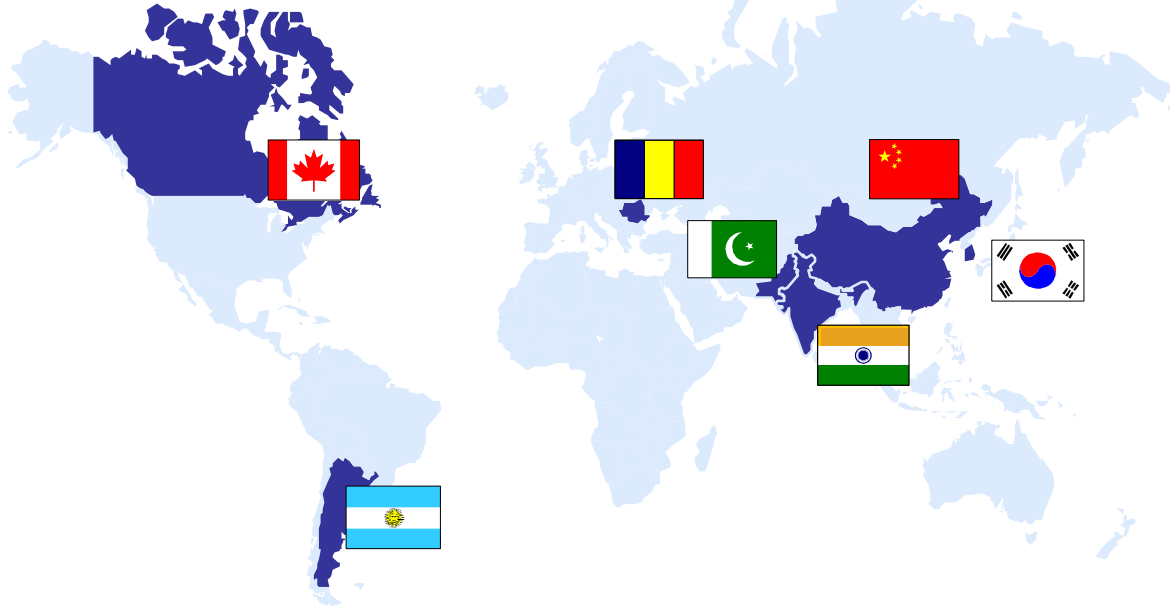


## **COG-JP-4499-025-R1**

K-410122-REPT-0010 R02

# **Whole-Site Risk Considerations for Nuclear Power Plants**



**Project Manager: Krish Krishnan**

**Date: September 2017**

# Whole-Site Risk Considerations for Nuclear Power Plants

Prepared by:

Glenn Archinoff

Candesco Division of Kinectrics Inc.

**Source of Funding:** The work reported in this document was funded by the COG Joint Project Agreement titled, *CANDU Whole-Site Probabilistic Safety Assessment* under the joint participation of *Bruce Power, Canadian Nuclear Laboratories, Korea Hydro and Nuclear Power, New Brunswick Power, Ontario Power Generation and Societatea Nationala NUCLEARELECTRICA*.

**Disclaimer of Liability:** This document was prepared by the organization(s) named above for work sponsored or co-sponsored by the CANDU Owners Group. Neither the organization(s) named above; nor co-sponsor(s); nor COG; nor COG's members; nor any of their employees, officers, or directors; makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe on privately owned rights.


**Quality Program:** The work reported herein performed under the Kinectrics Quality Manual which is consistent with CSA Z299.1-85 *Quality Assurance Program – Category 1* and the relevant sections of CSA N286-05 *Management System Requirements for Nuclear Power Plants*.

## Whole-Site Risk Considerations for Nuclear Power Plants

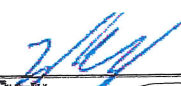
Report No. COG-JP-4499-025-R1

September 2017

Prepared by:

  
Glenn Archiboff  
Candesco Division of Kinetics Inc.


Reviewed by:

  
Peter Purdy  
Bruce Power


Reviewed by:

  
David Garrick  
Canadian Nuclear Laboratories

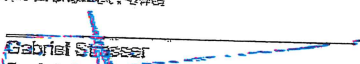
Reviewed by:

  
Hojun Jeon  
Korea Hydro and Nuclear Power


Reviewed by:

  
Derek Mullin  
New Brunswick Power


Reviewed by:

  
Gabriel Stasser  
Société Régionale NUCLEARELECTRICA

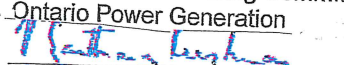
Reviewed by:

  
Jack Vecchiarelli  
Ontario Power Generation

Accepted by:

  
Jack Vecchiarelli  
Chair, JP4499 Steering Committee  
Ontario Power Generation

Publication Approved by  
COG Inc:

  
Krish Krishnan  
Project Manager  
CANDU Owners Group Inc.

