diagrams • lists of events developed for safety analysis of other NPPs, as applicable • analysis of operating experience data for similar plants • any events prescribed for inclusion in safety analysis by regulatory requirements(e.g., REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants)	accidents are included in the Safety Report. For the second bullet above, DSA scope for DBAs is usually performed up to establishing long term heat sink. PRA event tree considers the availability of long term heat sink and DSA for BDBAs is within the scope of PRA Level 2 to support the evaluation of plant safety goals. For the third bullet above, natural common cause events are not addressed in the Safety Report (Gap 1). It is being considered in the first phase of REGDOC-2.4.1 implementation. Guidance section of this clause: - Events initiated as a result of human errors are not explicitly identified in the Safety Report. PRA Initiating event frequency include implicitly any relevant operator error that may cause the initiating event (Gap 2). The specified elements to be considered in event identification or all applicable modes of operation are not comprehensively covered (Gap 3).	

Article No.	Clause Requirement	Assessment	Compliance Category
	• equipment failures, human errors and common-cause events identified iteratively with PSA • a cut-off frequency for common-cause events that is consistent across all events The list of identified events should be iteratively reviewed for accuracy and completeness as the plant design and safety analyses proceed. Reviews should also be periodically conducted throughout the NPP lifecycle, to account for new information and requirements. This regulatory document requires that, when identifying events, all permissible plant operating modes be considered. All operating modes used for extended periods of time should be analyzed. Modes that occur transiently or briefly can be addressed without a specific analysis, as long as it can be shown that existing safety analyses bound the behaviour and consequences of those states. NPP operating modes include, but are not limited to: • initial approach to reactor criticality • reactor start-up from shutdown through criticality to power • steady-state power operation, including both full and low power • changes in the reactor power level, including load follow modes (if employed) • reactor shutting down from power operation • shutdown in a hot standby mode • shutdown in a cold shutdown mode • shutdown in a refuelling mode or maintenance mode that opens major closures in the reactor coolant pressure boundary • shutdown in other modes or plant configurations with unique temperature, pressure or coolant inventory conditions • operation of limited duration, with some systems important		

Article No.	Clause Requirement	Assessment	Compliance Category
	to safety being unavailable For events identified by the systematic process used for this purpose, a full range of configurations and operating modes of equipment should be considered in the deterministic safety analysis. Special plant configurations may occur during major plant modifications such as plant refurbishment, lay-up, or decommissioning. These configurations should be considered, and potential events should be identified and included in the deterministic safety analysis.		
4.2.2	The list of events identified for the safety analysis shall include all credible: 1. component and system failures or malfunctions 2. operator errors 3. common-cause internally and externally initiated events, including those affecting multiple reactor units on a site A cut-off frequency shall be selected so that events with a frequency of occurrence less than the cut-off limit provide only a negligible contribution to the overall risk posed by the NPP. The elimination of such events from the analysis scope shall be justified and the reasons for eliminating them documented.	1. The list of PIEs provided in Table 2-1 of Part 3 of the Safety Report covers component and system failures or malfunctions. However, the limiting case with respect to RRS working or failed has not been demonstrated for all events (e.g. Small LOCA) and therefore is considered a gap against this requirement (Gap 1) 2. Although some PIEs listed in Table 2-1 of Part 3 of the Safety Report may be attributable to operator errors, this category of PIEs has not been explicitly identified (Gap 2). 3. Although some common-cause internally and externally initiated events form part of the design basis for the plant, these have not been explicitly addressed in the deterministic safety analysis (Gap 3). Events with a frequency of occurrence less than a cut-off limit are not explicitly identified or justified, however the deterministic safety analysis is supplemented with a probabilistic analysis that extends to low cut-off frequency and therefore is not considered a gap against this requirement, this is considered indirectly compliant.	Gap
4.2.2.1	During the design phase, the normal plant operation is analyzed as a separate class of event. This allows sources of radiation or releases of radioactive materials to be assessed in various modes of operation or transition between modes. For an existing plant, a safety analysis for normal operation may be	This is a guidance clause recommending to perform safety analysis for normal operation of operating plant only if significant design change or a new operational state is considered. Since neither is the case, no gap against this guidance clause.	C

Article No.	Clause Requirement	Assessment	Compliance Category
	required if a new operational mode is considered, or if significant design changes (any changes that may alter system characteristics) are implemented.		
4.2.2.2	SSC failures may include failure to operate when required, erroneous operation and partial failures. Events to be considered include: • failures or malfunctions of active systems, such as pumps, valves, control systems or power supply • failures of passive systems, such as breaks in the reactor's pressure-retaining boundaries, including pipes and rupture discs	This is a guidance clause and there is no gap against it since the considered events include both malfunctions of active systems and failures of passive systems.	C
4.2.2.3	As initiating events, operator errors normally produce the same results as events caused by equipment failure. Therefore, they do not need to be considered separately in the models and computer codes for deterministic safety analysis. However, the generic implications of human errors as initiating events should be considered to identify any further potential system failures. As such, if a specific operator error could result in a unique initiating event, it should be included in the list of PIEs for the deterministic safety analysis.	This is a guidance clause. Although some PIEs listed in Table 2-1 of Part 3 of the Safety Report may be attributable to operator errors, this category of PIEs has not been explicitly identified. See clause 4.2.2 item (2). Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	RNA
4.2.2.4	Common-cause events are multiple component failures that can be initiated by internal and external events (these events could be human-induced or naturally occurring). Internal common-cause events include fires, floods of internal origin, explosions, and equipment failures (such as turbine breakup) that may generate missiles. External, naturally occurring events (triggers for plant equipment failures) that are considered in deterministic safety analysis include: • earthquakes • external fires • floods/tsunamis occurring outside the site • biological hazards (for instance, mussels or seaweed	This is a guidance clause. Although some common-cause internally and externally initiated events form part of the design basis for the plant, these have not been explicitly addressed in the deterministic safety analysis. See clause 4.2.2 item (3). Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	affecting cooling water flow and/or temperature) • extreme weather conditions (temperature, precipitation, high winds, tornadoes etc.) External initiating events may cause internal and/or external events. For example, an earthquake could lead to plant equipment failures, loss of offsite power, flood, tsunami or fire. External events may cause accidents in one or more of the units where there are multiple units at a site. Human-induced external events that are considered in deterministic safety analysis include: • aircraft or missile impacts • explosions at nearby industrial facilities or transportation systems • release of toxic or corrosive chemicals from nearby industrial facilities or transportation systems • electromagnetic interference		
4.2.2.5	Combinations of events (which may occur either simultaneously or sequentially while restoring the plant to a stable state) should be considered. Types of combinations include: • multiple independent failures in equipment important to safety • failure of a process system and system important to safety • multiple process system failures • equipment failures and operator errors • common-cause events and operator errors Examples of event combinations include: • loss of coolant with subsequent loss of station electrical	This is a guidance clause. Combinations of initiating events and compounding failures in the special safety systems and other mitigating systems are identified and analyzed in the Safety Report, however, not all types of event combinations indicated in this guidance clause have been considered. See clause 4.2.2. Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	power, including station blackout • loss of coolant with loss of containment cooling • small loss-of-coolant accidents (LOCAs) with failure of primary or secondary depressurization • main steam line break with failure of the operator to initiate a backup cooling system		
4.2.2.6	Many events will be identified by following the aforementioned guidance, although it may not be practical or necessary to analyze all of these events. The identified events could be grouped into categories based on similarity of the initiating failures, key phenomena, or system and operator responses. Examples of event categories include decrease of the reactor coolant inventory, reactivity and power anomalies, and increase/decrease of heat removal. Since plant responses to an event depend on the design and availability of plant systems, the most suitable classification of events may vary. In the safety analysis of AOOs and DBAs for Level 3 defence in depth, bounding events should be identified for each applicable acceptance criterion within each category of events. In some cases, one accident scenario in the same category of events may be more severe in terms of one acceptance criterion (for example, containment pressure limit) and another may be more severe in terms of a different acceptance criterion (for example, public doses). All these scenarios should be considered in the safety analysis process as bounding events for different acceptance criteria.	This is a guidance clause. Although the intent of this clause in grouping the events based on the similarity in their characteristics and dominant phenomena is met, the events are not grouped into AOO, DBA and BDBA. See clause 4.2.2. Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	RNA
4.2.2.7	An event may be divided into sub-events for consideration in safety analysis, when there are substantial differences between the subdivided events, such as: • phenomena occurring at the plant in response to the events • challenges to safety and systems important to safety • frequencies For example, LOCAs are commonly sub-divided into small-break	This is a guidance clause. Subdivision of the events in the Safety Report complies with this clause.	C

Article No.	Clause Requirement	Assessment	Compliance Category
	LOCAs and large-break LOCAs because of significant differences in phenomena and challenges to the safety system. An event should not be sub-divided without sufficient justification, for the purpose of reclassifying one of the resulting sub-events from an AOO to a DBA, or from a DBA to a BDBA, or for the purpose of attaining a frequency below the cut-off frequency limits used in PSA.		
4.2.2.8	When beginning to identify events, both those of low frequency (including earthquakes with consequential tsunamis) and those of minor consequences should be included. In defining the scope of events to be analyzed, the deterministic safety analysis should select the same cut-off frequency as that used in the probabilistic analysis for the same facility. This frequency is chosen so the deterministic analysis can be integrated with the probabilistic analysis. Some events may be excluded from the detailed consideration (for example, because of their negligible contribution to exceeding the safety goals, or because they are bounded by an analyzed event). Such exclusion should be fully justified and the reasons well documented.	This is a guidance clause. Combinations of external hazards were considered in hazard screening. DSA for severe accidents are within the PRA scope. Regarding the guidance clause on cut-off frequency, the intent of the clause is to better integrate the DSA of BDBAs with PRA. This would be achieved by ensuring that all potential BDBAs within the PRA cut-off frequency are covered. See clause 4.2.2. Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	RNA
4.2.3	The identified events shall be classified, based on the results of probabilistic studies and engineering judgment, into the following three classes of events: 1. anticipated operational occurrences : these include all events with frequencies of occurrence equal to or greater than 10^{-2} per reactor year 2. design-basis accidents : these include events with frequencies of occurrence equal to or greater than 10^{-5} per reactor year, but less than 10^{-2} per reactor year 3. beyond-design-basis accidents : these include events with frequencies of occurrence less than 10^{-5} per reactor year Notes: • in accordance with REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants, the subset of BDBAs considered in	At present, the deterministic safety analysis does not distinguish between these three classes of events. The focus of the Safety Report is primarily on design basis events, which include design basis accidents and AOOs. The specific event classification scheme has not been followed for deterministic safety analysis (Gap 1). The definition of design extension conditions (DECs), the classification of events that are at the border between two classes, and the scope of BDBA extending to beyond DECs are recognized in the COG guidelines for DSA [COG-09-9030]. The requirement for the analysis of DECs is introduced in REGDOC-2.5.2. Bruce A design predates this REGDOC, however some of the analyzed events considered in the design basis and included in the Safety Report would be classified as BDBA according to the classification scheme of REGDOC-2.4.1. DSA for BDBAs are primarily	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	the design of a new NPP is referred to as design-extension conditions (DECs) • DECs do not replace BDBAs in most occurrences in REGDOC-2.4.1, since analysis will consider events of lower frequency than DECs; for example, in searching for cliff-edge effects, or in analyzing bounding events Other factors to be considered in the event classification are any relevant regulatory requirements or historical practices. Events with a frequency on the border between two classes of events, or with substantial uncertainty over the predicted event frequency, shall be classified into the higher frequency class. Credible common-cause events shall also be classified within the AOO, DBA and BDBA classes. Guidance Events are classified because each plant state has different safety analysis requirements and acceptance criteria. Safety analysis requirements reflect the level of protection in accordance with the principle of defence in depth. The normal plant states and accident conditions are considered in the safety analysis. Events are classified as follows: • AOOs: events that are more complex than the normal operation manoeuvres, with the potential to challenge the safety of the reactor, and which might be reasonably expected to happen during the lifetime of a plant • DBAs: events that are not expected to occur during the lifetime of a plant but, in accordance with the principle of defence in depth, are considered in the design of the NPP; however, certain groups of events with lower frequency may also be included in the plant design basis • BDBAs: events with low probabilities of expected occurrence, which may be more severe than DBAs, and – due to multiple failures and/or operator errors – may result in safety systems that fail to perform their safety functions, leading to significant core damage, challenges to the integrity of the containment barrier, and,	analyzed within PRA Level 2 scope to support the assessment of plant safety goals and does not normally include an assessment to search for cliff edge effects (Gap 2). Common-cause events not classified since they are not covered in the Safety Report. They are planned to be covered in the first stage of REGDOC-2.4.1. The recommended classification for events near the border between two event classes into the higher class and consideration of the uncertainty in the event frequency in event classification is not followed. It will be considered in REGDOC-2.4.1 implementation. Guidance The guidance allows for considering a short duration of an operation mode in specifying relevant event classification on a case-by-case basis. This is new statement compared to the corresponding [RD-310] clause requirement. Gaps in the guidance are similar to those in the clause requirements.	

Article No.	Clause Requirement	Assessment	Compliance Category
	eventually, to the release of radioactive material from the plant Plant states include operational states (normal operation and AOOs) and accident conditions (DBAs and BDBAs). However, as established in REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants, the design authority establishes the plant design envelope, which is the subset of all plant states considered in the design: normal operation, AOOs, DBAs and DECs (see figure 1). Figure 1: Plant states The assessed frequency of occurrence is the basis for event classification, but it is recognized that such assessments may be characterized by significant uncertainty. Therefore, an event with a predicted frequency that is on the threshold between two classes of events, or with substantial uncertainty in the predicted event frequency, is classified into the higher frequency class. Other factors, such as relevant regulatory requirements or historical practices, may affect the selection of certain events for inclusion. In order to establish an understanding of margins of safety or the robustness of the design, the regulatory authority may request that certain events be analyzed as design-basis accidents, or as representative severe accidents. Past practices and experience may indicate that certain scenarios are more critical and should be analyzed as DBAs. Some plant operating modes may be used only for short periods of time. Normally, events are classified without regard to the frequency of these operating modes. However, in classifying events, frequency of operating modes may be considered on a case-by-case basis. Examples of events of different classes based on CANDU experience are provided in Appendix A. These illustrate possible outputs of the event identification and classification process described in section 4.2. This list is for illustration only, and is not meant to be comprehensive. It should be noted that, in practice, such a list would normally be generated by probabilistic methods. The list will be subject to grouping of events (see section 4.2.2.6). It is expected that only representative or bounding events for each group of events would be analyzed.		

Article No.	Clause Requirement	Assessment	Compliance Category
4.2.3.1	Plant design is expected to be sufficiently robust, such that most AOOs would not require the initiation of safety systems to prevent consequential damage to the plant's SSCs. This is part of Level 2 defence in depth, and helps to ensure that events requiring use of safety systems are minimized. The plant control systems are expected to compensate for the event's effects and to maintain the plant in a stable state long enough for an operator to intervene. The operator intervention may include, if deemed necessary, activation of safety systems and plant shutdown according to established procedures. After addressing the initiating event, it should be possible to resume plant operations. For Level 3 defence in depth, in addition to meeting the above expectations for Level 2 defence in depth, the design is also expected to demonstrate with high confidence that safety systems can mitigate all AOOs without the assistance of plant control systems. Examples of AOOs include those in table 1, which provides examples for a CANDU reactor anda light-water reactor (LWR). The following list in table 1 is not exhaustive; a complete list would depend on the type of reactor and the design of the plant systems. Table 1: Examples of anticipated operational occurrences	This is a guidance clause. - Most of the analyzed events, that will be classified as AOOs, would not require the initiation of safety system (i.e. Level 2 of Plant Defence-in-Depth can be demonstrated). - Level three defence-in-depth is demonstrated for all single failure events that are analyzed in the Safety Report, including those that would be classified as AOOs. However, systematic event identification and event classifications into AOOs, DBAs and BDBAs have not been followed in the Safety Report and accordingly Level 3 defence-in-depth for all AOOs has not been demonstrated. See clause 4.2.3. Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	RNA
4.2.3.2	The events leading to DBAs are classified based on the estimated frequencies of equipment failures, operator errors or common-cause events. All the events identified as initiators of AOOs should also be considered as potential initiators for DBAs, given the relatively high likelihood of AOOs and the possibility of additional equipment failures or operator errors. Examples of DBAs include those in table 2, which provides examples for CANDU reactors, pressurized water reactors (PWRs) and other LWRs. The following list in table 2 is not exhaustive. A complete list of DBAs would depend on the type of reactor and actual design. Table 2: Examples of design-basis accidents	This is a guidance clause. The recommended classification scheme has not been followed in the Safety Report, see Gap against clause 4.2.3. Level 3 defence-in-depth for all AOOs has not been demonstrated. See clause 4.2.3. Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	RNA
4.2.3.3	PSA allows systematic identification of event sequences leading to	This is a guidance clause.	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	challenges to the fundamental safety functions. Representative event sequences are then analyzed using deterministic safety analysis techniques to assess the extent of fuel failures, damage to the reactor core, primary heat transport system and containment, and releases of radionuclides. The use of any cut-off limit for the frequency of occurrence of analyzed BDBAs should consider the safety goals established for the plant and be consistent with the safety analysis objectives. Examples of BDBAs include: • complete loss of the residual heat removal from the reactor core • complete loss of electrical power for an extended period This class of events also includes massive failures of pressure vessels. Some massive failures of pressure vessels can be exempted from the deterministic safety analysis, if it can be demonstrated that these failures are sufficiently unlikely, and if all the following conditions are satisfied: • the vessel is designed, fabricated, installed, and operated in compliance with the nuclear requirements of the applicable engineering codes and other requirements • an in-service inspection program is implemented • operating experience, with vessels of similar design and operating condition, support a low likelihood of failure • the vessel has adequate restraints to limit propagation of damage to the plant Note: Although the CANDU heat transport system header is considered a vessel, its failure should be postulated in the safety analysis. Events that have been excluded from the DBA analysis based on leak-before-break methodology are to be considered in the BDBA sequences. For example, any large LOCA or main steam line break that may have been excluded from the design basis accident set	Bruce A approach for PRA and DSA are consistent with the intent of this guidance clause. DSA for BDBAs for PRA Level 2 is specifically performed with an objective to assess the plant safety goals.	