## Table of Contents

|   |    |
|---|----|
| Executive Summary .....   | v  |
| 1 Introduction .....  | 1  |
| 2 Meaning of Safety and Risk.....                               | 1  |
| 3 Whole-Site Risk.....  | 3  |
| 4 Risk of Severe Accidents .....                                | 5  |
| 4.1 Qualitative Assessment.....                                 | 5  |
| 4.2 Quantitative Assessment Using PSA.....                      | 6  |
| 4.3 Whole-Site PSA Considerations.....                          | 9  |
| 5 Conclusions .....   | 11 |
| References.....   | 11 |
| Appendix A Additional PSA Results Presentation Approaches ..... | 17 |
| Appendix B Acronyms and Abbreviations .....                     | 21 |

## List of Tables

|                                    |    |
|------------------------------------|----|
| Table 1 - Typical PSA Results..... | 13 |
|------------------------------------|----|

## List of Figures

|   |    |
|---|----|
| Figure 1 - CNSC Safety and Control Areas .....                              | 14 |
| Figure 2 - CNSC Staff Assessment of Canadian NPP Performance 2016 [8] ..... | 15 |
| Figure 3 - Example PSA Results for Large Release Frequency .....            | 16 |
| Figure A-1 - Alternative Presentation of Aggregated PSA Results.....        | 19 |
| Figure A-2 - Whole-Site PSA Results Summary .....                           | 20 |

## **Acknowledgement**

The author acknowledges with thanks the feedback on a draft version of this report provided by Paul Lawrence of Kinectrics Inc. and Ben Hryciw of Amec Foster Wheeler.

## Executive Summary

The nuclear power industry has, from its inception, made safety the highest priority in the design, construction, operation, and decommissioning of nuclear power plants. A long-standing fundamental safety principle is that a nuclear power plant should pose only a very small incremental risk to the health and safety of the surrounding population. This principle is inherent in the way nuclear power plants are operated and is a fundamental element of the Canadian nuclear regulatory framework. Utilities have a comprehensive suite of programs which ensure that nuclear power plants are operated well within regulatory limits. Utilities would not operate a nuclear power plant, nor would the Canadian Nuclear Safety Commission allow it, if the risk to the surrounding population was unreasonable. The reasonableness of the risk is a value judgment based on extensive qualitative and quantitative information, including confirmation that regulatory limits and goals are met.

In recent years, the term "whole-site risk" has become the subject of discussion at licensing hearings in Canada and in the international nuclear community, particularly as it relates to multi-unit nuclear power plants. The discussion has centred around whether the safety assessments of multi-unit stations account for the "whole-site risk", meaning the overall risk associated with all sources of radioactivity on the site and all potential hazards. This report describes how the whole-site risk associated with a nuclear power plant is characterized and how it is managed by utilities to ensure that the level of safety remains acceptable.

The report describes the 14 Safety and Control Areas that are assessed by the Canadian Nuclear Safety Commission to determine whether regulatory requirements are met and whether the overall risk associated with a nuclear power plant, that is, the whole-site risk, is judged to be acceptable. The Safety and Control Areas span all sources of radioactivity on a site and all aspects of normal operation as well as postulated accidents.

The Safety and Control Areas consider the results of environmental monitoring programs, which are contained in public reports issued annually by Canadian nuclear utilities. All plants report that releases to the environment are well below regulatory limits and therefore pose insignificant risk to the public. As part of the industry's commitment to openness, the results of annual environmental monitoring are available to the public. The Safety and Control Area assessments also confirm that regulatory dose limits will be met for postulated accidents that are within the plant Design Basis. Meeting these limits ensures very low incremental risk to the surrounding population should such an accident occur.

The Safety and Control Areas also include consideration of very low probability accidents, referred to as Beyond Design Basis Accidents, and how Probabilistic Safety Assessment is used to determine whether established risk goals for such events are met. The report describes how Probabilistic Safety Assessment explicitly accounts for the presence of multiple reactors in a station, and illustrates how the results can be presented to understand the risk associated with different types of hazards.

In summary, the report demonstrates that whole-site risk, while not described in terms of a single number, is an important consideration by utilities and the regulator when assessing the overall safety of a nuclear power plant. The report describes the means by which whole-site risk is evaluated, with particular attention paid to how the results of

Probabilistic Safety Assessment contribute to understanding the risks of different types of hazards and the aggregate risk associated with multiple reactors at a site.

## 1 Introduction

The nuclear power industry has, from its inception, made safety the highest priority in the design, construction, operation, and decommissioning of nuclear power plants. A long-standing principle that has guided utilities and the regulator is that a nuclear power plant should pose only a very small incremental risk to the health and safety of the surrounding population. Utilities would not operate a nuclear power plant (NPP), nor would the Canadian Nuclear Safety Commission (CNSC) allow it, if the risk to the surrounding population was unreasonable.

In recent years, the term "whole-site risk" has become the subject of discussion at licensing hearings in Canada and in the international nuclear community, particularly as it relates to multi-unit nuclear power plants. The discussion has centred around whether the safety assessments of multi-unit stations account for the "whole-site risk", meaning the overall risk associated with all sources of radioactivity on the site and all potential hazards. This report describes an approach to characterizing whole-site risk for operating NPPs, including multi-unit stations. In particular, the potential for large off-site releases of radioactivity is addressed as it is a key part of the discussion of whole-site risk. This report was prepared for CANDU Owners Group (COG) Joint Project 4499. The approach described in this report leverages results from the COG Joint Project, and builds on the framework described in a COG report on this topic [1].

The following section discusses the key terms "safety" and "risk". Section 3 describes how whole-site risk is assessed in the context of the Canadian nuclear regulatory framework. Section 4 discusses how Probabilistic Safety Assessments (PSA) of severe accidents are performed for Canadian NPPs and how the results can be documented to provide insights into the risk of large off-site releases from NPPs. Conclusions are stated in Section 5.

## 2 Meaning of Safety and Risk

It is important to be clear on the meaning of terms such as "safety" and "risk", or more specifically "adequate safety" and "reasonable risk", when discussing the topic of whole-site risk and how it relates to the licensing of NPPs in Canada. These terms are discussed in this section.

An objective of assessing whole-site risk is to holistically demonstrate that a nuclear site with a single-unit, or an interconnected multi-unit NPP, or a group of single units within the exclusion zone<sup>1</sup>, is adequately safe and does not pose an unreasonable risk to the surrounding population or the environment. However, the word "safety" does not have a simple definition [3], [4]; it is not something that can be simply measured to determine its adequacy. The CNSC's website describes how the CNSC defines safety [5], and refers to a federal court decision which states:

*"...safety is not measured. It is judged and it is judged according to an assessment of an acceptable risk: ... An acceptable risk is essentially a value-based proposition determined by policy and/or by those authorized by governments to judge safety and/or by those exposed to the risk."*

---

<sup>1</sup> CNSC REGDOC-3.6 [2] defines site as: "With respect to nuclear facilities, the area within an exclusion zone where one or more nuclear facilities and all associated support structures and systems are located."



The statement that safety is not measured but rather is judged is consistent with the Nuclear Safety and Control Act (NSCA), which includes the following relevant statements (emphasis added):

- NSCA Section 3: The purpose of the Act is to provide for “**the limitation, to a reasonable level** and in a manner that is consistent with Canada’s international obligations, **of the risks** to national security, the health and safety of persons and the environment...”
- NSCA Section 9: Objects of the Commission: "to regulate...in order to... **prevent unreasonable risk**, to the environment and to the health and safety of persons..."
- NSCA Section 24(4): “No licence shall be issued, renewed...unless, **in the opinion** of the Commission, the applicant...is **qualified to carry on the activity**...and...will...**make adequate provision for the protection of the environment, the health and safety of persons**...”

The CNSC has recently published a glossary of terminology [2]. The terms "safety" and "whole-site risk" are not defined in the glossary, but "risk" is defined as:

*The chance of injury or loss, defined as a measure of the probability and severity of an adverse effect (consequence) to health, property, the environment or other things of value; mathematically, risk is the probability of occurrence (likelihood) of an event multiplied by its magnitude (severity).*

When judging the acceptability of risk, guidance can be taken from the fundamental safety goal stated in CNSC REGDOC-2.5.2 [6], the regulatory document on the design of nuclear power plants. The goal is that an NPP should not impose a “significant additional risk to the life and health of individuals”. Although this REGDOC applies to new NPPs, the principle is universal and applies to operating plants as well.