Article No.	Clause Requirement	Assessment	Compliance Category
	should be considered for the BDBA analysis.		
4.3	Acceptance criteria are established to serve as thresholds of safe operation in normal operation, AOOs, DBAs and, to the extent practicable, for BDBAs. The limits and conditions used by plant designers and operators should be supported by adequate experimental evidence, and be consistent with the safety analysis acceptance criteria as described in sections 4.3.1 to 4.3.4.	Section 1.5, Acceptance Criteria, of Part 3 of the Safety Report addresses radiological doses and derived acceptance criteria for DBAs but not explicitly for AOOs, since the limits for AOOs are currently taken to be the same as for DBAs. No reference to BDBA acceptance criteria or safety goals in the Safety Report (Gap 1). Bruce A operating limits and conditions are based on their relevant and bounding safety analysis as established in the OSRs.	Gap
4.3.1	Analysis for normal operation of the NPP, performed during the design phase, shall demonstrate that: 1. radiological doses to workers and members of the public are within the limits acceptable to the CNSC 2. releases of radioactive material into the environment fall within the allowable limits for normal operation Guidance The deterministic safety analysis for normal operation should: • verify the set points of the safety systems, to demonstrate that their initiation would occur only when needed • verify that process controls and alarms are effective in reducing (or avoiding) the need for safety system actions • address all NPP conditions under which systems and equipment are operated as expected, with no internal or external challenges, including all the operational configurations for which the NPP was designed to operate in the course of normal operations over its life, both at power and at shutdown	1. Section 1.4, Derived Release Limits, of Part 1 of the Safety Report addresses radiological doses and releases of radioactive material under normal operation in accordance with the Radiation Protection Regulations under the Act [Nuclear Safety and Control Act]. 2. Bruce A meets the allowable limits for normal operation. Guidance section of this requirement clause: The intent of all guidance elements identified in this section are met.	C
4.3.2	Analysis for AOOs and DBAs shall demonstrate that: 1. radiological doses to members of the public do not exceed the	1. Dose does not exceed the Single Failure dose limit. Events that will be classified as AOOs are expected to meet AOO dose limit. 2. Gap with respect to the requirement of experimental support	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	established limits 2. the derived acceptance criteria, established in accordance with section 4.3.4 are met Guidance The aim of safety analysis for AOOs and DBAs is to demonstrate the effectiveness of the following key safety functions: • controlling the reactor power, including shutting down the reactor and maintaining it in a shutdown state • removing heat from the core • preserving the integrity of fission product barriers • preserving component fitness for service for AOOs • ensuring that the consequences of radioactive releases are below the acceptable limits • monitoring critical safety parameters Acceptance criteria for AOOs and DBAs should include: • acceptance criteria that relate to doses to the public • derived acceptance criteria that relate to the protection of the defence-in-depth physical barriers (see section 4.3.4 and Appendix B for examples) The committed whole-body dose for average members of the critical groups who are most at risk, at or beyond the site boundary, is calculated in the deterministic safety analysis for a period of 30 days after the analyzed event. This dose is less than or equal to one of the following dose acceptance criteria: • 0.5 millisievert for any AOO	and demonstrating that safety margin is sufficient with accounting for uncertainties (See 4.3.4 compliance discussion) (Gap 1). Guidance section of this requirement clause: - The guidance clause on the aim of safety analysis is complied with. - Comprehensiveness of acceptance criteria to include those for dose and protecting defence-in-depth barriers are complied with. - Calculation of dose for average member of the critical groups who are most at risk, at or beyond the site boundary for a period of 30 days after the analyzed event is followed in the analysis of Part 3 of the Safety Report. - Dose limits of 0.5 mSv and 20 mSv are not used in the analysis of Part 3 of the Safety Report. Single Failure (SF) and Dual Failure (DF) limits of 5 mSv and 250 mSv respectively are used. Note that the guidance indicate that the AOO and DBA dose limits of 0.5 mSv and 20 mSv apply to new NPPs while for existing reactors the dose limits specified in the operating licences must be met. - Dose calculations of Part 3 of the Safety Report are not completely consistent with the guidance in Section 4.4.4.7 (Gap 2). - The analysis of Part 3 of the Safety Report complies with the guidance of having more stringent criteria than those for the class of events with lower frequencies of occurrence. - Guidance on specific assumptions related to crediting passive functions of containment system in AOOs dose calculation cannot be assessed since AOOs are not separately analyzed in Part 3 of the Safety Report (Gap 3). - Quantitative acceptance criteria of Part 3 of the Safety Report are based on direct physical evidence and well-understood phenomena, but accounting for uncertainties is not demonstrated (Gap 4).	

Article No.	Clause Requirement	Assessment	Compliance Category
	• 20 millisieverts for any DBA These dose limits apply to new NPPs. For existing reactors, the dose limits specified in the operating licences must be met. Note: New NPPs referenced in this section are effectively those first licensed after the issuance of RD-337, Design of New Nuclear Power Plants, in 2008. To demonstrate that the radiological consequences of an analyzed event do not exceed the limits, the doses should be calculated according to the guidance in section 4.4.4.7. Acceptance criteria for the class of events with higher frequencies of occurrence should be more stringent than those for the class of events with lower frequencies of occurrence. To demonstrate compliance with the public dose acceptance criteria for an AOO, the automatic isolation and pressure suppression functions of the containment system should not be credited, since these functions are normally considered part of Level 3 defence in depth. However, the containment passive barrier capability and normally operating containment subsystems could be credited, if they are qualified for the AOO conditions. Derived acceptance criteria have two components: qualitative and quantitative. Quantitative acceptance criteria should be developed, based on direct physical evidence and well-understood phenomena, and should account for uncertainties. Regarding the qualitative acceptance criteria (such as the examples provided in Appendix B), the following guides are applied only to AOOs: • the qualitative acceptance criteria should be satisfied without reliance on the automatic function of the safety systems, for a wide range of AOOs. The plant control systems should normally be able to correct transients and prevent damage to the plant's SSCs • the control systems should be able to maintain the plant in a stable operating state for a sufficiently long time, to allow the operator to diagnose the event, initiate required actions and, if necessary, shut	- Compliance with the guidance on qualitative acceptance criteria for AOOs cannot be assessed since the analysis in Part 3 of the Safety Report does not consider AOOs separately. However, it is expect that most of the guidance elements can be demonstrated (Gap 5). - The frequency of some Dual Failure events in Part 3 of the Safety Report is less than 10^{-5} per reactor year and the dual failure dose limit is used.	

Article No.	Clause Requirement	Assessment	Compliance Category
	the reactor down while following the applicable procedures • even though control systems may be shown to maintain the plant in a safe state following an AOO without the initiation of safety systems (Level 2 defence in depth), it should also be shown with high confidence, for all AOOs, that the safety systems can also mitigate the event without beneficial actions by the control systems (Level 3 defence in depth) Certain accidents with predicted frequency of occurrence less than 10^{-5} per reactor year could be used as the design basis event for a safety system. In this case, DBA dose limits should still be met, and the analysis should also consider meeting qualitative acceptance criteria relevant to this particular safety system. The safety system performance margins should be sufficient to ensure that the DBA dose limits are met.		
4.3.3	A safety assessment for BDBAs shall be performed to demonstrate that: 1. the NPP as designed meets the requirements for release limits established as the safety goals; a deterministic safety analysis provides consequence data for accident sequences to use in the PSA 2. the procedures and equipment put in place to handle the accident management needs are effective, taking into account the availability of cooling water, material and power supplies; consideration can be given to the plant's full design capabilities, including the possible use of safety, non-safety, and temporary systems beyond their originally intended function. Guidance The deterministic and probabilistic safety assessment should demonstrate that the Level 4 defence in depth prevents or mitigates the consequences of BDBAs (including severe accidents,) as described in REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants. The BDBA deterministic analysis addresses a set of representative sequences, in which the safety systems have malfunctioned and some of the barriers to the release of radioactive material may have failed, or have been bypassed. The accident	Deterministic safety analysis is used in support of PRA to perform consequence analysis for BDBAs and the evaluation of the plant safety goals and limits. Post Fukushima actions includes design modifications and enhancement to improve the plant response under severe accidents in particular through providing alternative emergency sources of water and electrical power supplies to ensure the adequacy and availability of heat sinks. PRA assessments taking into account Emergency Mitigation Equipment demonstrate significant improvements in SCDF and releases (see SFR6 for details). Guidance section of this clause: Bruce A PRA complies with or meets the intent of the guidance statements on the considered representative BDBAs and the aim of safety analysis of BDBAs. Most of the representative BDBAs that are analyzed deterministically were not part of the design basis of Bruce A. However, their analyses are used to support PRA to demonstrate meeting Bruce A safety goals.	C

Article No.	Clause Requirement	Assessment	Compliance Category
	sequences for analysis should be relevant and representative with respect to the objective of the analysis. In other words, representative BDBAs can be selected among the dominant accident sequences from the probabilistic safety assessment, or by adding safety system failures or incorrect operator responses to the DBA sequences. In general, the results of the PSA studies can be used for this purpose, if they are applicable. The aim of safety analysis for BDBAs is to: • evaluate the ability of the design to withstand challenges posed by BDBA and to identify plant vulnerabilities • assess the effectiveness of those design features which were incorporated in the plant design for the specific purpose to reduce the likelihood and/or mitigate the consequences of BDBAs, (including the assessment of equipment for accident management and instrumentation to monitor the accident) • evaluate the ability to restore and maintain the safety functions using alternative or diverse systems, procedures and methods, including the use of non-safety-grade equipment • assist in the development of an accident management program for BDBAs and severe accident conditions • provide input for offsite emergency planning For events where there are multiple units at a site, as well as for single-unit events, the capacity of essential cooling and power supplies should be evaluated. The design for BDBAs is aimed to meet risk criteria such as safety goals related to frequency of severe core damage and significant releases of radioactivity, as assessed by PSA. Deterministic calculations of the source terms for BDBAs can also be performed in accordance with the aim of the BDBA analysis. These calculations should demonstrate, for example, that: • containment failure will not occur in the short term following a severe accident (seeREGDOC-2.5.2, Design of Reactor Facilities:	Containment failure in the short term following the BDBAs considered within the PRA is not predicted.	

Article No.	Clause Requirement	Assessment	Compliance Category
	Nuclear Power Plants) • the public is 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		
4.3.4	Qualitative acceptance criteria shall be established for each AOO and DBA to confirm the effectiveness of plant systems in maintaining the integrity of physical barriers against releases of radioactive material. These qualitative acceptance criteria shall satisfy the following general principles: 1. avoid the potential for consequential failures resulting from an initiating event. 2. maintain the structures, systems and components in a configuration that permits the effective removal of residual heat. 3. prevent development of complex configurations or physical phenomena that cannot be modelled with high confidence. 4. be consistent with the design requirements for plant systems, structures and components. To demonstrate that these qualitative acceptance criteria applicable to the analyzed AOO or DBA are met, quantitative derived acceptance criteria shall be identified prior to performing the analysis. Such derived acceptance criteria shall be supported by experimental data. The results of safety analysis shall meet appropriate derived acceptance criteria with margins sufficient to accommodate uncertainties associated with the analysis. The analysis shall be performed for the event that poses the most challenges in demonstrating the meeting of derived acceptance criteria (i.e., the limiting event in an event category). Guidance In addition to the dose limits in section 4.3.2, the acceptance criteria for AOOs and DBAs also include a set of derived acceptance criteria, such as those examples of qualitative acceptance criteria identified in	Section 1.3, Designing for Reliability and Safety, of Part 2 of the Safety Report addresses the qualitative criteria in maintaining the integrity of physical barriers in terms of accident prevention and accident mitigation. 1-The criteria established in Section 1.3, Designing for Reliability and Safety, of Part 2 of the Safety Report, meet these requirements. 2- Section 1.5, Acceptance Criteria, of Part 3 of the Safety Report specifies quantitative derived acceptance criteria for maintaining fuel and fuel channel integrity that permits the effective removal of residual heat. 3- Emergency Operating Procedures (EOPs) are intended to identify design provisions and operator actions required to prevent event progression from defence-in-depth Level 3 to 4. Complex configurations are bounded by simpler more limiting analyzed configurations generally within the analyses documented in the appendices of Part 3 of the Safety Report or by adopting a more restrictive acceptance criteria selected specifically to avoid complex configuration. This is considered as indirect compliance. 4- This practice has been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report. The acceptance criteria are not systematically supported by experimental data (Gap 1). The results of safety analysis has not been shown systematically to meet quantitative acceptance criteria with margins sufficient to accommodate uncertainties associated with the analysis (Gap 2). The analysis is performed for the limiting event in an event category for each applicable acceptance criterion.	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	appendix B. These acceptance criteria are established by the designer to limit the damage to different defence barriers. Compliance with these requirements ensures that there are physical barriers preserved to limit the release of radioactive material and prevent unacceptable radiological releases following an AOO or DBA. The failure to meet a derived acceptance criterion does not necessarily mean that dose limits will be exceeded. However, if the derived acceptance criteria are met with significant margin, then the dose calculation can be simplified, because fission product releases are expected to be limited. The derived acceptance criteria are generally more stringent for events with a higher frequency of occurrence. For example, for most AOOs, the actions of the control systems should be able to prevent consequential degradation of any of the physical barriers to the extent that the related SSCs are no longer fit for continued service (including fuel matrix, fuel sheath/fuel cladding, reactor coolant pressure boundary or containment). More demanding requirements may be set to demonstrate the availability of a margin between the predicted value and the quantitative acceptance criteria, or to simplify an analysis (for example, to avoid having to perform complex modelling). The conditions of applicability for each additional criterion should be clearly identified. For each of the qualitative acceptance criteria, as illustrated in appendix B, quantitative acceptance criteria (or limits) should be established. These quantitative limits should: • be applicable to the particular NPP system and accident scenario • provide a clear boundary between safe states (when failure of an SSC is prevented with high confidence,) and unsafe states (when a failure of an SSC may occur) • be supported by experimental data • incorporate margins or Safety Factors to account for	Guidance clauses are mainly complied with except; - A more conservative quantitative acceptance criterion has not been selected in some cases where qualified models with high confidence does not exist (e.g., for events with fuel sheath temperatures exceeding 1500 C (Gap 3). - Incorporation of margins or Safety Factors to account for uncertainty in experimental data and relevant models has not been systematically demonstrated in selecting the quantitative acceptance criteria (Gap 4).	

Article No.	Clause Requirement	Assessment	Compliance Category
	uncertainty in experimental data and relevant models When there is insufficient data to identify the transition from a safe state to an unsafe state, or to develop accurate models, then the quantitative limit for the corresponding safety requirement should be set at the boundary of the available data, provided that the established limit is conservative.		
4.4	Methods and Assumptions for Deterministic Safety Analysis	This is not a requirement/guidance clause (this is a title only).	NA
4.4.1	The analysis shall provide the appropriate level of confidence in demonstrating conformity with the acceptance criteria. To achieve the appropriate level of confidence, the safety analysis shall: 1. be performed by qualified analysts in accordance with an approved QA process 2. apply a systematic analysis method 3. use verified data 4. use justified assumptions 5. use verified and validated models and computer codes 6. build in a degree of conservatism 7. be subjected to a review process Guidance Section 4.4 mainly addresses analysis methods and assumptions for the deterministic safety analysis of AOOs and DBAs for Level 3 defence in depth. Similar analysis methods and assumptions can be applied for Levels 2 and 4 defence in depth (with appropriate levels of conservatism). Certain conservative rules, such as the single-failure criterion, are not applied in Level 2 and Level 4 analyses. The safety analyst has the option of selecting safety analysis methods and assumptions, as long as the regulatory requirements and expectations are satisfied.	1. This procedure on Quality Assurance of Safety Analysis [DPT-NSAS-00001] specifies the QA process for deterministic safety analysis and includes requirements for personnel under Section 4.3 on Personnel Capability. 2. [DPT-NSAS-00015] procedure on Execution of Safety Analysis outlines the systematic methodology for conducting safety analysis. 3. The verification of the legacy analysis does not meet current standards (Gap 1). [DPT-NSAS-00013] procedure on Guidelines for Managing Reference Data Sets ensures that only verified datasets are used for deterministic safety analysis. 4. For legacy analysis of small LOCA and transition breaks analysis assumptions (such as RRS control working) should be justified (Gap 2). This practice has been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report. 5. Not all of the existing analyses have used validated models and computer codes that would meet the current standards (Gap 3). 6. For some legacy analysis of small LOCA, Feedwater and Steam Supply System Failures, and Electrical System Failures not all key operating and safety system parameters are simultaneously assumed at SOE limits (Gap 4). 7. This procedure on Execution of Safety Analysis [DPT-	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	The selection of the safety analysis methods and assumptions should be such that the appropriate level of confidence can be achieved in the analysis results.	NSAS-00015] outlines the review process for safety analyses. Guidance clauses recommend that single failure criterion is not applied to Level 2 and Level 4 defence-in-depth. This is less restrictive requirement for Level 2 of AOOs and BDBA events, however, DSA in the Safety Report does not distinguish between AOO and DBA and does not address BDBAs explicitly.	
4.4.2	The analysis method shall include the following elements: 1. identifying the scenarios to be analyzed as required to attain the analysis objectives 2. identifying the applicable acceptance criteria, safety requirements, and limits 3. identifying the important phenomena of the analyzed event 4. selecting the computational methods or computer codes, models, and correlations that have been validated for the intended applications 5. defining boundary and initial conditions 6. conducting calculations, including: a. performing sensitivity analysis and identifying, where necessary, margins to cliff-edge effects b. analyzing the event from the initial steady state up to a predefined long-term stable state, considering the guidance for duration in section 4.4.2.6 7. accounting for uncertainties in the analysis data and models 8. verifying calculation results for physical and logical consistency 9. processing and documenting the results of calculations to demonstrate conformance with the acceptance criteria Guidance The basic elements included in the safety analysis method are described in sections 4.4.2.1 to 4.4.2.9. There are three main analysis	[DPT-NSAS-00015] on Execution of Safety Analysis provides a clear guidance on the framework of the safety analysis process consistent with the requirements of this clause with the exception of item 6. Analyses documented in the appendices of Part 3 of the Safety Report comply with the requirements of items 1, 2, 8, and 9. The requirements of item 3 have not been followed in some cases, for example, Moderator System and Moderator Auxiliary System Failure legacy analysis and identification of the deuterium deflagration in moderator cover gas (Gap 1). Note that the additional Safety Report Improvement Database (SRID) issue relevant to the same RD-310 clause regarding the impact of cobalt adjuster heatup is for Bruce B only. The requirement of item 4 has not been followed in that some of the old analyses documented in the Safety Report were produced using legacy tools predating N286.7-99 (Gap 2). New analyses follow the requirement of item 4. Selected boundary and initial conditions for legacy analysis of SLOCA, LLOCA, breaks outside containment, electrical system failures, moderator system failures, shutdown and maintenance cooling system failures, and feedwater and steams have not been properly justified or well defined (Gap 3). See event-specific gap assessments in SRI plan for more details. 6-a. The analysis of the various events include the assessment of safety margins to acceptance criteria which are selected to avoid any relevant cliff edge effects during the assessment of trip coverage. Key parameters impacting the calculated safety margins are identified and ranked for the various events in the Safety Report based on sensitivity analysis	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	methods used in the deterministic safety analysis: • conservative analysis method, such as the method used for Level 3 defence in depth • best-estimate-plus-evaluation–of-uncertainties method, such as the method used for Level 3 defence in depth • best-estimate analysis method, such as the method used for Level 2 and Level 4 defence in depth The first and second methods above are considered as part of the application of conservatism in safety analysis, and are addressed in section 4.4.6. Evaluation of uncertainties is elaborated in section 4.4.2.7.	assessing the impact of a change in these parameters on the calculated safety margins. This is also recognized by the industry P&G for DSA (Section 3.8.4), For safety margins in parameters beyond trip effectiveness, cliff edge effects have not been systematically investigated (Gap 4). 6-b. This practice has been consistently followed in the analyses documented in the appendices of Part 3 of the Safety Report. 7. This practice has not been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report (Gap 5). 8. This practice has been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report. 9. This practice has been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report. The current DSA in the Safety Report is based on a conservative method in line with the first approach recommended by the Guidance clause "analysis methods include conservative analysis method, such as the method used for Level 3 defence in depth".	
4.4.2.1	The scenario to be analyzed, or the analyzed event, should be defined by including descriptions of the following: • initial conditions • the initiating event and any additional events • expected actions of the plant systems and of the operator, in response to the initiating event • general description of the anticipated transient • associated safety concerns • long term stable state (including cold and depressurized shutdown) at the end of an event	This is a guidance clause. This practice has been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report.	C