A recent document issued by the US Nuclear Regulatory Commission (NRC) [7] aligns with the Canadian approach to risk and safety. The NRC document states:

*In the context of NRC regulation, safety means avoiding undue risk or, stated another way, providing reasonable assurance of adequate protection for the public in connection with the use of source, byproduct and special nuclear materials.*

*Quantitative (absolute) risk estimates serve as an important measure of plant safety, but do not embody the full range of considerations that enter into the judgment regarding adequate protection. The judgment regarding adequate protection derives from a more diverse set of considerations, such as acceptable design, construction, operation, maintenance, modification, and quality assurance measures, together with compliance with NRC requirements including, license conditions, orders, and regulations.*

It is clear from the above discussion that in the Canadian (and US) nuclear regulatory context, "adequate safety" and "reasonable risk" are value-based judgments made by the authorized body. In Canada, utilities are responsible for operating nuclear power plants in a manner that ensures adequate safety and reasonable risk, and the Commission Tribunal makes a determination of whether these objectives have been achieved. In making this determination, the Commission Tribunal takes into account input from the utility, CNSC staff, as well as other interested parties including those who may be exposed to the risk, through the licence hearing

intervention process. These judgments are based on a broad set of qualitative and quantitative information, as discussed in the next section. There is no requirement to reduce the input to the Commission's licensing decision to a single number. In fact, it can be argued that by requiring the Commission to "form an opinion", and in accordance with the principle that safety is judged and not measured, the NSCA prohibits licensing decisions from being based solely or primarily on a formulaic or simple numerical approach.

The implication is that whole-site risk should be defined and evaluated in a way that supports the value-based approach to safety determination and licensing decisions and takes into account both qualitative and quantitative information. That is, rather than attempting to characterize whole-site risk by a single number or even a series of numbers, the approach should be to provide quantitative and qualitative information to support a judgment on whether the whole-site risk is limited to a reasonable level. This is further discussed in the context of an NPP site in the next section.

### 3 Whole-Site Risk

Canadian nuclear utilities and the CNSC take an integrated approach to the evaluation of safety, consistent with a value-based approach as discussed in the previous section. The utilities as the licensees are responsible for safety. The CNSC oversees licensed activities and confirms that the requirements of the NSCA, and other applicable requirements, are met.

CNSC staff's oversight and evaluation of licensee performance is documented in annual regulatory oversight reports on NPP safety performance. These reports are available on the CNSC's public website, and they evaluate NPP safety across 14 Safety and Control Areas (SCAs), comprising 73 sub-topics as illustrated in Figure 1. The figure shows that the evaluations of the SCAs performed by CNSC staff are inputs to the Commission's licensing decisions. The evaluations assess both qualitative and quantitative information.

The CNSC staff evaluates NPP performance regularly and reports on it annually for each of the 14 SCAs. The most recent report available is for 2016 [8]. The results are shown in Figure 2 and indicate that all Canadian NPPs performed at a Satisfactory or Fully Satisfactory level for each SCA. The ratings in the CNSC's oversight report reflect a utility's effectiveness in managing the safety of and risk associated with its NPPs. Each utility has formal programs in place to ensure effective performance in each SCA. Achieving effective performance ensures that adequate safety is achieved and that the overall risk associated with the plant is limited to a reasonable level, as required by the NSCA.

The Satisfactory or Fully Satisfactory Integrated Plant Rating at the bottom of the figure is an indication that the overall risk associated with each NPP site is limited to a reasonable level, consistent with the requirements of the NSCA. That is, the Integrated Plant Rating is interpreted to mean that the whole-site risk is considered by CNSC staff to be acceptable. It is noteworthy that the whole-site risk is judged to be acceptable without requiring the total risk to be numerically quantified. This approach reflects a value judgment that depends on the specific circumstances, and is consistent with that described in Section 2.

In terms of the risk of off-site releases of radioactivity, there are several important indicators included in the SCAs and assessments of each station's performance that support the overall conclusion that the risk is acceptably low, as follows:

**Actual off-site releases** – Actual releases of radioactivity from each NPP site are monitored through a comprehensive environmental monitoring program. The results

reflect actual safety performance in terms of off-site releases of radioactivity and so provide a quantitative input to the evaluation of whole-site risk. Bruce Power, Ontario Power Generation (OPG) and New Brunswick Power (NB Power) operate NPPs in Canada<sup>2</sup>, and each utility reports annually on the results of its environmental monitoring program. As an example, Bruce Power's report for 2015 [9] documents actual releases of radioactivity from the Bruce site for the year and calculates the associated dose to the public. The report states that the maximum dose to an off-site individual was 2.89  $\mu\text{Sv}$ , which is 0.29% of the legal limit of 1,000  $\mu\text{Sv}$ . Moreover, the report states that 2015 was the 24<sup>th</sup> consecutive year that the calculated dose was less than 10  $\mu\text{Sv}$ , which is the value regarded as the lower threshold for health significance. Similar results are reported for OPG [10] and NB Power [11], with OPG reporting that public dose in 2015 from both the Pickering and Darlington stations was about 0.1% of the limit, and NB Power reporting that public dose from the Point Lepreau Generating Station was less than 0.1% of the limit. In summary, actual releases of radioactivity from Canadian NPP sites are extremely low and have not had any adverse health effect on the public.