Article No.	Clause Requirement	Assessment	Compliance Category
4.4.2.2	A set of applicable criteria should be identified, including any regulatory requirements. These criteria should address all safety challenges while also demonstrating compliance with the dose acceptance criteria given in section 4.3.2, as well as the derived acceptance criteria adopted by the designer. In addition to these criteria, others may be defined – in order, for example, to simplify the analysis by imposing more restrictive criteria, or to allow intermediate assessments in search of bounding cases.	This is a guidance clause. The identification of applicable acceptance criteria and the relevant regulatory requirements have been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report.	C
4.4.2.3	Key phenomena, key parameters, and the range of parameter values associated with the analyzed event should be identified. The supporting experimental data should also be provided or referenced, and theoretical understanding should be demonstrated. If an event is characterized by sufficiently different stages, then key phenomena should be identified for each stage. The importance of the involved phenomena should be judged against each acceptance criterion, separately. Key parameters are identified for each important phenomenon. These parameters are then ranked for their importance in influencing the applicable acceptance criteria. Sensitivity analyses can be used, in conjunction with expert judgment, to help identify and rank the parameters by assessing their influence on analysis results for each acceptance criterion. Particular importance should be given to the identification of cliff-edge effects, such as any abrupt changes in phenomena during any stage of the analysis. The results of experiments should also be used to help identify important parameters, assist in ranking the importance, and to identify if and where abrupt changes occur.	This is a guidance clause. Key phenomena and parameters relevant to each appendix of Part 3 of the safety Report are identified and ranked. The supporting experimental data are included in the validation matrices; however, they are not referenced in the Safety Report. The importance of each phenomenon to each phase of the analysis is addressed in the validation Technical Basis Document and validation matrices; however, it is not systematically referenced in the Safety Report. The importance of the phenomena to each safety concern/acceptance criterion is addressed in Part 3 of the Safety Report. The identification and ranking of phenomena is based on sensitivity analysis and expert judgement. Cliff edge-effects are inherently covered in the assessment of trip coverage, however, it is not consistently addressed for quantitative acceptance criteria beyond reactor trip. In principle, any relevant experimental results have been used in identifying phenomena and any associated cliff edge effects. See clause 4.4.2. Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
4.4.2.4	Safety analysis is performed using models of the plant systems and physical phenomena. All the important phenomena, as identified in section 4.4.2.3, should be represented in the models embedded in the computer code used for the calculations. The models and computer code applicability to the analyzed event should be demonstrated. Models of plant systems should be verified to reflect as-built plant condition, taking into account plant states and aging effects (such as pump degradation, steam generator fouling, increased roughness). Severe accidents may have a particular impact on NPPs with multiple units at a site; this emphasizes the need for a model for severe accidents with multiple units at a site. Further guidance is provided in section 4.4.5.	This is a guidance clause. Detailed assessment of code applicability to the analyzed event is not included in Part 3 of the Safety Report. New analysis complies with this guidance. DSA for BDBAs are not explicitly analyzed in the Safety Report, however they are performed within the scope of PRA Level 2. Bruce A PRA indicates that multi-unit events are considered. The completeness of such consideration needs to be confirmed, in particular, it may require complementary DSA for BDBAs with accounting for the capacity and limitations of long-term makeup water and electrical power supplies to support the evaluation of the safety goals. See clause 4.4.2. Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	RNA
4.4.2.5	The analysis should define the data characterizing the plant condition preceding the analyzed event and plant performance during the event – such as, but not limited to: • plant operating mode • reactor power • fuel burnup and burnup distribution • fuel temperatures • coolant temperatures and pressures • trip set points and action set points for mitigating systems • instrumentation delays and uncertainties • safety system performance characteristics • performance of other plant equipment (such as pumps, valves, coolers, boilers, and turbine)	This is a guidance clause. The data characterizing the plant condition preceding the analyzed event and plant performance during the event are identified in all appendices of Part 3 of the Safety Report. Plant operating limits and conditions are taken into account in the analysis assumptions and inputs of Part 3 of the Safety Report. Analysis of the main events impacted by ageing are revised to reflect plant conditions applicable to the licence duration. The results of new analysis are consistently used to confirm the adequacy of the OLCs and if necessary used to derive a more suitable value for use as an operating limit.	C

Article No.	Clause Requirement	Assessment	Compliance Category
	• weather conditions In the application of such data, the plant operating limits and conditions (OLCs) should be taken into account. The plant condition used as the initial conditions for the analysis may reflect the actual plant condition or (in many cases) reflect the limits selected for enforcement of the OLCs. This would be done so that the analysis can confirm that the selection of an OLC value is effective. Alternatively, the analysis results may be employed to derive a suitable value for use as an operating limit. Care and good judgment are required to ensure that the set of OLCs derived from such safety analyses are consistent with each other.		
4.4.2.6	Comprehensive calculations are conducted to assess the plant performance against each applicable acceptance criterion. Sensitivity studies are undertaken to assess the impact on analysis results of key assumptions – for example, in identifying the worst single failures in various systems, or to assess the impact of using simplified models instead of more accurate and sophisticated approaches (requiring significant effort in the calculations). Sensitivity analysis, with systematic variations in computer code input variables or modelling parameters, should confirm that there are no “cliff-edge” effects. A systematic process should be used to identify parameters with small margins to a cliff edge, such as fuel dry out, pressure boundary failure and tank depletion. Where the likelihood is considered to be high and the potential impact large, sensitivity calculations should explore the impact of passing these thresholds. The duration of the transients considered in the analysis should be sufficient to determine the event consequences. Therefore, the calculations for plant transients are extended beyond the point where the NPP has been brought to shutdown and stable core cooling, as established by some identified means (i.e., to the point where a long-term stable state has been reached and is expected to remain as long as required). The analysis should take into account the capacity and limitations of long-term makeup water and electrical power supplies. In cases where the various stages of the transient are governed by different phenomena and/or different time scales, different methods	This is a guidance clause. A single failure for each safety system is not explicitly identified. Sensitivity analyses are included but cliff-edge effects beyond reactor trip are not systematically addressed. On the duration of the transient, SR DBA analysis is performed up to the initiation of the long-term heat sink. PRA needs to confirm that this REGDOC-2.4.1 requirement on accounting for the capacity and limitation of long term makeup water and electrical power supplies are captured in the Level 1/2 PRAs and the supporting DSA for BDBAs The guidance with respect to the possible use of different tools for different phases of the events where dominant phenomena are different is in line with the approach used in Part 3 of the Safety Report. See clause 4.4.2, Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	and tools can be applied to model the consecutive stages.		
4.4.2.7	In the deterministic safety analysis for Level 3 defence in depth, all key uncertainties should be identified and accounted for. The safety analysis for Level 3 should incorporate appropriate uncertainty allowances for the parameters relevant to the analyzed accident scenario. Such uncertainties include modelling and input plant parameters uncertainties. The modelling-relevant parameters include those used to start the action of a mitigating system and/or those which can have a significant impact in challenging the integrity of a barrier preventing the release of fission products. The modelling uncertainties are associated with the models and correlations, the solution scheme, data libraries and deficiencies of the computer programs. The code accuracy obtained as the result of validation work should be used as a source for uncertainties of relevant modelling parameters. The code accuracy is defined by the bias and the variability in bias, and should be obtained from the comparison of code predictions with experimental data, station data or other applicable data. Input plant parameters (also referred to as operational parameters) are those parameters that characterize the state of plant's SSCs or are used to actuate a mitigating system. These are measured using in-reactor instrumentation. The measurement uncertainties are available from the plant instrumentation and control system documentation or the OLCs. The systematic ("bias") and random uncertainty components ("standard deviation") should be accounted for. The measurement bias represents an element of measurement uncertainty arising from a systematic error known to cause deviation in a fixed direction. The standard deviation represents an element of measurement uncertainty which cannot be defined exactly, or which can cause deviation in either direction, but can be estimated on the basis of a probability distribution. The aforementioned uncertainties should be accounted for	This is a guidance clause. Accounting for uncertainties in key modeling and plant parameters is not systematically demonstrated in Part 3 of the Safety Report. Simulation uncertainty is considered in the analysis of some events to account for modeling uncertainties relevant to trip parameters. Accounting for other modeling uncertainties is not demonstrated. Accuracy assessment obtained in validation has not been used as source to modeling uncertainties. New analysis includes accuracy assessments of key parameters and an accounting for their impact on the analysis results. Key parameters that characterize the state of plant's SSCs that are used to actuate a mitigating system are measured using in-reactor instrumentation. The systematic and random components of measurement uncertainty are considered in the analysis and operation limits and conditions. Accounting for uncertainties in key modeling and plant parameters are not systematically demonstrated through the analysis approach used in Part 3 of the Safety Report. DSA of the Safety Report does not include an explicit analysis for Level 2 and Level 4 defence-in-depth. See clause 4.4.2. Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	accordingly, either in the conservative analysis or in the best-estimate-plus-evaluation-of-uncertainties methodologies. In the safety analyses for Level 2 and Level 4 defence in depth (where a realistic, best-estimate analysis method may be used) it is not necessary to account for uncertainties to the same extent.		
4.4.2.8	Verification is performed to ensure that the deterministic safety analysis results are: • correctly extracted from the analysis codes' output • physically and logically sound • consistent with experimental data from suitable integral tests, plant recorded data, previous similar safety analyses or simulations with more advanced models • bounding predictions for each of the safety analysis acceptance criteria	This is a guidance clause. This practice has been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report. [DPT-NSAS-00015] on Execution of Safety Analysis complies with requirements.	C
4.4.2.9	Results of deterministic safety analysis calculations are documented in such a way as to facilitate their review and understanding. The documentation of safety analysis results should include: • objective of the analysis • analysis assumptions and their justification • plant models and modelling assumptions • any computer code user options that differ from the options used in code validation • analysis results in comparison with acceptance criteria • findings and conclusions from sensitivity and uncertainty analyses Further guidance is provided in section 4.5.	This is a guidance clause. With the exception of the fourth item, the analysis in Part 3 of the Safety Report complies with this clause. The analysis in Part 3 of the Safety Report does not identify computer code user options that differ from the options used in code validation (Gap 1). DPT-NSAS-00015 on Execution of Safety Analysis addresses this issue requiring to *stipulate that when multiple changes in code versions and/or models have occurred from a reference analysis, sensitivity studies shall be performed to determine the impact of each change on the specific analysis.*	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
4.4.3	Assumptions made to simplify the analysis – as well as assumptions concerning the operating mode of the NPP, the availability and performance of the systems, and operator actions – shall be identified and justified. The boundary and initial conditions used as the analysis input data shall: 1. accurately reflect the NPP configuration 2. account for the effects of aging of systems, structures and components 3. account for various permissible operating modes 4. be supported by experimental data, where operational data are not available Significant uncertainties in analysis data, including those associated with NPP performance, operational measurements, and modelling parameters, shall be identified. Guidance This regulatory document requires the safety analysis be based on plant design and complete and accurate as-built information. Operational historical recorded data (such as thermal power, flow rates, temperature and pressure) should also be included, where applicable. This information should cover plant SSCs, site-specific characteristics and offsite interfaces. For an NPP in the design phase, the operational data, if needed, should be derived from generic data from operating plants of similar design, or from research or test results. For an operating NPP, the safety analysis should use plant specific operational data. The safety analysis values for each plant input parameter should be determined based on: • design specifications	1. [DPT-NSAS-00013] procedure on Guidelines for Managing Reference Data Sets ensures that only verified datasets are used for deterministic safety analysis. Some of the legacy analysis does not reflect exactly the current plant configuration (Gap 1). 2. Although ageing effects have not been comprehensively addressed in legacy analyses, newer analyses for the most impacted events account for aging effects (Gap 2). 3. This practice has been followed in most of the analyses documented in the appendices of Part 3 of the Safety Report. However, some Safety Report issues related to gaps in covering all permissible operating modes are identified (Gap 3). 4. Initial and boundary conditions that are not based on operational data are not necessarily based on experimental data. Modeling uncertainties have not been consistently identified in Part 3 of the Safety Report (Gap 4). Guidance section of this clause: The initial and boundary conditions of the new safety analysis considers the various elements of this guidance. The Operational Safety Requirements (OSRs) and their relevant Instrumentation Uncertainty Calculations are prepared within the SOE program and being introduced in the next licensing period. The starting point of the OSRs is the determination of the Safety Limits, which corresponds to the analysis limits after accounting for the associated instrumentation uncertainty. The OSRs cover process parameter and hardware limits.	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	• tolerances • permissible ranges of variability in operation • uncertainties in measurement or evaluation for that parameter The operational data should include: • information on component and system performance, as measured during operation or tests • delays in control systems • biases and drift of instrumentation • system unavailability due to maintenance or testing Applicable limits for NPP parameters that are used as initial and boundary conditions should be identified. The NPP parameters assumed in the safety analysis should bound the ranges of parameters allowed by the operating procedures or, in a statistical approach, cover a predetermined high percentile of each range at a predetermined high confidence level. The following NPP parameters may be used in analysis as input data, and should be specified in the OLCs, as measured or evaluated during plant operation: • neutronic and thermal powers, including power distribution • pressures • temperatures • flows • levels • leakage or bypass of valves, seals, boiler tubes, and containment • inventory of radioactive materials		

Article No.	Clause Requirement	Assessment	Compliance Category
	• fuel sheath defects • flux shapes • isotopic purity of coolant and moderator (where relevant) • neutron poison concentration • core burnup and burnup distribution • instrument tolerances • instrument time constants and delays • parameters related to SSC aging (besides accounting for aging effects on other parameters) • position of rods, valves, dampers, doors, gates • number of operational components, such as pumps and valves Note: In the preparation of the data in the list above, there are some parameters (such as core burnup and burnup distribution) that are not measured directly. Core characteristics for all fuel loads should be accounted for. In this example, they are evaluated and extracted from computer simulation for which the accuracy of these tools is supported by station and experimental data. There are generally some inputs to the safety analysis that are derived or inferred from data obtained experimentally. It should also be noted that the effects of aging include long-term mechanisms causing gradual degradation as well as mechanisms causing rapid degradation. Degradation mechanisms include thermal cycles, deformation, strain, creep, scoring, fatigue, cracking, corrosion and erosion. The allowed aging limits are part of the safety analysis input data. Uncertainties in plant data should be determined and recorded. These uncertainties should be considered in the uncertainty and sensitivity analyses.		

Article No.	Clause Requirement	Assessment	Compliance Category
4.4.4	Assumptions made to simplify the analysis, as well as assumptions concerning the operating mode of the nuclear power plant, the availability and performance of the systems, and operator actions, shall be identified and justified. The analysis of AOO and DBA shall: 1. apply the single-failure criterion to all safety systems and their support systems 2. account for consequential failures that may occur as a result of the initiating event 3. credit actions of systems only when the systems are qualified for the accident conditions, or when their actions could have a detrimental effect on the consequences of the analyzed accident 4. account for the possibility of the equipment being taken out of service for maintenance 5. show that the plant can be maintained in a stable, cold and depressurized state for a prolonged period 6. credit operator actions only when there are: a. unambiguous indications of the need for such actions b. adequate procedures and sufficient time to perform the required actions c. environmental conditions that do not prohibit such actions For the analysis of a BDBA, it is acceptable to use a more realistic analysis methodology consisting of assumptions that reflect the likely plant configuration, and the expected response of plant systems and operators in the analyzed accident. Guidance Assumptions are made in the input data, such as those related to the design and operating parameters, as well as in the physical and numerical models implemented in the computer codes.	This practice has been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report. 1. This practice has been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report in accordance with the interpretation of the single failure criterion prevalent at the time. The analyses do not follow newer, more restrictive, interpretations of the criterion (Gap 1). 2. The requirements of item 2 have not been followed in some cases, for example, consequential failures arising during a loss of moderator inventory accident, deuterium deflagration in moderator cover gas (Gap 2). 3. This practice has been followed in most of the analyses documented in the appendices of Part 3 of the Safety Report. However, some gaps exist regarding crediting RRS in SLOCA and transition breaks in legacy analysis and therefore this is considered a gap (Gap 3). 4. This practice has been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report. 5. DSA is usually performed until long term heat sink is established. Discussion on how and for how long a stable cold and depressurized state is maintained has not been demonstrated for the various events in the Safety Report. This should be within the scope of PRA and its supporting DSA for BDBAs (Gap 4). 6. This practice has been followed in the analyses documented in the appendices of Part 3 of the Safety Report except for the time allowed to perform operator action for accidents involving the irradiated fuel port where operator action is credited 10 minutes after the incident. This is less than the usual 15 minutes allowed from first unambiguous indication of a problem requiring operator action from inside the main control room (Gap 5). The use of more realistic assumptions for BDBAs is consistent with PRA approach and DSA for BDBAs. Some of the analyzed events in the Safety Report will be classified as BDBAs and any	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	Assumptions may be either intentionally realistic or deliberately biased in a conservative direction. The assumptions generally used for the Level 3 defence-in-depth analysis of AOOs and DBAs are described in sections 4.4.4.1 to 4.4.4.7. It should be noted that some of these assumptions are not necessary in the analysis of AOOs for assessing control system capability (Level 2 defence in depth,) if such an approach can be justified. For BDBA safety analysis, one objective is to demonstrate the capabilities of SSCs to meet the design requirements specified for BDBA conditions. The analysis should account for the full design capabilities of the plant, including the use of some safety and non-safety systems beyond their originally intended function (to return the potential severe accident to a controlled state, or to mitigate its consequences). The BDBA analysis assumptions on crediting and modelling plant systems and their capability during a BDBA should be consistent with the objectives of the analysis. If credit is taken for use of systems beyond their originally intended function, there should be a reasonable basis to assume they can and will be used as assumed in analysis. This basis can be obtained from the evaluation of effectiveness of these systems to operate in severe accident conditions, if they are still available.	required revision of their analysis will adopt a more realistic analysis methodology (Gap 6). Guidance - This guidance suggests possible relaxation to the assumptions in AOOs. Level 2 defence-in-depth analysis as compared to Level 3 analysis. The analysis in Part 3 of the Safety Report is Level 3 analysis and AOOs are addressed within SF events rather than explicitly. -This guidance promotes that the analysis should account for the full design capabilities of the plant, including the use of some safety and non-safety systems beyond their originally intended function (to return the potential severe accident to a controlled state, or to mitigate its consequences) with demonstrating reasonable basis of their effectiveness under the severe conditions. This is in line with the DSA for BDBA within PRA.	
4.4.4.1	The single-failure criterion stipulates that the safety group consisting of a safety system and its support systems should be able to perform its specified functions even if a failure of single component occurs within this group. Expectations related to the application of the single-failure criterion in design can be found in REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants. The analysis should assume a single failure to occur for each element of a safety group in turn, and identify the worst single failure for each acceptance criterion. In addition to a single failure of a component, the analysis should account for the impact of possible maintenance, testing, inspection or repair on safety group performance.	This is a guidance clause. The conservatism in the analysis assumptions include multiple single failures impacting the various acceptance criteria. However, the analyses do not follow newer, more restrictive, interpretations of the criterion. See clause 4.4.4. Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	Safety analysis of AOOs and DBAs for Level 3 defence in depth should apply the single-failure criterion to each safety group. The single-failure criterion does not need to be applied in the analysis of AOO for Level 2 defence in depth and BDBA.		
4.4.4.2	The analysis should take into account consequential failures that may occur as a result of an initiating event. Any failures that occur as a consequence of the initiating event are part of that event and are not considered to be a single failure for the purpose of safety analysis. For example, equipment that is not qualified for specific accident conditions should be assumed to fail unless its normal operation leads to more conservative results.	This is a guidance clause. See clause 4.4.4. Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	RNA
4.4.4.3	Guidance for availability of systems The operation of systems should be credited only when they are designed or shown to be capable of performing the intended function, and are qualified to withstand all challenges and cross-link effects arising from the accident. In the safety analysis of an AOO for Level 2 defence in depth, credit may be taken for the operation of process and control systems whose actions could help mitigate the event, as long as the credited systems are not impaired as a consequence of the initiating event. The status of these systems and the values assigned to their parameters need to be justified. In the safety analysis of AOOs and DBAs for Level 3 defence in depth, no credit should be taken for the operation of the control systems in mitigating the effects of the initiating event. The effects of control system actions should be considered, if these actions would aggravate the transient or delay the actuation of the protection features. If the operation of non-qualified equipment results in worse event consequences, this will lead to the general assumption that such equipment is operated in a manner that makes the event worse. Any process equipment that is operating prior to the event is assumed	This is a guidance clause. This practice is followed consistently in Part 3 of the Safety Report Level 2 defence-in-depth is not explicitly assessed in Part 3 of the Safety Report. Gap is identified in some cases where a control system is credited in a Level 3 defence in depth analysis although its action would improve the event consequence, e.g. RRS operation in SLOCA. Part 3 of the Safety Report is consistent with not crediting non-qualified equipment operation. Part 3 of the Safety Report is consistent with the guidance on considering continuous operation of process equipment that were operating prior to the event. Partial and total failures are covered in the Safety Report. The various modes of failures are covered in the Safety Report. Guillotine break analysed in the Safety Report consider a discharge area twice the cross-sectional area of the piping.	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	to continue operating, if it is not affected by the initiating event. For example, boiler feed can be assumed to continue until loss of electrical power, for those events which do not produce a harsh environment. Guidance for partial and total failures Partial and total failures of equipment should be considered in the analysis of each failure sequence, to identify the worst failure for each acceptance criterion. Guidance for worst piping failure Various modes of piping failures should be considered in loss-of-coolant analyses. They include circumferential, guillotine, and longitudinal failures at any location in a system. For circumferential and guillotine failures, analysis should consider a discharge area up to, and including, twice the cross-sectional area of the piping. For longitudinal breaks, the analysis should justify the upper limit of the range of postulated break size. The worst break location, size, and orientation, in the context of posing the most challenges to a safety analysis requirement, should be identified through analysis, including sensitivity analysis, using a conservative break model. For CANDU reactors, failures of reactor inlet and outlet headers are considered in the same way as piping failures. Guidance for loss of offsite power In addition to a single failure and any consequential failures, a loss of offsite power should be assumed, unless a justification is provided. The loss of offsite power may be assumed to occur either at the initiation of the event or as a consequence of reactor and turbine trip. For example, when loss of Class IV power (CANDU-type reactor) is assumed, the event should be analyzed both with and without the loss of offsite power, and the most limiting results should be used.	Justification for the largest longitudinal break (e.g. PT rupture event) is included. Limiting breaks are based on identifying the limiting size and location for each acceptance criterion. Breaks in inlet and outlet headers are considered as pipe breaks in the Safety Report. Part 3 of the Safety Report is consistent with the guidance on loss of off-site power. See clause 4.4.4. Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	

Article No.	Clause Requirement	Assessment	Compliance Category
4.4.4.4	Safety systems should be credited at their minimum allowable performance, in accordance with the OLCs. Guidance for shutdown means The deterministic safety analysis should demonstrate the effectiveness of all credited shutdown means by demonstrating that the design meets applicable acceptance criteria (see section 4.3). This subsection contains different expectations, depending on the reactor's design and inherent characteristics, as described in REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants. Two broad categories of reactors are considered, as follows: • reactors with inherent safety: designs that demonstrate that any AOO or DBA with failure of the fast-acting shutdown means (anticipated transient without reactor trip type analysis) does not lead to severe core damage and a significant early challenge to containment • reactors with engineered safety: designs that cannot demonstrate that any AOO or DBA with failure of the fast-acting shutdown means does not lead to severe core damage and a significant early challenge to containment The following are the applicable acceptance criteria for the two categories of reactors: Guidance for shutdown means for reactors with inherent safety For the first shutdown means, which is fast-acting, the analysis should demonstrate that the criteria applicable to the initiating event class (AOO or DBA, as applicable) are met. Operator actions to supplement the fast-acting shutdown means may be credited, provided that the conditions for manual reactor trip are satisfied (see end of this subsection). For the second shutdown means (that may be manually initiated), the frequency of occurrence of an AOO and the failure frequency of the fast-acting shutdown means may result in a combined frequency that falls in the DBA range, in which case the applicable limits are the DBA	This is a guidance clause. Guidance for shutdown means: The applicable guidance is that for shutdown means for reactors with engineered safety. This guidance identifies that the objective of the two shutdown systems is to have two trips for each event. Bruce A meets this requirement with some justified exemptions. Table 3 notes of this guidance clause allows having one applicable trip for events with slow or no power increase. The analysis of slow LOR is in line with this guidance where NOP is the only effective trip. Guidance for emergency core cooling system Part 3 of the Safety Report is in line with crediting the conditioning signal for emergency coolant injection only when it is not blinded. Assessment of other factors mentioned in the guidance (e.g., Non-condensable gases) are not addressed explicitly in Part 3 of the Safety Report. Guidance for containment Consequences of situations when the containment isolation instrumentation is blinded are covered in the Safety Report. As documented in [NK21-CORR-00531-11005] the Bruce A vacuum type containment was not designed with testing capability for penetrations. Various components of the containment system can be tested separately to demonstrate the integrity of the system, as well as the system as a whole. Cable penetrations can be tested by pressurizing the space between the primary and secondary seals. Detailed containment test procedures are in effect. Overall containment integrity is confirmed by a positive pressure test of the entire system, during station outages, as described in Section 6.2.4 of the Bruce A Safety Report [NK21-SR-01320-00002]. Containment performance is also monitored	IC

Article No.	Clause Requirement	Assessment	Compliance Category
	dose limits. If the designer can demonstrate a very high reliability for the fast-acting shutdown means, it may be acceptable to use BDBA limits (i.e., the safety goals). The frequency of a DBA and the failure frequency for the fast-acting shutdown means may result in a combined frequency that falls in the BDBA range, in which case the applicable limits are the safety goals. Guidance for shutdown means for reactors with engineered safety The design includes two redundant, fast-acting means of shutdown, both of which should be demonstrated to be equally effective (see REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants). The criteria for both shutdown means will be the same, and will be AOO or DBA criteria, as applicable to the event class. To help better understand trip parameter expectations, table 3 can be used to determine the performance objectives for the specific event under consideration. Objectives for reactor designs with inherent safety and reactor designs with engineered safety are shown. Table 3: Performance objectives for the number of trip parameters Notes: 1. for accident scenarios with slow or no power increase, two-parameter trip coverage should be demonstrated if practicable 2. or scenarios where analysis is being performed not to demonstrate trip coverage, but to provide support such as environmental qualification (EQ) room conditions analysis for equipment survivability, a backup trip parameter is demonstrated only if practicable. A manual reactor trip can be considered to be equivalent to a trip parameter if: the requirements for crediting operator action from the main control room are met (see subsection 4.4.4.5); and the reliability of manual shutdown meets the reliability requirements for an automatic trip. Guidance for emergency core cooling system If the emergency core cooling system (ECCS) logic has an injection	and trended via the quarterly on-power leak rate test (QLRT), which measures the leak tightness of the containment structure at negative pressure. The results of these on-power tests show that containment leakage remains well within the OP&P limit of 2%/hr at the design pressure and Metric Standard Conditions. As noted in Section 5.6.3.1.4 of the Safety Report [NK21-SR-01320-00003], the measured leak rate profile is reproduced conservatively for analysis purposes by assuming the presence of a base laminar leak rate of 2.32%/hr.	

Article No.	Clause Requirement	Assessment	Compliance Category
	logic conditioned by the presence of other indicators (i.e., conditioning signal), then the safety analysis should identify and evaluate the consequences of situations where those conditioning signals may be blinded. If the ECCS activation logic is complex (i.e., several different actions are required for the system to be considered fully activated), then the safety analysis should consider the consequences if some of these actions do not occur – for example, a failure to re-align the ECCS pump suction to the containment sump. For certain designs, the following considerations should be taken into account: • the potential for gas entrainment that could result in damage due to the occurrence of water hammer • the impact on recirculation flows in the presence of filter plugging, debris blockage, heat exchanger blockage, or pump cavitations • the effect of non-condensable gases on flow and heat transfer The safety analysis should consider the impact on the effectiveness of the ECCS of the inaction, partial action, and normal functioning of any other systems that supplement or degrade the cooling capability of the ECCS. Guidance for containment The deterministic safety analysis should identify and evaluate consequences of situations when the containment isolation instrumentation is blinded. For containment, “blinded” refers to conditions for which a containment isolation actuation set point is approached, but not reached. For example, the containment may be blinded by the inaction, partial action, or normal functioning of other systems that supplement or degrade the containment performance. Containment blinding scenarios are important, because an accident with a potential for radioactivity release may not trigger the activation of containment isolation.		

Article No.	Clause Requirement	Assessment	Compliance Category
	The containment leakage rate assumed in the analysis should be based on containment design leak-tightness requirements, and confirmed by the leakage rate tests. Guidance for equipment under maintenance The analysis should account, where applicable, for the possibility of the equipment being taken out of service for maintenance.		
4.4.4.5	Specific operator actions required in response to an accident should be identified. Operator actions can be credited in the safety analysis for Level 3 defence in depth only if: • there is reliable instrumentation designed to provide clear and unambiguous indication of the need to take action • the power plant has operating procedures that identify the necessary actions, operator training, support personnel, spare parts, and equipment • environmental conditions do not prevent safe completion of operator actions Following the first clear and unambiguous indication of the necessity for operator actions, such actions may normally be credited in the safety analysis (Level 3 defence in depth) to be started no sooner than: • 15 minutes for actions in the main control room • 30 minutes for actions outside the main control room Times for operator actions in new nuclear power plants are established in REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants. Note: New nuclear power plants referenced in this section are those first licensed in 2014 and beyond. It should be shown by assessment that the specified times are sufficient for the operator to detect and completely diagnose the event, and to carry out the required actions. Such assessment should	This is a guidance clause. See clause 4.4.4. Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	account for the following: • time starting from the occurrence of the initiating event to the receipt of the event indication by the operator • time to carry out the diagnosis • time required to perform the action • time for the safety related function to be completed In certain circumstances, which must be justified, a completion time shorter than 15 minutes for a control room action might be assumed, provided that: • the operator is exclusively focused on the action in question • the required action is unique, and does not involve a choice from several options • the required action is simple and does not involve multiple manipulations The assessment of the credited human action items should be formally documented. It should include a validation process, which can encompass: • documented procedures that define specific operator action entry points and actions • training of personnel on those procedures (training outline, materials, records) • performing station drills, exercises or control room simulator studies, to confirm that human actions can be completed and to assess response times • consideration of control room simulator data from training activities • analysis and assessment of the response times, to provide credible time estimates for safety analysis usage		

Article No.	Clause Requirement	Assessment	Compliance Category
	• validation reports		
4.4.4.6	The assumptions incorporated in the computer codes, or made during code applications, should be such that safety analysis results (whether best-estimate or conservative) remain physically sound. In performing safety analysis, justifications should be provided for all instances where the assumptions used are different than those used in the validation.	This is a guidance clause. Safety Report analyses do not include assessment whether code model options used in the analysis are similar to those used in their validation (Gap 1).	Gap
4.4.4.7	As mentioned in section 4.3, the committed whole-body dose for average members of the critical groups who are most at risk (at or beyond the site boundary) is calculated in the deterministic safety analysis for a period of 30 days after the analyzed event. The effective dose should be used in dose calculations, and should include contributions from: • external radiation from cloud and ground deposits • inhaled radioactive materials • skin absorption of tritium In dose calculations, the worst weather scenario in terms of predicted dose should be assumed. All weather scenarios with probabilities of occurrences higher than 5 percent should be accounted for. No intervention in the form of decontamination or evacuation should be assumed. Intervention against ingestion of radioactive materials and natural removal processes may be assumed. Dose calculations should also be conducted for several time intervals, and up to one year after the accident.	This is a guidance clause. Part 3 of the Safety Report does not demonstrate whether it covers weather scenarios with probabilities of occurrences higher than 5% and does not include dose calculations for intervals up to 1 year (Gap1).	Gap
4.4.5	Computer codes used in the safety analysis shall be developed, validated, and used in accordance with a quality assurance program that meets the requirements of CSA N286.7-99, Quality Assurance of	All computer codes used in new analysis meets CSA N286.7-99. There is a gap related to the use of legacy codes and their qualifications predating N286.7-99 (Gap 1).	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	Analytical, Scientific, and Design Computer Programs for Nuclear Power Plants. Guidance The use of realistic computer codes in safety analysis is preferable, given that the use of conservative codes may produce misleading or unrealistic results. However, an extensive experimental database should be established to demonstrate the code applicability and to validate the code, thereby providing a basis for confidence in code predictions. Fully integrated models could give a more accurate representation of the event, and should be used to the extent practicable. These models address all important phenomena within a single code or code package. Sequential application of single-discipline codes is more likely to misrepresent feedback mechanisms than fully integrated models, and should be avoided unless there is a specific advantage. The selection of computer codes should consider the code applicability, the extent of code validation, and the ability to adequately represent the physical system.	Guidance - Safety Report analysis is mainly based on realistic computer codes in line with the guidance. - Preference of integrated models becomes the norm of new analyses. - The intent of the guidance on code selection is met.	
4.4.5.1	For the safety analysis of an event, the applicability of computer codes used to predict the consequences is established before conducting the analysis. The demonstration of code applicability includes the following steps: • identification of all phenomena significantly influencing the key output parameters (see section 4.4.2.3) • confirmation that the code implements adequate models for all key phenomena, and demonstrating that these models have been verified and validated against separate effect tests • assessing the closure equations and constitutive relationships • assessing scaling effects; the scalability of the integral effects tests should be assessed to confirm that there is no significant distortion in the database; scaling distortions and their impact on the code assessment should be identified, evaluated and addressed in	This is a guidance clause. Code applicability is not systematically or comprehensively addressed in the Safety Report. Newer analysis started to include code applicability assessments. See clause 4.4.5. Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	the safety analysis • assessing the numerical stability of calculations and temporal and spatial convergence of iterative approximations; the spatial and temporal convergence are achieved when an increase or a reduction in the node or time step sizes (which includes changing the minimum time step, if necessary) does not change simulation results significantly • addressing any gaps or deficiencies in the code applicability for the analyzed event The code applicability assessment and relevant knowledge bases are documented in sufficient detail to allow for an independent review. To model behaviour involving many coupled phenomena, it should be demonstrated that data are transferred through interfaces (i.e., from the calculation of one phenomenon to another) in a manner which adequately captures the physical phenomena and feedback mechanisms.		
4.4.5.2	This document requires all computer codes to be validated for their application in safety analysis. The purpose of validation is to provide confidence in the ability of a code for a given application, and also to determine the code accuracy. The validation should: • demonstrate the capability and credibility of a computer code for use in specific analysis application • quantify the accuracy of the code calculations (quantified through comparison of code prediction with experimental data or other known solutions) The codes used in safety analysis are validated by comparing code predictions with: • experimental data • commissioning data and operating data, where available	This is a guidance clause. Code accuracy is not systematically or comprehensively addressed in the Safety Report. Newer analysis started to include relevant code accuracy assessments. Computer code validation of the legacy codes used in the Safety Report does not comply with the guidance on code validation. See clause 4.4.5. Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	• solutions to standard or benchmark problems • closed mathematical solutions • results of another validated computer program The comparison of code predictions with solutions to standard problems or closed mathematical solutions for the purposes of validation is acceptable, but they should normally be supplemented with other types of comparisons. The experimental database used for validation may encompass separate effects, as well as component and integrated tests. Chosen test validation should satisfy the following criteria: • test data are obtained at physical and geometrical conditions and phenomena that are relevant either to normal operation conditions, or to a postulated accident scenario in the reactor • tests used for validation are free of distortions due to geometry or other properties, to the extent practicable • measurement uncertainties are quantified • systematic errors (bias) are minimized, and their sources are understood • the integrated tests used for validation should be specific to the reactor, and contain components representative of those used in the NPPs • data used for model development is independent from data used for computer code validation Accuracy of code predictions should be provided for the key modelling parameters, and for the plant parameters used to control power generation or to initiate a mitigating system (see section 4.4.2.7). The bias and variability of bias in the computer code can be obtained from the comparison of code predictions with experimental data. The code models used during validation should be identified and		