**Potential future off-site releases** – The potential for future off-site releases is evaluated for normal operation and for abnormal events and accidents.

- Normal operation – The potential for future releases during normal operation is assessed based on past experience, the physical condition of the plant and expected aging effects, adherence to deterministic limits established for normal operation, and programs in place for managing radiological waste and for monitoring and mitigating releases to the environment. These factors are all considered in the SCAs identified in Figure 1 and shown in Figure 2 to be Satisfactory or Fully Satisfactory.
- Anticipated operational occurrences (AOOs) and design basis accidents (DBAs) – The potential for releases to occur as a consequence of AOOs and DBAs<sup>3</sup> is assessed based on the maintenance program that keeps plant equipment fit for service so as to prevent accidents due to equipment failure, operational testing to confirm that mitigating systems are reliable, operation within specified limits, and deterministic safety analysis (DSA). The DSA shows that any resultant off-site doses will be within specified limits and therefore will pose negligible incremental health risk to the off-site public. These factors are all considered in the SCAs identified in Figure 1 and shown in Figure 2 to be Satisfactory or Fully Satisfactory.
- Beyond design basis accidents (BDBAs) – These are accident scenarios that are lower probability than design basis accidents and which potentially have greater consequences. The plant design may not have been intended to cope with them but mitigating provisions in place will help to limit the consequences. PSA is performed to assess plant robustness and to quantify the likelihood of events that can lead to severe core damage and large off-site releases. PSA results are used to identify potential safety enhancements and to inform procedures and guidance aimed at mitigating BDBAs. Such procedures and guidance are in place to use available plant equipment and new equipment, such as Emergency Mitigating Equipment (EME) that was installed or is in the process of being

---

<sup>2</sup> The Gentilly-2 plant is permanently shutdown.

<sup>3</sup> Accidents, even those with low frequency, the plant is designed to cope with such that off-site doses are within regulatory limits.

installed based on lessons learned from the Fukushima accident in 2011, to prevent an accident from escalating to a severe accident (refer to Section 4.1 for more details). Utility staff is trained on these procedures and guides, and exercises are performed to ensure the response will be effective. All aspects of BDBA evaluation are considered in the SCAs identified in Figure 1 and shown in Figure 2 to be Satisfactory or Fully Satisfactory.

In summary, the potential for future off-site releases is evaluated holistically, covering normal operation, abnormal occurrences, design basis accidents, and beyond design basis accidents. The experience to date, programs in place, and the supporting safety analysis, demonstrate that the potential is low, and this conclusion contributes to the Integrated Plant Rating.

The discussion in this section demonstrates that the overall safety of an NPP is assessed through an evaluation of actual experience, the fitness for service of equipment, the effectiveness of programs, and the safety analysis, including both DSA and PSA. The outcome of this assessment that the Integrated Plant Rating is Satisfactory or Fully Satisfactory means that the whole-site risk is limited to a reasonable level, confirming that the fundamental safety objective is met.

An additional observation is that only very low probability scenarios, i.e., those in the BDBA category, have the potential for significant off-site releases. Actual experience demonstrates that off-site releases during normal operation are inconsequential. It also shows that there have not been abnormal occurrences or accidents with significant off-site consequences. The SCA ratings show that the predicted consequences of such events will be within prescribed limits, meaning there will not be a significant risk to the health of individuals in areas around the site. The conclusion is that the plant design, operation and maintenance ensures that the likelihood of significant off-site consequences is of very low probability and is therefore associated with highly unlikely events in the BDBA category. The next section focuses on BDBAs and how the risk associated with severe accidents is evaluated.

## 4 Risk of Severe Accidents

### 4.1 Qualitative Assessment

A defence-in-depth approach to design, operation, safety analysis, and accident management ensures that accidents that could lead to a large off-site release of radioactivity are very unlikely to occur. The defence-in-depth concept provides multiple, overlapping barriers to achieve the desired result of very low probability of an accident with significant off-site consequences.