Article No.	Clause Requirement	Assessment	Compliance Category
	recommended for use in safety analysis, so that the safety analysis is consistent with the validation. Otherwise, the impact of using different models on the simulation results (code accuracy) should be assessed. Clear recommendations should be made on the use of a code beyond the conditions for which validation has been performed, and all the effects of such extrapolations should be assessed and accounted for. The effect of the modelling assumptions on the validation results should be assessed, including confirmation that a spatial and temporal convergence of the solution is achieved. Documentation of the computer tools should be clear and easy to follow, so the uncertainties due to user effects would be negligible. The use of different computer hardware or operating systems should also have negligible effects. Means such as user training and compliance with quality assurance procedures should be clearly stated. Computer code validation should be performed by qualified persons. Validation reports should be reviewed by qualified persons who had not participated in the validation. The guidance given above is consistent with and complements the requirements in CSA N286.7-99, Quality Assurance of Analytical, Scientific, and Design Computer Programs for Nuclear Power Plants.		
4.4.5.3	Data are also prepared to provide a mathematical representation of the physical components, and how their arrangements are to be represented by the computer simulation. This input data should be prepared in accordance with the following principles: • a systematic method for representing components and connections should be developed • the basis for the methodology should be documented; the methods used are usually based on experience in representing experimental facilities and other plants of similar configurations • the representation should be verified and validated • in some cases, plant tests (sometimes as commissioning	This is a guidance clause. Plant simulations are performed using reference data sets (RDSs), which includes the plant representation details based on the analysis requirements identified in the relevant analysis technical basis. RDS maintenance, change control and verification are governed by BP guidelines for managing RDS [DPT-NSAS-00013 R003]. Validation of plant representation (model) cannot be performed separately from code validation. Recent validation exercises use available plant data and the validation results as a measure of the adequacy of the code and the used mode representation. See clause 4.4.5. Given that there is a gap identified against this	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
	tests) are required to establish the precision of such representations In general, representations used for plant simulations should be created using the same principles as the representation used for code validation to minimize the related user effects.	requirement, the guidance portion of this clause has not been further assessed.	
4.4.6	The safety analysis shall build in a degree of conservatism to off-set any uncertainties associated with both NPP initial and boundary conditions and modelling of NPP performance in the analyzed event. This conservatism shall depend on event class and shall be commensurate with the analysis objectives. Guidance Safety analysis needs to incorporate a degree of conservatism that is commensurate with the safety analysis objectives and is dependent on the event class. Conservatism in safety analysis is often necessary to cover the potential impact of uncertainties, and may be achieved through judicious application of conservative assumptions and data. The concept of conservatism is applied to Level 3 defence-in-depth safety analysis. This is to ensure that limiting assumptions are used when knowledge of the physical phenomena is insufficient. For Level 2 and Level 4 defence in depth, the safety analysis should be carried out using best-estimate assumptions, data and methods. Where this is not possible, a reasonable degree of conservatism (appropriate for the objectives of these levels) should be used, to compensate for the lack of adequate knowledge concerning the physical processes governing these events. While it is permissible – and sometimes encouraged – to use conservative codes, it is usually preferable to apply realistic (best-estimate) computer codes. Where conservative analysis results are required for Level 3 defence-in-depth (AOO and DBA) analysis, best-estimate computer codes should be used along with the assessment of modelling and input plant parameter uncertainties. The deterministic safety analysis for AOO and DBA (conservative analysis for Level 3 defence in depth) should:	Conservative assumptions are used in the analysis. However, there is no demonstration that the conservatism of the analysis would cover modeling uncertainties (Gap 1). Guidance This practice has been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report. Part 3 of the Safety Report is consistent with the guidance on applying conservatism in Level 3 defence-in-depth. Level 2 and Level 4 defence-in-depth are not explicitly covered in Part 3 of the Safety Report. New analyses will be based on COG P&G for DSA [COG-09-9030 Version 2009 (superseded now at Revision 003)], which is consistent with the recommendation of using best estimate methods and assumptions. Assessment of modeling and plant parameter uncertainties have not been consistently considered, this relates to the gap in the requirement and is therefore not repeated against the guidance. The analyses documented in the appendices of Part 3 of the Safety Report are in accordance with the interpretation of the single failure criterion prevalent at the time. The analyses do not follow newer, more restrictive, interpretations of the criterion. This relates to the gap in the requirement and is therefore not repeated against the guidance. Part 3 of the Safety Report assumptions are in line with the guidance of using analysis assumptions that are consistent with the OLCs) for safety groups and account for consequential failures	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	• apply the single-failure criterion to all safety groups, and ensure that the safety groups are environmentally and seismically qualified • use minimum allowable performance (as established in the OLCs) for safety groups • account for consequential failures that may occur as a result of the initiating event • credit the actions of process and control systems only where the systems are passive and environmentally and seismically qualified for the accident conditions • include the actions of process and control systems when their actions may have a detrimental effect on the consequences of the analyzed accident • credit the normally running process systems that are not affected by the analyzed accident • if operator actions are credited, demonstrate that credible “worst case” operator performance has been considered in the analysis and assessment Independent selection of all parameters at their conservative values can lead to plant states that are not physically feasible. When this could be the case, it is recommended to select conservatively those key parameters that have the strongest influence on the results in comparison with the acceptance criterion under consideration. The remaining parameters can be specified more consistently in the ensuing calculations. Each calculation should account for the impact of a particular parameter, so that the effects of all parameters can be assessed.	that may occur as a result of the initiating event. Part 3 analyses of the Safety Report are consistent with the guidance on crediting running process and control systems (e.g. Feedwater control action in LOCA events). Section 1.3 of Part 3 of the Safety Report includes a summary of Operator Actions used in the analyses of Part 3 of the Safety Report. Part 3 analyses of the Safety Report are consistent with the guidance on selecting conservatively those key parameters that have the strongest influence on the results in comparison with the acceptance criterion under consideration.	
4.5	The safety analysis documentation shall be comprehensive and sufficiently detailed to allow for a conclusive review. The document shall include: 1. the technical basis for the analyzed event and key phenomena and processes	1. This practice has been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report and supported by the validation technical basis and validation matrices. 2. This is provided in Part 2: Plant Components and	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	2. A description of the analyzed facility, including important systems and their performance, as well as operator actions 3. information describing the analysis method and assumptions 4. a description of the assessments of code applicability for the analyzed event and computer code uncertainty 5. an easily understood description of the results of the analysis, and the drawing of conclusions with respect to conformance with acceptance criteria Analysis documentation shall facilitate the update of the analysis when new results become available. Guidance The review should be an independent review and conducted by suitably qualified experts. In particular, the following elements need to be included in the safety analysis documentation: • a technical basis that includes: o the objective(s) of the analysis o a description of the analyzed event, which should include a description of the NPP operating mode, action of SSCs, operator actions and significant phases of the analyzed event (note that other events bounded by the analyzed event should also be identified) o a description of safety concerns, challenges to safety, and applicable safety analysis criteria, requirements and numerical limits o identification of key phenomena significantly affected by the key parameters for the analyzed event, along with a description of the systematic process used for identification of key parameters • a description of the analyzed facility, including important systems and their performance, as well as operators actions • information on the analysis method and assumptions	Systems, of the Safety Report. 3. This practice has been followed in all new analyses documented in the appendices of Part 3 of the Safety Report. 4. This practice has not been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report (Gap 1). 5. This practice has been consistently followed in all the analyses documented in the appendices of Part 3 of the Safety Report. The current system of periodic updates to the Safety Report supplemented by other Analyses of Record between updates meets the clause satisfactorily. Guidance Application of the following guidance elements is not demonstrated in Part 3 of the Safety Report; - Demonstration of code applicability - Assessment of code accuracy - Consideration of modeling uncertainties. Given that there is a gap identified against this requirement, the guidance portion of this clause has not been further assessed.	

Article No.	Clause Requirement	Assessment	Compliance Category
	• information demonstrating the code applicability, including (when available) evidence that codes have been validated against prototypical experiments and assessment of code accuracy, as well as references to the relevant experimental results; demonstration that the analysis assumptions are consistent with the plant operating limits (with evidence from NPP operation and experiments demonstrating the assumed observed variances in operating parameters, and uncertainties in modelling parameters, respectively) • a description of the results of analysis, including results of sensitivity and uncertainty studies with sufficient detail to show dominant phenomena; evidence of independent verification of the inputs and the results; evidence of analysis review, including an assessment of the impact (if any) on the plant's operating limits, conditions, manuals, etc. Safety analysis documentation should be written in a manner that can be easily understood by the station staff controlling the plant's OLCs.		
4.6	Review and Update of Deterministic Safety Analysis	This is not a requirement/guidance clause (this is a title only).	NA
4.6.1	The licensee shall systematically review the safety analysis results to ensure that they are correct and meet the objectives set for the analysis. The results shall be assessed against the relevant requirements, applicable experimental data, expert judgment, and comparison with similar calculations and sensitivity analyses. The licensee shall review the analysis results using one or more of the following techniques, depending on the objectives of the analysis: 1. supervisory review 2. peer review 3. independent review by qualified individuals 4. independent calculations using alternate tools and methods to the extent practicable Guidance	The procedure on Execution of Safety Analysis [DPT-NSAS-00015] outlines the review and verification process for safety analyses, and includes the techniques listed in the clause. Guidance The review of new analyses is in line with the guidance elements.	C

Article No.	Clause Requirement	Assessment	Compliance Category
	Procedures should be developed to determine the extent of the independent review to be applied at each step of the safety analysis. To review the safety analysis and identify potential deficiencies, reviewers should be familiar with: • safety standards, analytical methods, and technical and scientific research • changes in power plant data, design, operating envelope and operating procedures • information on operating experience from other NPPs In reviewing the safety analysis, the following review elements should be considered: • plant design information, supported by layout, system and equipment drawings, and design manuals • operating limits and permitted operational states • information about the functional capability of the plant, systems and major items of equipment • the findings of tests which validate the functional capability • the results of inspection of components • site characteristics, such as flood, seismic, meteorological, and hydrological databases • offsite characteristics, including population densities • results of similar analyses • developments in analytical methods and computer codes • regulatory rules for safety analysis • safety analysis standards and procedures The extent and method of the review should be commensurate with:		

Article No.	Clause Requirement	Assessment	Compliance Category
	• the analysis complexity and novelty • similarity to previously reviewed analyses • predicted margins to acceptance criteria For novel and complex analysis, the use of alternative methods should be considered to confirm analysis results. Alternative methods used for confirmation may be simplified, but should be capable of demonstrating that the original analysis results are reasonable.		
4.6.2	The safety analysis shall be periodically reviewed and updated to account for changes in NPP configuration, conditions (including those due to aging), operating parameters and procedures, research findings, and advances in knowledge and understanding of physical phenomena, in accordance with CNSC regulatory standard S-99, Reporting Requirements for Operating Nuclear Power Plants, or successor documents. In addition to periodic updates, the safety analysis shall also be updated following the discovery of information that may reveal a hazard that is different in nature, greater in probability, or greater in magnitude than was previously presented to the CNSC in the licensing documents. Guidance The periodic update of the safety analysis report should: • incorporate new information • address identified new issues • use current tools and methods • address the impact of modifications to the design and operating procedures that might happen over the life of the NPP Updating the safety analysis ensures that it remains valid, while taking into account: • the actual status of the NPP	The procedure on Nuclear Safety Assessment Initiation and Review [DIV-ENG-00012] prescribes how safety analyses are initiated. The procedure on Guidelines for Evaluating and Prioritizing Safety Report Issues [DPT-NSAS-00003] supports the updating process. Although current practices are in compliance with the requirement for review, not all analyses within Part 3 Accident Analysis [NK21-SR-01320-00003] have been fully kept up with the condition of the plant (Gap 1). The procedure on Processing of S-99 Reportable Conditions Arising from Safety Analysis [DPT-NSAS-00007] implements the requirements of CNSC S-99, which is the mechanism through which this clause is satisfied. REGDOC 3.1.1 (issued on May 2014) is the successor regulatory document to S-99 and is part of the licence. [DPT-NSAS-00002] procedure on Safety Report Analysis Update Process Overview prescribes the update process. Guidance The new analyses are performed in line with the guidance elements except: - Ensuring the analysis is valid with accounting to predicted plant end-of-life state. Safety analyses are revised by accounting for	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	• permitted plant configuration and allowable operating conditions • predicted plant end-of-life state • changes to analytical methods, safety standards and knowledge that invalidate existing safety analysis In order to achieve the above objective, the following guidelines can be used in updating safety analyses: • review safety analysis methods against the applicable standards, and research findings available in Canada and internationally, to identify the elements that should be taken into account • review the changes made in the NPP data, design, operating envelope, and operating procedure, to identify the elements that need to be updated • review information on NPP commissioning and operating experience, both in Canada and worldwide, to identify relevant information that should be accounted for • review the progress in the resolution of previously identified safety analysis issues, to identify the impact on the safety analysis methods and results	plant state covering to at least 2019 (i.e., up to a specified number of EFPDs) rather than end-of- life state.	
4.7	Safety analysis shall be subject to a comprehensive QA program applied to all activities affecting the quality of the results. The QA program shall identify the management system or quality assurance standards to be applied and shall include documented procedures and instructions for the complete safety analysis process, including, but not limited to: 1. collection and verification of NPP data 2. verification of the computer input data 3. validation of NPP and analytical models 4. assessment of simulation results	[DPT-NSAS-00001] procedure on Quality Assurance of Safety Analysis establishes the quality assurance process for performing analysis work in support of nuclear safety assessment. However, use of legacy codes and their qualifications for some analysis predate N286.7 therefore do not meet the requirements for verification of computer input data nor validation of NPP and analytical models (Gap 1). Guidance Consistently followed.	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	5. documentation of analysis results Guidance All sources of data should be referenced and documented, and the various steps of the process should be recorded and archived, to allow independent checking. The safety analysis QA program should comply with regulatory requirements, codes and standards, and be consistent with the best international practices.		
Part II 5. to 8.7		Clauses 5 to 8.7 in Part II of REGDOC-2.4.1 apply only to small reactors and are therefore not applicable.	NA

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 CNSC 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. to 4.1.3		These are assessed in SFR 1.	NR
4.2	The NSCA and the technical safety objectives provide the basis for the following criteria and goals: 1. dose acceptance criteria 2. safety goals Safety analyses shall be performed to confirm that these criteria and goals are met, to demonstrate effectiveness of measures for preventing accidents, and mitigating radiological consequences of accidents if they do occur.	Dose acceptance criteria for DBAs and the plant safety goals for BDBAs are met. Single Failure (SF) and Dual Failure (DF) limits of 5 mSv and 250 mSv respectively are used in Part 3 of the Safety Report. The plant safety goals for BDBAs are 10^{-4} for SCDF and 10^{-5} for LRF (see SFR6 for more details).	C
4.2.1	The acceptance criteria for normal operations are provided in section 6.4. The committed whole-body dose for average members of the critical groups who are most at risk, at or beyond the site boundary, shall be calculated in the deterministic safety analysis for a period of 30 days after the analyzed event. This dose shall be less than or equal to the dose acceptance criteria of: 1. 0.5 millisievert (mSv) for any AOO or 2. 20 mSv for any DBA	Acceptance Criteria, of Part 3 of the Safety Report address radiological doses and derived acceptance criteria for DBAs but not explicitly for AOOs, since the limits for AOOs are currently taken to be the same as for DBAs (Gap 1).	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	The values adopted for the dose acceptance criteria for AOOs and DBAs are consistent with accepted international practices, and take into account the recommendations of the IAEA and the International Commission on Radiological Protection.		
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 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	Bruce A safety goals are less restrictive (larger) than those proposed for new plants (Gap 1). See SFR6 for more details	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	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} Becquerel of iodine-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} Becquerel 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 the risk metrics for external events are conservatively estimated, their summation with the risk metrics for internal events can lead to misinterpretation. Should the		

Article No.	Clause Requirement	Assessment	Compliance Category
	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 CNSC REGDOC-2.4.2, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants.		
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: 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.	DSA in the Safety Report does not distinguish between AOO and DBA and does not address BDBAs explicitly (Gap 1). DECs were not considered in the design basis; however, the design basis includes some event sequences that would be categorized as BDBAs.	Gap
4.2.4 to 4.3.2		These are assessed in SFR 1.	NR
4.3.3	Operational limits and conditions (OLCs) are the set of limits and conditions that can be monitored by or on behalf of the operator, and that can be controlled by the operator.	The completion of the SOE project and subsequent programmatic activities (NK21-CORR-00531-05260) have established a good basis for compliance with CSA N290.15 which include the preparation of all OSRs, IUCs requirements which are consistent	AD

Article No.	Clause Requirement	Assessment	Compliance Category
	The OLCs shall be established to ensure that plants operate in accordance with design assumptions and intent (parameters and components), and include the limits within which the facility has been shown to be safe. The OLCs shall be documented in a manner that is readily accessible for control room personnel, with the roles and responsibilities clearly identified. Some OLCs may include combinations of automatic functions and actions by personnel. OLCs shall include: 1. safety limits 2. limiting safety system settings 3. OLCs for normal operation and AOOs, including shutdown states 4. control system constraints and procedural constraints on process variables and other important parameters 5. requirements for surveillance, maintenance, testing and inspection of the plant to ensure that SSCs function as intended in the design and comply with the requirement for optimization by keeping radiation exposures ALARA, as per the Radiation Protection Regulations 6. specified operating configurations, including operational restrictions in the event of the unavailability of SSCs important to safety 7. action statements, including completion times for actions in response to deviations from the operational limits and conditions The basis on which the OLCs are derived shall be readily available in order to facilitate the ability of plant personnel to interpret, observe and apply the OLCs. Guidance The approaches and terminologies used for OLCs may vary as a result of the practices and regulatory systems that have been established in the country of origin for the plant's design. Regardless of the approaches and terminologies used, the design authority should provide clear definitions of the OLC terminologies used.	with the OLCs and their basis derived from safety analysis. However, gaps in continuous compliance and areas for improvement in programmatic aspects identified in the self-assessment and pilot inspection are being addressed and a transition plan for the introduction of CSA N290.15 in the next licensing period is being prepared.	