The levels of defence can be described as follows (quoted text is from Reference [6]):

Level 1 - "The aim of the first level of defence is to prevent deviations from normal operation, and to prevent failures of structures, systems and components (SSCs) important to safety." This is achieved through the use of high quality materials and equipment, good maintenance and inspection, and operating within predetermined limits.

Level 2 - "The aim of the second level of defence is to detect and intercept any deviations from normal operation in order to prevent AOOs from escalating to accident conditions and to return the plant to a state of normal operation." This is achieved through effective control systems that are routinely exercised, and through procedures that operating staff is trained on including refresher training.

Level 3 - "The aim of the third level of defence is to minimize the consequences of accidents by providing inherent safety features, fail-safe design, additional equipment and mitigating procedures." This is achieved through the provision of systems specifically designed to mitigate accidents. These systems are routinely tested, and staff is trained on their operation.

Level 4 - "The aim of the fourth level of defence is to ensure that radioactive releases caused by severe accidents are kept as low as practicable." This is achieved by an effective containment system, together with the new EME whose purpose is to prevent an accident from progressing to a severe accident or to mitigate a severe accident should severe core damage occur.

Level 5 - "The aim of the fifth level of defence is to mitigate the radiological consequences of potential release of radioactive materials that may result from accident conditions". This is achieved through effective emergency management provisions which are regularly tested.

As noted in Section 3, Canadian nuclear utilities have made or are in the process of completing safety improvements which, in part are a result of lessons learned from the Fukushima accident. These improvements are aimed primarily at defence-in-depth Levels 3, 4 and 5, and further reduce the already low risk of events that may lead to a large off-site release of radioactivity. The specific improvements vary among the stations but generally include the following areas:

- Provision of additional make-up water for fuel cooling;
- Pressure relief for heat sinks such as the shield tank and for the calandria vault;
- Additional hydrogen mitigation;
- Portable electrical power supplies for key equipment and instrumentation and control;
- Updated Severe Accident Management Guidance which incorporates multi-unit effects and effective use of Emergency Mitigating Equipment, including for irradiated fuel bays; and
- Incorporation of severe accident and multi-unit scenarios in emergency planning and exercises.

The information presented in Section 3 indicates that all of the elements of defence-in-depth, including the Fukushima-related improvements, have been evaluated and constitute a high degree of safety for all Canadian NPPs. This provides a high level of confidence that the likelihood of a severe accident is very low, and that the NPPs are robust in guarding against a wide range of different hazards, including internal events, fires, floods, seismic, high wind, malevolent acts, cyber security threats and other hazards.

## **4.2 Quantitative Assessment Using PSA**

As described in Section 3, Deterministic Safety Analysis is used to confirm that postulated accidents within the plant design basis meet regulatory dose limits. Deterministic analysis may also be used for some BDBA events to confirm that the consequences meet even the conservative dose limits for design basis events. For such events, quantification of the risk is not required.

For postulated BDBAs that can result in a severe accident, quantitative assessment is performed using PSA techniques. Quantitative goals for operating reactors have been established to assess the PSA results. These goals are:

- The Severe Core Damage Frequency (SCDF) should be less than 1 in 10,000 per reactor per year. Severe core damage is defined as extensive physical damage of multiple fuel channels due to overheating leading to loss of core structural integrity. This is consistent with the definition of core damage in Reference [2].
- The Large Release Frequency (LRF) should be less than 1 in 100,000 per reactor per year. A large release is defined as exceeding  $10^{14}$  Becquerels of Cs-137 released to the environment.

These goals are surrogates for higher level qualitative goals, such as the goal described in Section 2, that a nuclear power plant should pose only a small incremental risk to the life and health of the surrounding population. Meeting the quantitative PSA goals helps to assure that the higher level goals are met. Consistent with a value-judgment-based approach to risk, the goals are not treated as hard limits, and if the PSA goals are not met or even if the margin to the goals is small, an evaluation is performed to determine whether additional measures should be taken to confirm that the risk of a severe accident and a large off-site release is limited to a reasonable level.

Consistent with international best practice, the PSAs for Canadian NPPs start with identification of initiating events that could potentially lead to fuel failures and severe core damage. This includes internal equipment failures and other hazards such as fire, as well as external hazards such as seismic events, tornados, etc. Screening is performed to identify those hazards that require more detailed evaluation. The hazard categories typically selected for quantitative PSA evaluation are:

- Internal<sup>4</sup> failures while the reactor is operating at power;
- Internal failures while the reactor is shutdown;
- Internal fires;
- Internal floods;
- Seismic events; and
- High winds.