Article No.	Clause Requirement	Assessment	Compliance Category
	The design should also include clear objectives and goals for the OLCs. The information related to OLCs should list the relevant standards (national or international) used, and document how the requirements from these standards have been met. OLCs should be defined for a suitable set of bounding plant operating configurations, and be based on the final design of the plant. Additional information Additional information may be found in: o CSA Group, N290.15, Requirements for the safe operating envelope of nuclear power plants, Toronto, Canada. o IAEA Safety Guide NS-G-2.2, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, Vienna, 2000.		
4.3.4 to 5.5		These are assessed in SFR 1.	NR
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. 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	The SOE program ensures that the operation, maintenance and management that are important to safety. Bruce A PROL and LCH identify requirements for the establishment and maintenance of the SOE. The program is established based on the guidance of COG-02-901 P&G on the definition, implementation and maintenance of SOE consistent with CSA N290.15-10 requirements. The implementation and maintenance of documentation shall be maintained in a dynamic suite of documents, to reflect changes in design as the plant evolves. The most relevant implementation procedures are BP-PROC-00363, Nuclear Safety Assessment, DPT-NSAS-00012, Preparation and Maintenance of SOE Requirements, and DPT-RS-00015, Safe Operating Envelope Gap Assessment.	C

Article No.	Clause Requirement	Assessment	Compliance Category
	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 • 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		

Article No.	Clause Requirement	Assessment	Compliance Category
	Activities, Vienna, 2009.		
5.7 to 6.0		These are assessed in SFR 1.	NR
6.1	The design of an NPP shall incorporate defence in depth. The levels of defence in depth shall be independent to the extent practicable. Defence in depth shall be achieved at the design phase through the application of design provisions specific to the five levels of defence. Level One Achievement of Level one defence in depth shall include conservative design and high-quality construction to provide confidence that plant failures and deviations from normal operations are minimized and accidents are prevented. This shall entail careful attention to selection of appropriate design codes and materials, design procedures, equipment qualification, control of component fabrication and plant construction, and use of operational experience. Level Two Level two shall be achieved by controlling plant behaviour during and following a postulated initiating event (PIE) using both inherent and engineered design features to minimize or exclude uncontrolled transients to the extent possible. Level Three Achievement of Level three defence in depth shall include the provision of inherent safety features, fail-safe design, engineered design features, and procedures that minimize the consequences of DBAs. These provisions shall be capable of leading the plant first to a controlled state, and then to a safe shutdown state, and maintaining at least one barrier for the confinement of radioactive material. Automatic activation of the engineered design features shall minimize the need for operator actions in the early phase of a DBA.	Level 2 defence-in-depth is not demonstrated explicitly for AOOs (Gap 1).	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	Level Four Level four shall be achieved by providing equipment and procedures to manage accidents and mitigate their consequences as far as practicable. Most importantly, adequate protection shall be provided for the confinement function by way of a robust containment design. This includes the use of complementary design features to prevent accident progression and to mitigate the consequences of DECs. The confinement function shall be further protected by severe accident management procedures. Level Five The design shall provide adequately equipped emergency support facilities, and plans for onsite and offsite emergency response. Guidance IAEA INSAG-10, Defence in Depth in Nuclear Safety, provides information regarding the concept and application of defence in depth. Guidance on performing a systematic assessment of the defence in depth can be obtained from the IAEA safety reports series No. 46, Assessment of Defence in Depth for Nuclear Power Plants. The application of defence in depth in the design should ensure the following: • The approach to defence in depth used in the design should ensure that all aspects of design at the SSCs level have been covered, with emphasis on SSCs that are important to safety. • The defence in depth should not be significantly degraded if the SSC has multiple functions (e.g., for CANDU reactors, the moderator and end-shield cooling systems may serve the functions of a process system and include the functions of mitigating DECs). • The principle of multiple physical barriers to the release of radioactive material should be incorporated in the design; there should		

Article No.	Clause Requirement	Assessment	Compliance Category
	be a limited number of cases where there is a reduction in the number of physical barriers (as may be the case where some components carrying radioactive material serve the function of primary coolant barrier and containment), and adequate justification should exist for such design choices. • The design (e.g., in safety design guides, management system programs) should provide: • levels of defence in depth that are addressed by individual SSCs • supporting analysis and calculation • evaluation of operating procedures • The safety analysis should demonstrate that the challenges to the physical barriers do not exceed their physical capacity. • The structure for defence in depth provisions at each level of defence should be established for a given plant design, and the evaluation of the design from the point of view of maintaining each safety function should be carried out. This evaluation should consider each and every one of the provisions for mitigation of a given challenge mechanism, and confirm that it is well founded, sufficient, feasible, and correctly engineered within the design. • Special attention should be given to the feasibility of a given provision and the existence of supporting safety analyses. Deficiencies in the completeness of the supporting safety analyses should be documented and flagged as issues to be queried. To ensure that different levels of defence are independently effective, any design features that aim to prevent an accident should not belong to the same level of defence as design features that aim to mitigate the consequences of the accident. The independence between all levels of defence should be achieved, in particular, through diverse provisions. The strengthening of each of these levels separately would provide, as far as reasonably achievable, an overall reinforcement of defence in depth. For example, the use of dedicated systems to deal with DECs ensures the independence of the		

Article No.	Clause Requirement	Assessment	Compliance Category
	fourth defence level.		
6.1.1 to 6.3		These are assessed in SFR 1.	NR
6.4	Achievement of the general nuclear safety objective (discussed in section 4.1) depends on all actual and potential sources of radiation being identified, and on provision being made to ensure that sources are kept under strict technical and administrative control. Radiation doses to the public and to site personnel shall be as low as reasonably achievable. During normal operation, including maintenance and decommissioning, doses shall be regulated by the limits prescribed in the Radiation Protection Regulations. The design shall include provisions for the prevention and mitigation of radiation exposures resulting from DBAs and DECs. The design shall also ensure that potential radiation doses to the public from AOOs and DBAs do not exceed dose acceptance criteria provided in section 4.2.1. The calculated overall risk to the public shall meet the safety goals in section 4.2.2. Guidance A detailed radiation dose assessment should include estimated annual collective and individual effective and equivalent radiation doses to site personnel and members of the public for normal operation, potential radiation doses to the public for AOOs and DBAs, and potential releases into the environment for DECs. The assessment process should be clearly documented and should include the process for consideration and evaluation of dose-reduction changes in the NPP design. Radiation doses resulting from the operation of the NPP should be reduced by means of engineered controls and radiation protection measures to levels such that any further expenditure on design, construction and operational measures would not be warranted by the expected reduction in radiation doses. The radiation dose assessment should include the expected occupancy of the NPP's radiation areas, along with estimated annual person-	DSA in the Safety Report does not distinguish between AOO and DBA and does not address BDBAs explicitly (Gap 1). Bruce A design basis includes some event sequences that would be categorized as BDBAs, however, Bruce A does not meet this requirement intended for new builds (Gap 2). The limits for AOOs are currently taken to be the same as for DBAs (Gap 3). This is the same gap identified for Clause 4.2.1.	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	Sievert doses associated with major functions, including radioactive waste handling, normal maintenance, special maintenance, refuelling and in-service inspection. Such assessments should include information as to how ALARA and operating experience are used in the design to deal with dose-significant contributors. Additional information Additional information may be found in: • CNSC, G-129, rev. 1, Keeping Radiation Exposures and Doses “As Low as Reasonably Achievable (ALARA)”, Ottawa, Canada, 2004. • CSA Group, N288.2, Guidelines for Calculating Radiation Doses to the Public from a Release of Airborne Radioactive Material under Hypothetical Accident Conditions in Nuclear Reactors, Toronto, Canada.		
6.5 to 6.6		These are assessed in SFR 1.	NR
6.6.1	The design shall take due account of challenges to multiple units at a site. Specifically, the risk associated with common-cause events affecting more than one unit at a time shall be considered. Guidance The presence of multiple units at a site, or common-cause events could exacerbate challenges that the plant personnel would face during an accident. The events and consequences of an accident at one unit may affect the accident progression or hamper accident management activities at the neighbouring unit; available resources (personnel, equipment and consumable resources) would need to be shared among several units. These challenges should be identified and the available resources and mitigation strategies shown to be adequate.	Common-cause events are not analyzed explicitly in Part 3 of the Safety Report (Gap 1). This gap is scheduled to be considered early within Safety Report update towards the compliance with REGDOC-2.4.1.	Gap
7. to 7.3.4.1		These are assessed in SFR 1.	NR

Article No.	Clause Requirement	Assessment	Compliance Category
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. 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 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.	A systematic event identification process is not well documented and/or demonstrated. Postulated initiating events are not categorized into AOOs, DBAs or BDBAs (Gap 1). For more details, see Assessment against REGDOC-2.4.1.	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	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.		
7.4.1 to 7.5		These are assessed in SFR 1.	NR
7.6 to 7.6.1.3		These are assessed in SFR 1 and SFR 6.	NR
7.6.2	All safety groups shall function in the presence of a single failure. The single-failure criterion requires that each safety group can perform all safety functions required for a PIE in the presence of any single component failure, as well as: 1. all failures caused by that single failure 2. all identifiable but non-detectable failures, including those in the non-tested components 3. all failures and spurious system actions that cause (or are caused by) the PIE Each safety group shall be able to perform the required safety functions under the worst permissible systems configuration, taking into account such considerations as maintenance, testing, inspection and repair, and equipment outage. Analysis of all possible single failures, and all associated consequential failures, shall be conducted for each component of each safety group until all safety groups have been considered. Unintended actions and failure of passive components shall be considered as two of the modes of failure of a safety group. The single failure shall be assumed to occur prior to the PIE, or at any	The analyses do not follow newer, more restrictive, interpretations of the single failure criterion (Gap 1).	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	time during the mission time for which the safety group is required to function following the PIE. Passive components may be exempt from this requirement. Exceptions to the single-failure criterion shall be infrequent, and clearly justified. Exemptions for passive components may be applied only to those components that are designed and manufactured to high standards of quality, that are adequately inspected and maintained in service, and that remain unaffected by the PIE. Design documentation shall include justification of such exemptions, by analysis, testing or a combination of analysis and testing. The justification shall take loads and environmental conditions into account, as well as the total period of time after the PIE for which the functioning of the component is necessary. Check valves shall be considered to be active components if they must change state following a PIE. Guidance The application of the single-failure criterion (SFC) in design should follow a systematic approach applied to all safety groups. The approach should be adequately verified, such as by using failure modes and effects analysis. The SSCs inside the safety group should include both the primary SSCs and the supporting SSCs. The detectability of failures is implicit in the application of the SFC. Detectability is a function of the system design and the specified tests. A failure that cannot be detected through periodic testing, or revealed by alarm or anomalous indication, is non-detectable. An objective in a single- failure analysis is to identify non-detectable failures. To deal with identifiable but non-detectable failures, the following actions should be considered: • preferred action: the system or the test scheme should be redesigned to make the failure detectable • alternative action: when analyzing the effect of each single failure, all identified non- detectable failures should be assumed to have occurred. Therefore, the design should take appropriate measures to address these non-detectable failures, such as adequate redundancy		

Article No.	Clause Requirement	Assessment	Compliance Category
	and diversity Justification in support of an exception to the SFC should consider the consequences of failure, practicality of alternatives, added complexity and operational considerations. The integrated effect of all exceptions should not significantly degrade safety; in particular, defence in depth should be preserved. For passive components that are exempt from the SFC, the following should be considered in order to demonstrate a high degree of performance assurance: • adequate testing during the manufacturing stage • sample testing from those components received from the manufacturer • adequate testing during construction and commissioning stages • necessary testing to verify their reliability after the components have been removed from service during the operation stage Any consideration for an exception to the SFC during testing and maintenance should fall into one of the following permissible categories: • the safety function is provided by two redundant, independent systems (e.g., two redundant, fully effective, independent cooling means) • the expected duration of testing and maintenance is shorter than the time available before the function is required following an initiating event (e.g., spent fuel storage pool cooling) • the loss of safety function is partial and unlikely to lead to significant increase in risk even in the event of failure (e.g., small area containment isolation) • the loss of system redundancy has minor safety significance		

Article No.	Clause Requirement	Assessment	Compliance Category
	(e.g., control room air filtering) • the loss of system redundancy may slightly increase PIE frequency, but does not impact accident progression (e.g., leak detection) A request for an exception during testing and maintenance should also be supported by a satisfactory reliability argument covering the allowable outage time. The OLCs should clearly state the allowable testing and maintenance time, along with any additional operational restrictions, such as suspension of additional testing or maintenance on a backup system for the duration of the exception. Additional information Additional information may be found in: • IAEA, Safety Series No. 50-P-1, Application of the Single Failure Criterion, Vienna, 1990. • Institute of Electrical and Electronics Engineers (IEEE), Standard 379, Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems, Piscataway, New Jersey, 1988.		
7.6.3 to 8.4		These are assessed in SFR 1.	NR
8.4.1	The design authority shall specify derived acceptance criteria for reactor trip parameter effectiveness for all AOOs and DBAs, and shall perform a safety analysis to demonstrate the effectiveness of the means of shutdown. For each credited means of shutdown, the design shall specify a direct trip parameter to initiate reactor shutdown for all AOOs and DBAs in time to meet the respective derived acceptance criteria. Where a direct trip parameter does not exist for a given credited means, there shall be two diverse trip parameters specified for that means. For all AOOs and DBAs, there shall be at least two diverse trip	The analysis in Part 3 of the Safety Report is consistent with demonstrating that both redundant shutdown systems are effective independently in shutting down the reactor. With the exception of a few justified cases, trip coverage maps for the various events demonstrate that two trips are effective. Acceptance criteria are not explicitly specified for AOOs (Gap 1). See assessment against REGDOC-2.4.1 requirements.	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	parameters unless it can be shown that failure to trip will not lead to unacceptable consequences. There shall be no gap in trip coverage within the OLCs for any operating condition (such as power, temperature), taking into account plant aging. This shall be ensured by the provision of additional trip parameters if necessary. A different level of effectiveness may be acceptable for the additional trip parameters. The extent of trip coverage provided by all available parameters shall be documented for the entire spectrum of failures for each set of PIEs. An assessment of the accuracy and the potential failure modes of the trip parameters shall be provided in the design documentation. Guidance The effectiveness of trip parameters should be assessed through safety analysis performed in accordance with REGDOC-2.4.1, Deterministic Safety Analysis. Trip coverage should be demonstrated across the full range of operating states, for all credited shutdown means and all credited trip parameters. Note that the number of credited shutdown means and the number of credited trip parameters can vary with the event, the reactor design, and whether there is a direct trip available. Defining derived acceptance criteria appropriate to a particular design is the responsibility of the design authority. CNSC REGDOC-2.4.1, Deterministic Safety Analysis, provides the requirements. Derived acceptance criteria should be defined separately for AOOs and DBAs. The derived acceptance criteria should be set to give an appropriate level of confidence that a fundamental safety function is assured, or that a barrier to fission product release will not fail. The derived acceptance criteria should: • be quantifiable and well understood • account for the fact that the safety analysis is stylized, and the plant condition at the time of the accident may be significantly different from the analyzed state		

Article No.	Clause Requirement	Assessment	Compliance Category
	• cover uncertainties in analysis, input plant and analysis parameters, as well as code validation Direct trips are the preferred means of actuating a shutdown means, due to their robustness and low dependence on calculational models. Diverse trip parameters measure different physical variables on the reactor, thus providing additional protection against common mode failure. Where it is impracticable to provide full diversity of trip parameters, different measurement locations, different instrument types and different processing computers should be provided. Manual trip is considered an acceptable trip parameter, if the operator has adequate time to initiate the shutdown action following unambiguous indication of the need to perform the action (in accordance with section 8.10.4). It is the responsibility of the design authority to identify and justify those trip parameters that can be considered “direct”. The design authority should also demonstrate that any trip parameters that are a measure of the event, but not a measure of the challenge to acceptance criteria, cannot be “masked” or “blinded” by control system action or other means. Trips that are dependent on a number of measured variables, such as low DNBR (departure from nucleate boiling ratio) trips in PWRs can only be considered direct if all the variables are direct. Guidance on applying the requirements for number and diversity of trip parameters is given in REGDOC-2.4.1, Deterministic Safety Analysis. REGDOC-2.4.1 also provides the minimum expectations for the number of trip parameters. A manual reactor trip can be considered to be equivalent to a trip parameter, if the requirements for crediting operator action from the main control room are met (see section 8.10.4) and the reliability of manual shutdown meets the reliability requirements for an automatic trip.		
8.4.2		This is assessed in SFR 1 and SFR 6.	NR