An important aspect of the PSA is that it explicitly accounts for the potential for an initiating event, and for additional failures caused by the initiating event or that occur randomly, to affect more than one reactor unit in a multi-unit station. Therefore, the PSAs performed for multi-unit NPPs in Canada are, in effect, what are referred to as MUPSAs (Multi-Unit PSAs). This is a critical element of the PSAs because it explicitly takes into account interactions among units and phenomena that affect all units when calculating the PSA results. Although PSA results are expressed on a per reactor basis, the results take into account multi-unit effects and interactions that contribute to the SCDF and LRF.

For example, if an initiating event were severe enough, it could potentially cause severe core damage in all 4 units at a 4-unit station. The release of radioactivity from all 4 units is therefore considered when determining whether the Large Release threshold is exceeded. In order to not exceed the threshold, the release per unit can only be one quarter of the threshold value (assuming all units behave the same). This imposes greater safety constraints compared to

---

<sup>4</sup> An internal event is any event that proceeds from a human error or from failure of a structure, system or component. This includes equipment failures and other hazards such as a fire in the station. External events are an event of natural or human-induced origin that originates outside the site and whose effects on the reactor facility are considered as potentially hazardous. These definitions are consistent with Reference [12].

only considering the units individually. In this example, if only individual units were considered the release from a single unit could be a factor of four greater and still not exceed the Large Release threshold. This example illustrates how the current PSAs for multi-unit NPPs in Canada are MUPSAs and also how the per reactor PSA goals are applied in a multi-unit context.

These concepts are discussed in a recently issued Commission Member Document (CMD) that was presented to the Commission Tribunal in August 2017 [13]. The CMD includes a report prepared by CNSC staff titled "Regulatory Role of Probabilistic Safety Assessment" and a third-party report titled "Probabilistic Safety Assessment - Safety and Regulatory Framework". Both reports in the CMD are consistent with the concepts described thus far in this report. The following discussion elaborates on how the results of PSA can be documented and evaluated to gain further insights into NPP safety.

Table 1 shows how PSA results can be presented to facilitate understanding the relative risks associated with different hazard categories and the margins to the PSA goals. The results in the table do not correspond to those for a specific NPP but are typical of PSA results for a multi-unit Canadian NPP. The table shows the SCDF and LRF for each hazard category as well as the summed results for all internal events and comparison to the PSA goals.

Table 1 has the following attributes:

- The top half of the table shows the SCDF and LRF for hazard categories associated with internal plant failures.
- The results for At Power events are aggregated results covering a wide range of equipment failures, such as pipe breaks, control system failures, electrical system failures, etc. The results include initiating events that affect only a single reactor, as well as events that affect multiple units in a multi-unit station, such as loss of external electrical power.
- Events while the reactor is shutdown are assessed explicitly, to obtain insights for the plant when a reactor is in an outage state. For a multi-unit station, there can be combinations of reactors operating and shutdown, so expressing the results on a per reactor per year basis facilitates understanding of individual reactor behaviour in the two states.
- Results are shown separately for internal flood and internal fire. These events can affect multiple reactors simultaneously. In addition, since an internal fire may be initiated by an event that is not an equipment failure, the uncertainty in the initiating event severity as a function of frequency is different compared to that for equipment failures. Therefore, it is appropriate to present the results separately.
- The SCDF and LRF are summed for all internal hazards assessed with PSA and compared to the PSA goals on a per-reactor basis. The result is an indication of the incremental risk to the public associated with a large release of radioactivity due to internal plant failures. This result can be used with actual release results for normal operation and safety analysis of DBAs to assess the overall risk of the NPP. In the example in Table 1, there are significant margins to the PSA goals, which is typical for Canadian NPPs.

The bottom half of the table (labeled External Events) presents results separately for the two external event categories assessed with PSA: seismic events and high wind events. The first and third of the four rows in this part of the table show PSA results for initiating event

frequencies as low as 1 in 1,000 years, corresponding to events that may occur over the life of the plant and those that are unlikely to occur. The table shows that in this example the contribution to SCDF and LRF is very low. Expressing the results in this manner provides insights into the robustness of the plant for external events that are plausible and is a means to confirm that the plant poses no significant incremental risk for plausible external events.

The second and fourth rows in this part of the table present results for more unlikely external events, including those with frequencies as low as 1 in 10,000 years. Table 1 shows that these example PSA results for external events are well below those for internal events and that there are large margins to the PSA goals. For such very low initiating event frequencies for external events, it can be expected that the event itself would directly impact the safety of the surrounding population irrespective of the NPP. In such circumstances, the table is a means to convey that the LRF risk is small despite the elevated risk to the public directly associated with the initiating event, and hence the qualitative safety goal described in Section 2 is met.