Article No.	Clause Requirement	Assessment	Compliance Category
8.4.3 to 8.10.3		These are assessed in SFR 1.	NR
8.10.4	If operator action is required for actuation of any safety system or safety support system equipment, all of the following requirements shall apply: 1. there are clear, well-defined, validated, and readily available operating procedures that identify the necessary actions 2. there is instrumentation in the control rooms to provide clear and unambiguous indication of the necessity for operator action 3. following indication of the necessity for operator action inside the control rooms, there are at least 30 minutes available before the operator action is required 4. following indication of the necessity for operator action outside the control rooms, there is a minimum of 1 hour available before the operator action is required For automatically initiated safety systems and control logic actions, the design shall facilitate backup manual initiation from inside the appropriate control room. Guidance The design should ensure that no failure of monitoring or display systems will influence the functioning of other safety systems. The available time before operator action can be credited should be counted from the receipt of an unambiguous indication of a potential accident (typically an alarm) and includes diagnostic time. The time available to perform the actions should be based on the analysis of the plant response to AOOs and DBAs, using realistic assumptions. The time required for operator action should be based on a human factors engineering analysis of operator response time, which (in turn) is based on a documented sequence of operator actions. Uncertainties in the analysis of time required are identified and assessed. An adequate time margin should also be added to the	Operator actions in Part 3 of the Safety Report are assumed to be 15 minutes for actions inside the control room and 30 minutes for actions outside the control room. These assumptions do not meet the proposed values of REGDOC-2.5.2 for new plants (Gap 1). They are consistent with the guidance of REGDOC-2.4.1 and CSA N290.1.	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	analyzed time. If operator action is required for actuation of any safety function, other than meeting the requirements of this regulatory document, the analysis should also demonstrate that: • there is sufficient time available for the operator to perform the required manual action • the operator can perform the actions correctly and reliably in the time available The sequence of actions should use only alarms, controls, and displays that would be available in locations where the tasks will be performed and should be available in all scenarios analysed. A preliminary validation should be conducted, to provide independent confirmation to the validity of the estimated “time available” and “time required” for human actions. The preliminary validation results should support the conclusion that the time required, including margin, to perform individual steps and the overall documented sequence of manual operator actions are reasonable, realistic, repeatable, and bounded by the initial analysis. An integrated system test should also be conducted, to validate the manual actions credited in the safety analysis, using a full-scale simulator. Tasks conducted outside the control room should be included in the integrated system validations. Where justified, alternative action times may be used. The alternative action times should make due allowance for the complexity of the action to be taken, and the time needed for activities such as diagnosing the event and accessing the field location. Additional information Additional information may be found in: • ANSI/ANS, 58.8, Time Response Design Criteria for Safety Related Operator Actions, La Grange Park, Illinois, 2008. • CSA Group, N290.4, Requirements for Reactor Control		

Article No.	Clause Requirement	Assessment	Compliance Category
	Systems of Nuclear Power Plants, Toronto, Canada. • CNSC, G-225, Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills, Ottawa, Canada, 2001, or successor document. • IEC, 60964, Nuclear Power Plants - Control Rooms – Design, Geneva, 2009. • IEC, 60965, Nuclear Power Plants - Control Rooms - Supplementary Control Points for Reactor Shutdown Without Access to the Main Control Room, Geneva, 2009. • NEI 99-03, Control Room Habitability Assessment Guidance, Washington, D.C., 2001. • U.S. NRC, NUREG-0696, Functional Criteria for Emergency Response Facilities, Washington, D.C., 1981. • U.S. NRC, Regulatory Guide 1.196, Control Room Habitability at Light-Water Nuclear Power Reactors, Washington, D.C., 2003.		
8.11 to 9.		These are assessed in SFR 1.	NR
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.	As for clause 7.4, systematic methodology for event identification is not demonstrated (Gap 1).	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
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 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 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	The new safety analysis for events impacted by ageing includes ageing effects. Part 3 of the Safety Report demonstrates the effectiveness of the safety systems and safety support systems and the capability of the design in withstanding the analyzed DBAs. The Safety Limits identified in the OSRs are based on the analysis limits used in the safety analysis and supporting documents after an accounting for the associated instrumentation uncertainty. The analysis assumptions, including any credited operator action, are considered in relevant emergency response and accident management procedures and manuals. A summary of the operator actions credited in the various events is given in Part 3 of the Safety Report. The dose and other acceptance criteria for AOOs are not explicitly assessed in Part 3 of the Safety Report (Gap 1). The deterministic safety analysis of BDBAs are not included in the Safety Report, however, they are analyzed within PRA scope. PRA results shows that the plant safety goals are met (see SFR6 for more details). Guidance Not applicable	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	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.		
9.3		This is assessed in SFR 1.	NR
9.4	The deterministic safety analysis shall be conducted in accordance with the requirements specified in CNSC regulatory document REGDOC-2.4.1, Deterministic Safety Analysis. Additional information Additional information may be found in: • CNSC, REGDOC-2.4.1, Deterministic Safety Analysis, Ottawa, Canada, 2014. • CNSC, RD/GD-369, Licence Application Guide: Licence to Construct a Nuclear Power Plant, Ottawa, Canada, 2011. • CSA Group, N286.7.1, Guideline for the Application of N286.7-99, Quality Assurance of Analytical, Scientific, and Design Computer Programs for Nuclear Power Plants, Toronto, Canada. • CSA Group, N286.7, Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants, Toronto, Canada. • IAEA, SSG-2, Deterministic Safety Analysis for Nuclear Power Plants, Vienna, 2009. • IAEA NS-G-1.2, Safety Assessment and Verification for Nuclear Power Plants, Vienna, 2001.	Assessment against REGDOC-2.4.1 identified gaps in the deterministic safety analysis that are related to; • event identification and classification (Gap 1), • treatment of modeling uncertainty (Gap 2), and • the use of legacy tools for some analysis (Gap 3). For more details, see REGDOC-2.4.1.	Gap
9.5		This is assessed in SFR 6.	NR
9.5 to 10.2		These are assessed in SFR 1.	NR

B.3. CNSC REGDOC-2.3.2, Accident Management

In support of the review tasks listed in Section 5, relevant clauses of CNSC REGDOC-2.3.2 have been assessed in Table B3. A more detailed assessment is performed in “Safety Factor 13: Emergency Planning”.

Table B3: CNSC REGDOC-2.3.2, Accident Management

Article No.	Clause Requirement	Assessment	Compliance Category
3.	This section specifies the requirements for an IAMP. The first subsection sets the goals of accident management. The second subsection gives the general or high-level requirements. Then, specific requirements covering various elements for an IAMP are grouped under the requirements for equipment, procedures, and organizational and human aspects.	This is not a requirement/guidance clause.	NA
3.1	In accordance with the NSCA and associated regulations, the overarching nuclear safety objective is to protect individuals, society, and the environment from harm by establishing and maintaining effective defences against radiological hazards and hazardous substances. When an accident occurs in a nuclear reactor facility, the above objective is achieved by fulfilling the following fundamental safety functions: • control of reactivity • removal of heat from the fuel • confinement of radioactive material • shielding against radiation • control of operational discharges and hazards substances, as well as limitation of accidental releases • monitoring of safety-critical parameters to guide operator actions	Bruce Power emergency measures program BP-PROG-08.01 takes authority from the Management System Manual BP-MSM-1. The program is consistent with the intent of REGDOC-2.3.2 goals. The purpose of the program is to describe how Bruce Power manages risks that have the potential to impact reactor safety, public safety, employee and responder safety, environmental safety and corporate reputation through a risk-based program of prevention, mitigation, preparedness, response, and recovery.	C

Article No.	Clause Requirement	Assessment	Compliance Category
	The specific goals of a comprehensive and effective IAMP are to: 1. terminate the progression of the accident as early as possible 2. prevent an accident from leading to severe consequences 3. maintain the integrity of fission product barriers including containment and spent fuel storage 4. minimize the release of radioactive materials into the environment 5. achieve a long-term safe stable state of the reactor core or spent fuel storage To fulfill these high-level requirements, the licensee shall meet all the requirements specified in this section and consider the guidance given in sections 4, 5, 6 and 7.		
3.2	In support of the development, implementation, and validation of an IAMP, licensees shall: 1. develop and implement a reactor-specific IAMP, to ensure that adequate capabilities are maintained to cope with scenarios ranging from AOOs to severe accidents 2. address, to the extent practicable, the initiating events that have the potential to cause extensive infrastructure damage such that offsite resources are not readily available 3. ensure that the IAMP covers all modes of reactor operation including the shutdown state; events that could cause damage to the fuel in a reactor core, in transport to storage, or stored in a spent fuel pool shall be considered 4. identify and document challenges to safety functions and physical barriers and perform safety analysis 5. identify and confirm reactor site capabilities to cope with the challenges to safety functions in performing accident management actions 6. conduct periodic reviews, drills and integrated exercises to confirm	The Emergency Management Program BP-PROG-08.01 is developed to enable effective response to all hazards at Bruce Power. This considers the following: - Design basis accidents - Beyond design basis accidents - Other emergencies (e.g. Conventional) leading to nuclear emergencies - Multi-unit accident scenarios, if applicable BP-PROG-08.01 outlines an Integrated Management System (IMS) approach to addressing the program objectives where applicable through a systematic Plan, Do, Check, Act process. This program is implemented by 13 plans and procedures including BP-PLAN-00001, Bruce Power Nuclear Emergency Plan and BP-PROC-00659, Severe Accident Management Procedure. The Plans address the following objectives where applicable: - Identification and classification of hazardous conditions and events.	C

Article No.	Clause Requirement	Assessment	Compliance Category
	or improve the effectiveness of the established IAMP 7. ensure that the IAMP interfaces with the emergency preparedness program 8. make accident management provisions, including: a. developing criteria for use in determining what procedures to use b. demonstrating the capability to take actions to protect and inform personnel at the scene c. identifying the roles and responsibilities of the personnel responsible for accident management d. identifying and evaluating reactor systems and features suitable for use during accident management e. providing adequate training to personnel involved in managing an accident	- Development of procedures describing the response to hazardous conditions and events and recovery from the consequences of those events. - Establishment of response organizations. - Establishment of response facilities and equipment. - Establishment of Recovery Organization. - Communication to the applicable stakeholders (employees, public, regulatory agencies) as appropriate. - Evaluation of program effectiveness. BP-PROG-08.01, Emergency Management Program performance is assessed in relation to its purpose using the criteria found in BP-PROC-00010, Emergency Management Drills and Exercises. Program Assessment results are reported to Bruce Power Management and corrective actions developed and implemented to address those gaps, if required. The purpose of the Bruce Power Nuclear Emergency Response Plan (NERP) [BP-PLAN-00001] is to describe the concepts, structures, roles, and processes needed to implement and maintain Bruce Power's capability to prepare for and to respond to a nuclear radiological emergency. This Plan outlines the command, control, and coordination structure and activities, activation, site integration, external agency coordination, deployment of emergency resources, and emergency facilities through the use Emergency Response Procedures developed to guide effectively trained emergency response staff in emergency response and mitigation techniques. The operation-based implementing documents are the Abnormal Incidents Manuals (AIMs) which include procedures that are specifically established to mitigate various design basis events, and Severe Accident Management Guidance (SAMG) for use if the plant has entered, or is going to enter, a state outside its design and analysis base.	

Article No.	Clause Requirement	Assessment	Compliance Category
3.3		This is assessed in SFR 13.	NR
3.4	Licensees shall: 1. develop, verify and validate accident management procedures and guidelines, including EOPs and SAMGs 2. account for factors specific to the reactor design in the development of SAMGs for severe accidents 3. consider that information available to the operating staff or emergency groups may be incomplete and characterized by significant uncertainties 4. include the following in SAMGs: a. the parameters and their thresholds that define the transition from EOPs to SAMGs b. key parameters to diagnose the state of various reactor and reactor systems throughout the progression of the accident c. actions to be taken to counter the damage mechanisms that would potentially challenge the integrity of the containment, irrespective of predicted frequencies of occurrence for those damage mechanisms d. indicators that can be used to judge the success of the implemented actions e. the communication protocol to be followed during implementation of accident management f. guidance on dealing with multi-unit damage, uncovered fuel in spent fuel pools, releases of radioactive materials and hydrogen into buildings adjacent to the containment 5. ensure the EOPs and SAMGs consider sufficiently long time periods to initiate and complete required actions, taking into account the human and organizational performance and the possibility of prolonged time required to restore power due to multi-unit damage or large-scale external disturbances	A comprehensive set of Bruce Power specific AIMs and SAMG procedures are prepared. The technical basis, entry and exit conditions, and assumptions used in AIM procedures make use of the deterministic analysis of the design basis events, while those used in SAMG technical basis are largely based on the deterministic safety analysis of severe BDBAs analyzed within PRA Level 2 scope, as well as PRA Level 1 and 2. Significant progress has been made on a large number of planned post Fukushima design enhancements to prevent and mitigate severe accidents. These enhancements include, e.g., adding design features to allow external water makeup to the HTS, moderator system, steam generators and the irradiated fuel bay, as well as enhancements to the emergency power supply. PRA assessments with taking into account Emergency Mitigation Equipment demonstrate significant improvements in SCDF and releases (see SFR6 for details). The SAMG was developed to guide response to a severe accident occurring on a single unit only. For multi-unit sites, Bruce A PRA indicates that multi-unit events are considered. The completeness of such consideration needs to be confirmed, in particular, it may require complementary DSA for BDBAs to confirm meeting the safety goals (Gap 1).	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	6. include necessary steps into guidelines for events where supplementary equipment (also called emergency mitigating equipment (EME)) and where external supports are required to mitigate the accident consequences 7. provide for transition from the accident management activities to accident recovery		
3.5 to 4.2		These are assessed in SFR 13.	NR
4.2.1	The development of an IAMP should consider postulated initiating events and accident sequences that could be caused by credible failures or malfunctions of SSCs, human errors, common-cause internal and external hazards, and combinations thereof. Challenges that are not considered in the reactor design envelope, but could potentially threaten the integrity of the containment should be practically eliminated; that is, the existing process systems, safety and control systems, complementary design features, available SSCs, and procedural provisions should make the occurrence of these challenges practically impossible. For example, the installed rupture disks or relief valves that provide reliable and sufficient depressurization capability for a reactor core or vessel can eliminate the high-pressure corium ejection phenomenon and thus the possibility of direct containment heating by corium. Among credible events, a selected set of accident sequences that can be used to represent the consequences of each group of accident sequences should be used to obtain insights into the behaviour of the accident and to identify challenges to reactor safety functions. This requires investigating how specific accidents will challenge safety functions and – if safety functions are lost and not restored in due time – how the accident progresses, how the fission product barriers are breached, how long it will take to reach each stage of the accident, and how severe each accident stage will be. In the domain of beyond-design-basis accidents (BDBA), insights into the response of the reactor to BDBAs, including severe accidents, should be obtained. A technical basis for SAM should document the	The Emergency Management Program BP-PROG-08.01 is developed to enable effective response to all hazards at Bruce Power. This considers the following: - Design basis accidents - Beyond design basis accidents - Other emergencies (e.g. Conventional) leading to nuclear emergencies - Multi-unit accident scenarios, if applicable. Bruce Power specific AIMs are developed to address DBAs and SAMG procedures are prepared to address severe accidents. Bruce Power NERP [BP-PLAN-00001] is developed to maintain an Emergency Plan and an organization to implement that focuses on an all hazards' approach to response requirements. In addition, response to design basis events, this plan takes into account requirements to support a sustained response to a Beyond Design Basis multi-unit event resulting in an extended loss of off-site power for up to 72 hours without assistance. The technical bases for AIMs are provided by the safety analysis of DBAs in Part 3 of the Safety Report. SAMG technical basis is largely based on the deterministic safety analysis of selected severe BDBAs representing various groups of severe events. The deterministic safety analysis of these representative severe events is performed using MAAP-CANDU within PRA Level 2 scope. The SAMG was developed to guide response to a severe accident	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	understanding of severe accident phenomena and reactor-specific physical processes, such as core degradation, in-vessel core debris retention, ex-vessel corium spreading and coolability, molten fuel coolant interaction, molten core concrete interaction, and all known containment challenge mechanisms. The technical basis should also include severe accident phenomena in spent fuel bays and multi-unit distress. The technical basis should be updated as necessary to reflect the state-of-the- art knowledge and experimental data obtained from applicable severe accident research programs and lessons learned from the reactors that have experienced severe core damage. The updated knowledge and data should be used to evaluate the reactor ability to cope with accidents and to deduce suitable accident management strategies, provisions, procedures, and guidelines. Reactor-specific beyond-design-basis initiating events, such as events triggered by extreme external hazards (e.g., earthquakes, flooding, and extreme weather conditions), should also be considered to increase the reactor coping capability. The aim is to ensure that a set of sufficient, supplementary onsite equipment and consumables (e.g., fuel and water inventories) are identified, obtained, protected and stored onsite or offsite. These can be used to maintain or restore the cooling of the core, the containment, and the spent fuel pool following a beyond-design-basis initiating event. After the consumables are used up, offsite resources should be obtained to sustain those cooling functions indefinitely. Accident management should consider that some beyond-design-basis initiating events may result in similar challenges to all units on the site. Challenges for severe accidents and beyond-design-basis initiating events may be identified using a targeted assessment of safety margins against a set of postulated extreme conditions that cause a consequential loss of safety functions leading to severe core damage. Such a reactor-specific “stress test” can be used to determine the time of autonomy of reactor-critical safety functions, any potential weak points, and any cliff-edge effects for a given set of the considered extreme situations. This type of exercise may be used to identify the potential for safety improvements and to provide input to the	occurring on a single unit only. Bruce A PRA indicates that multi-unit events are considered. The completeness of such consideration needs to be confirmed, in particular, it may require complementary DSA for BDBAs to confirm meeting the safety goals (Gap 1).	

Article No.	Clause Requirement	Assessment	Compliance Category
	development of an IAMP.		
4.2.2	Similar to identification of challenges, all reactor capabilities to fulfill the safety functions and to preserve fission product barriers during DBAs or BDBAs should be investigated in terms of capabilities of both SSCs and personnel. Reactor capabilities to cope with BDBAs by the available SSCs including the complementary design features should be identified, including the use of non- dedicated systems, external water sources, temporary connections (hoses, mobile or portable equipment), and offsite hardware and personnel resources. Considerations should also be given to whether failed systems can be restored to service. In addition, an assessment should be made of how operator actions are carried out to mitigate accident consequences. Multiple diverse SAM measures should be provided for significant challenges to containment integrity. Consideration should be given to both the benefit and potential negative impact of using portable or supplementary equipment to cope with beyond–design-basis initiating events. Relevant information including lessons learned from past nuclear accidents as well as data from experimental activities should be considered during the identification of reactor capabilities.	Reactor capabilities in protecting and mitigating DBAs are demonstrated through the analysis of the DBAs and the demonstration of meeting their dose acceptance criterion and the other applicable acceptance criteria related to integrity of barriers to fission products release. DBA event sequences and assumptions including relevant operator actions are considered in AIMs. Significant progress has been made on a large number of planned post Fukushima design enhancements to prevent and mitigate severe accidents. These enhancements include, e.g., adding design features to allow external water makeup to the HTS, moderator system, steam generators and the irradiated fuel bay, as well as enhancements to the emergency power supply. PRA assessments with taking into account Emergency Mitigation Equipment demonstrate significant improvements in SCDF and releases (see SFR6 for details).	C
4.2.3		This is assessed in SFR 13.	NR
4.2.4	Safety analysis to support an IAMP can be largely based on the existing analysis (e.g., documented in safety reports or probabilistic safety assessment [PSA] documents). Additional analysis, if required, should be performed specifically to address accident management issues. Safety analysis should be used to assist in developing an IAMP by: • formulating the technical basis for identification of reactor challenges and capabilities and development of strategies, measures, procedures and guidelines	The technical basis, entry and exit conditions, and assumptions used in AIM procedures make use of the deterministic analysis of the design basis events, while those used in SAMG technical basis are largely based on the deterministic safety analysis of severe BDBAs analyzed within PRA Level 2 scope, as well as PRA Level 1 and 2. Significant progress has been made on a large number of planned post Fukushima design enhancements to prevent and mitigate severe accidents. These enhancements include, e.g., adding design features to allow external water makeup to the HTS,	C

Article No.	Clause Requirement	Assessment	Compliance Category
	• demonstrating the acceptability of the identified solutions to support the selected strategies, measures, procedures and guidelines against the established criteria • determining the reference source terms and accident conditions for environmental qualification of equipment for DBAs and survivability/operability assessments of equipment for BDBAs, including severe accidents Safety analysis performed to support SAM should use the best-estimate approach. Uncertainties in the analytical prediction of challenges to fission product barriers should be taken into account if the level of knowledge of important severe accident phenomena and physical processes is low and if the associated supporting experimental data are insufficient. Necessary computational aids should be identified and developed to assist in the overall success of accident management activities performed by the response organization prior to an actual event. These computational aids are typically obtained using simplified assumptions and are often presented graphically. The results of deterministic severe accident analysis should assist the licensee to: • specify the criteria that would indicate the onset of severe core damage • identify the symptoms (i.e., parameters and their values) by which reactor personnel may determine the reactor core condition and state of protective barriers • identify the challenges to fission product boundaries in different reactor states, including shutdown states • evaluate the timing of such challenges to improve the potential for successful human intervention • identify the reactor systems and materiel resources that may be used for SAM purposes • assess that SAM actions would be effective to counter	moderator system, steam generators and the irradiated fuel bay, as well as enhancements to the emergency power supply. PRA assessments with taking into account Emergency Mitigation Equipment demonstrate significant improvements in SCDF and releases (see SFR6 for details). Safety analysis for severe accidents within PRA scope is based on using best estimate methods. The Safety Report includes events that would be classified as BDBAs. These BDBAs were performed using conservative methods.	

Article No.	Clause Requirement	Assessment	Compliance Category
	challenges to protective barriers • evaluate performance of equipment and instrumentation under accident conditions • develop and validate computational aids for SAM For severe accidents, the results of PSA should assist the licensee to: • verify that SAM would be effective for representative severe accident sequences, including multi-unit events, events triggered by natural and human-induced external hazards, and events involving an extended loss of all AC power • provide a basis for assessing safety benefits of potential design enhancement options • identify accident scenarios for personnel training and drill purposes The credited human actions in preparation of the IAMP should be supported with adequate analyses. Considerations should be given to: • the instrumentation to provide clear and unambiguous indication of the need to take action • allowing sufficient time for the operator to detect and diagnose the event, and carry out the required actions • environmental conditions that do not prevent safe completion of the operator action • the required training		
4.2.5	Procedures and guidelines to implement the strategies and measures for accident management should be developed and described in documents such as EOPs and SAMGs, or equivalent documents (see the requirements specified in section 3.4). If EOPs and SAMGs already exist, the IAMP can be built using these existing elements. Any new information on reactor site configuration, changes in hazards, and knowledge gained should be considered, and if	AIMs and SAMG procedure meet the general intent of this guidance. There is a gap against this clause requirement relevant to events with multi-unit. As identified against previous clauses (Gap 1).	Gap

Article No.	Clause Requirement	Assessment	Compliance Category
	appropriate procedures and guidelines should be updated accordingly. The EOPs should contain a set of information, instructions and actions designed to prevent the escalation of an accident, mitigate its consequences and bring the reactor to a safe and stable state. The SAMGs should contain a set of information, instructions and actions designed to mitigate the consequences of a severe accident according to the chosen strategies. Uncertainties may exist both in the reactor status and in the outcome of a selected action. Therefore, SAMGs should propose a range of possible actions and allow for additional evaluation and alternative actions. SAMGs should also address various positive and negative consequences of proposed actions, including the use of equipment, limitations of the equipment, cautions and benefits. The procedures and guidelines should be verified and validated. This should include the usability of the procedures and guidelines (see section 5.2). Clear criteria for EOP to SAMG transition should be defined. Adequate guidance should be provided in the design of the IAMP to ensure that its event and symptom-based EOP components, or equivalent, are appropriately coordinated among the responsible personnel and that the symptom-based approach is invoked when it is required. Measures, including providing guidelines and training, should be defined to support staff decision- making for situations where an event has progressed to a stage for which procedures have not been defined. EOPs and SAMGs should cover events with multi-unit damage, potential damage to the fuel in spent fuel pools, releases of radioactive materials and hydrogen into buildings adjacent to the containment, and run-off of contaminated water to the environment. The time period that EOPs or SAMGs assume to initiate and complete required actions should reflect potential damage to the reactor. For example, a SAMG may specify a time period required to hook up		

Article No.	Clause Requirement	Assessment	Compliance Category
	alternative power and water sources. For external events, the extent of reactor damage and disturbances from outside or at the grid should be taken into account to prolong this time period. Having a diesel back on line may take a whole day or even longer, much more than the time that is assumed sufficient for an intact site area without large disturbances from outside. For beyond-design-basis initiating events, the reactor may require supplementary equipment stored onsite or offsite and external support to mitigate the accident consequences. These necessary measures should be specified in guidelines for coping with these events.		
4.3	Additional important elements that should be considered in the development of an IAMP include equipment and instrumentation, organizational responsibilities, and communication interfaces.	All these items are well covered by Bruce Power NERP [BP-PLAN-00001], and its implementing documents.	C
4.3.1 to 5.1		These are assessed in SFR 13.	NR
5.2	The overall process of verification and validation should be formally documented. The level of documentation required will depend upon the complexity of issues addressed and the potential impact on safety. The objectives of the verification and validation of accident management procedures and guidelines are to: • demonstrate that procedures and guidelines achieve the goals for which they were developed • confirm their usability (in terms of being easily understood and followed by their users) • verify technical accuracy (meaning identification of the correct equipment and line-ups) • assure completeness of scope (that is, to provide adequate guidance for all expected activities) • confirm that all specified actions are reasonable (i.e., consider possible challenges and threats to the personnel) and	Drills and exercises are part of the overall process for assessing the integrated performance of the organization and the capability of people, facilities, and equipment. BP-PROC-00010, Emergency Preparedness Drills and Exercises provides the drill and exercise objectives along with the planned frequency to test each of these objectives over a 5-year period. In addition, it describes the process used to plan, develop a scenario and supporting data, conduct, evaluate, and critique an exercise or a drill.	C

Article No.	Clause Requirement	Assessment	Compliance Category
	identify alternatives, where appropriate.		
5.3		This is assessed in SFR 13.	NR
5.4	Appropriate levels of training should be provided to the operating personnel and responsible organizations to ensure their competency in using all instructions and actions specified in EOPs, and their knowledge of the information required to identify events and accidents that are beyond the design basis and of the guidelines specified in SAMGs. Training should be commensurate with every personnel's respective roles in the case of an accident, enabling them to: • understand their roles and responsibilities within the IAMP • learn about accident phenomena and processes • become familiar with the activities to be carried out • enhance their ability to perform in stressful conditions • verify the effectiveness and improve the clarity of procedures and guidelines The licensee should establish qualification, training, deployment, and staffing numbers for the various organizational groups involved in accident management. Training programs should address the roles to be performed by the different groups, and include drills and exercises to enable assessment of the interactions between the various groups involved in IAMP. A set of drills should be developed to cover multi-unit events and external events. The purpose of conducting regular drills and integrated exercises is to confirm and maintain that each of the essential elements related to procedures, equipment and personnel of the IAMP has a high degree of assurance of effectiveness, should an accident occur. While there are potential limitations to the use of simulators for BDBA,	TQD-00005, ERO Training and Qualification document describes the program that is used to qualify and train personnel appointed to the ERO. This program was developed using the Systematic Approach to Training (SAT) per the requirement identified in BP-PROG-02.02, Worker Learning and Qualification Program. A General Employee Training (GET) program is provided and includes emergency response training. GET training is delivered to all employees requiring unescorted access to the nuclear facility so they are knowledgeable in the emergency response actions required of them. Various drills and exercises that require general staff involvement occur during the year to fortify and verify the correct response from staff at the site. Other venues that reinforce the required emergency action from general employees at site include safety awareness meetings and line supervision briefings. Emergency tones are broadcast and tested routinely at all locations.	C

Article No.	Clause Requirement	Assessment	Compliance Category
	the licensee should use simulator training, as appropriate, because it provides a realistic and interactive environment, and is an efficient method for enhancing human response in complex situations. Where simulator training is not used, other means to address the human response/ human and organizational performance aspects should be implemented. Licensees should also consult REGDOC-2.2.2, Personnel Training for information concerning requirements and guidance for training systems.		
6.	To satisfy the requirements specified in section 3 pertinent to validation of an IAMP, the licensee should consider the guidance given in this section. The first step of validating an IAMP is to review the program to assess its completeness and adequacy. The review also gives an opportunity to identify specific areas in the IAMP that need improvement to enhance reactor capabilities to cope with an accident. The adequacy of the SSCs and human/materiel resources that are required to complete IAMP actions should be assessed. To ensure the continued effectiveness of the IAMP, the licensee should have a procedural mechanism (see requirement 6 in section 3.2) by which its components are continuously reviewed to ensure that the technical basis remains sound and current, and that station staff can carry them out effectively. Where the review indicates that improvements are required, the IAMP should be revised promptly to incorporate those improvements.	Emergency Management Performance Measure Index, is used to measure and monitor the overall performance of the Bruce Power NERP [BP-PLAN-00001]. There are 5 key elements of the Plan and each is assigned an indicator and the criteria for measuring the performance of that indicator. The summation of those performance indicators provides the measure of the Plan's performance. SEC-EPP-00007, Emergency Management Program Assessment is the procedure that lists and describes the processes that are used to assess the Plans, which implement BP-PROG-08.01, Emergency Management Program. Bruce Power's NERP is audited by Bruce Power's internal audit organization for a quality assurance over a period of 3 years. Audit findings will be subject to root cause evaluations as appropriate, corrective actions will be identified, and, a schedule for corrective action will be developed. Important corrective actions will be tracked in the Corrective Action system. As part of the self-assessment, the Drill and Exercise program will provide an overall integrated assessment. Drill and exercise reports will provide a list of findings. The Emergency Management Department will initiate a causal factor evaluation as appropriate and identify the corrective actions. Completion of corrective actions will be tracked using the management Action Tracking System. Bruce Power management can initiate an external, independent assessment of the Emergency Management Program at any time. Such an assessment will be initiated when	C

Article No.	Clause Requirement	Assessment	Compliance Category
		performance indicates a need for it. Such action is also warranted if it is determined that it will be a necessary enhancement to the self-assessment process and the audit programs.	
6.1 to 7.		These are assessed in SFR 13.	NR

B.4. CSA N290.1-13, Requirements for the Shutdown Systems of CANDU Nuclear Power Plants

In support of the review tasks listed in Section 5, relevant clauses of CSA N290.1-13 have been assessed in Table B4. A more detailed assessment is performed in "Safety Factor 1: Plant Design".

Table B4: CSA N290.1-13, Requirements for the Shutdown Systems of CANDU Nuclear Power Plants

Article No.	Clause Requirement	Assessment	Compliance Category
4.1.2.1	The SDS shall terminate the chain fission reaction when a failure of a reactor process system occurs that could fail fuel sheaths or other barriers, to prevent a significant release of radioactivity. Notes: 1) Termination of the chain fission reaction is generally accomplished by inserting rods or liquids that absorb neutrons. 2) In CANDU reactors, SDS is credited for overpressure protection.	Bruce A reactor incorporates these common CANDU design features. More detailed assessment is performed in SFR1.	C
4.1.2.2.2	During normal operation, in AOOs and in DBAs, at least one means shall be independently capable of quickly rendering the reactor subcritical by an adequate margin on the assumption of a single failure.	Although AOOs are not explicitly assessed, they are covered within the single failure events where shutdown system effectiveness in rendering the reactor subcritical is demonstrated in Part 3 of the Safety Report.	IC
4.2.1.1	The reliability evaluation shall demonstrate that the reliability of the shutdown function from all credited means is such that the cumulative probability of failure to shutdown on demand can be shown to meet its requirement. The contribution of all sequences, involving failure to shutdown, to the large release frequency shall be less than the target stated in regulatory requirements.	This clause is assessed in SFR 1.	NR

Article No.	Clause Requirement	Assessment	Compliance Category
	Notes: 1) General requirements on reliability and reliability analysis for safety systems can be found in CSA N290.0, Clause 4.5. 2) The probability of an SDS failure on demand for existing CANDU plants is typically lower than 10-3. 3) CNSC RD/GD-98 requires a licensee who constructs or operates an NPP to develop and implement a reliability program that assures that the systems important to safety can and will meet their defined design and performance specifications at acceptable levels of reliability throughout the lifetime of the NPP.		
4.2.1.2	Existing CANDU plants may meet reliability requirements by demonstrating SDS availability. If this approach is taken, each SDS shall have a demonstrated unavailability that meets its requirement. An SDS shall be considered to be available only when it meets all its minimum allowable performance standards. All the components in the trip chain shall be included in the SDS unavailability calculations. Notes: 1) The SDS demonstrated unavailability requirement for existing CANDU plants has been 10-3 years per year due to all causes. (This is equivalent to a maximum of one failure out of 1000 demands for SDS action.) 2) The unavailability is demonstrated by actual direct SDS experience or reasonable extrapolation from it, in conjunction with the test frequency. The causes to be included in the analysis are random component failures, operator disabling of the SDS, common-cause failures, and safety support system failure.	Refer to REGDOC-2.5.2 corresponding requirement.	RNA

Article No.	Clause Requirement	Assessment	Compliance Category
4.3.1.1	SDS trip parameters shall be selected to sense the plant conditions of concern that result from the PIEs considered in the plant design. Notes: 1) Examples of SDS trip parameters for a CANDU NPP are neutron overpower, high rate of change of neutron flux, high (or low) primary heat transport system (PHTS) pressure, PHTS low flow, and steam generator low level. 2) Annex B provides a list of postulated failures for CANDU reactors.	Sections 6.4.4 and 6.5.4 of the Safety Report Part 2 [NK21-SR-01320-00002 Ver005] summarize the various trip parameters applicable to the various events. Trip coverage assessments for the various events are included in Part 3 of the Safety Report.	C
4.3.1.2	There shall be two diverse SDS trip parameters to protect against a PIE, unless it is impracticable or it can be shown that failure to trip when a single trip parameter is provided will not lead to unacceptable consequences.	Except few cases where limited windows of single parameter coverage exist, at least two diverse trips are demonstrated to be effective for each analysed event. The limited windows of single trip coverage are justified by the impracticality of closing them.	AD
4.3.1.4	In order to credit (in the safety analysis) operator action to shutdown (manually trip) the reactor, the design shall provide a) clear, well-defined, validated, and readily available operating procedures that identify the necessary actions; b) instrumentation in the control rooms to provide clear and unambiguous indication of the necessity for operator action; c) adequate time before operator action is required, following indication of the necessity for operator action inside the control rooms; and d) adequate time before operator action is required, following indication of the necessity for operator action outside the control rooms.	Operator actions considered in Bruce A safety analysis are consistent with the requirements for existing CANDU plants.	C

Article No.	Clause Requirement	Assessment	Compliance Category
	Notes: 1) For new plants, adequate time is at least 30 min for operator action inside the control room and 60 min for operator action outside the control room. 2) For existing CANDU plants, adequate time is 15 min for operator action inside the control room and 30 min for operator action outside the control room.		
4.3.3.4	Trip set points shall be selected to provide sufficient allowance between the set points and corresponding safety analysis limits to account for uncertainties. The uncertainties include but are not limited to a) instrument calibration uncertainties; b) instrument uncertainties during normal operation; c) instrument drift; d) instrument uncertainties caused by design basis events; e) process-dependent effects; f) calculation effects; g) dynamic effects; and h) calibration and installation bias accounting. Notes: 1) Based on ANSI/ISA-67.04.01. 2) Set point margins should accommodate normal operational transients to minimize spurious trips without compromising the safety margin.	Bruce A has completed the baseline SOE projects which consisted of documenting the limits and conditions derived from the safety analysis in OSRs, and completing the corresponding IUCs that are considered in setting the OLCs.	C