It is reiterated that these results account for multi-unit effects such as scenarios where all 4 units in a station are affected and contribute to the release of radioactivity to the environment.

### 4.3 Whole-Site PSA Considerations

Further insights into the robustness of multi-unit NPPs with respect to severe accidents and large off-site releases of radioactivity can be obtained by comparing the PSA results expressed on a per reactor basis to results expressed on a station basis. The discussion in this section focuses primarily on LRF as it is a more direct indicator of risk to the public than SCDF. It is the primary indicator used by utilities to assess and manage the risk associated with severe accidents.

Through the Joint Project described in Section 1, COG members have developed the following approach to aggregating PSA results to express the LRF on a per station basis for a given hazard. For a station comprising 4 reactor units, for example, the station LRF for a given hazard category is obtained as follows:

$$\begin{aligned} \text{LRF per station} = & 4 \times \text{LRF per reactor for initiating events that affect a single unit only} \\ & + 2 \times \text{LRF per reactor for initiating events that affect two units} \\ & \text{simultaneously (this term accounts for all possible combinations of two-} \\ & \text{unit events)} \\ & + 1 \times \text{LRF per reactor for initiating events that affect all units} \\ & \text{simultaneously (three-unit sequences are very few and are lumped in with} \\ & \text{four-unit cases)} \end{aligned}$$

The underlying basis for this formula is that initiating event frequencies are established on a per reactor basis independently of how many reactors are in a station. Therefore, if a random event affects only a single reactor unit, the probability that the event will occur in a multi-unit station is the probability per reactor multiplied by the number of reactors. For example, if the predicted frequency of occurrence of a small pipe break in the reactor coolant system is 1 in 100 years per reactor, then the predicted frequency of a small pipe break in a 4 unit station is 4 in 100 years. Therefore, for event sequences that affect only a single reactor and which result in the LRF threshold being exceeded, the LRF for the station is 4 times the LRF calculated for the event sequence (the first term in the above equation). The other two terms account for events that can affect combinations of two, three or all four reactors at a time.

Figure 3 demonstrates a method for graphically showing PSA results aggregated on a per reactor basis and separately on a per station basis. The results are typical for a multi-unit



Canadian NPP but do not correspond to a specific station. The "Unit Aggregation" results show the LRF aggregated for all event sequences for the given hazard category, expressed on a per reactor unit per year basis taking into account multi-unit effects that can affect the per reactor LRF. These results are the same as shown in Table 1 and for external events reflect initiating event frequencies as low as 1 in 10,000 years. The "Station Aggregation" results for each hazard category are based on the formula described above.

Figure 3 is a means to show whether a particular initiating event category dominates the calculated LRF. In this example, it is internal fire. The figure also characterizes modeling conservatism and uncertainty in the PSAs for the different hazard categories. This information is provided at the bottom of the figure, below the horizontal axis. In this context, modeling conservatism refers to assumptions in the accident progression modeling, especially for sequences that lead to severe core damage in multiple units. Uncertainty refers primarily to uncertainties associated with characterizing the initiating event severity as a function of initiating event frequency plus uncertainties associated with failure probabilities of mitigating provisions.

This information is useful when considering how to interpret and aggregate the results. For instance, common cause hazards such as internal fire, seismic events and high winds are modeled more conservatively and have larger uncertainty than at-power internal events, as shown in the figure. There are two primary reasons for this difference:

- (i) There is greater uncertainty in the initiating event severities for fire, seismic and high winds for low frequencies compared to internal equipment failures. For the latter, the equipment is either functional or not. There is also greater availability of relevant component failure data for frequency quantification of equipment failures. For common cause hazards, the severity for low frequency events is extrapolated from experience with less severe but higher frequency events, so there can be substantially greater uncertainty in the initiating event severity at low frequencies. For example, it is difficult to quantify with a high degree of certainty what a 1 in 10,000 year wind is, or a 1 in 10,000 year earthquake. Sensitivity analysis is used to assess the change in SCDF or LRF to variations in event severity for low frequency initiating events.
- (ii) For common cause hazards, all units in a station can be affected. Simplifying conservative assumptions are made that the accident progression is identical in all units. This typically leads to predictions of the earliest and most severe core damage and release of radioactivity, and adds a degree of conservatism beyond that in analysis for events that are limited to a single unit.

Figure 3 indicates that differences in modeling approach and uncertainty among the PSAs for different hazard categories may not change the insights gained from PSAs, in that internal fire still dominates the risk profile in this example. Similarly, consideration of station LRF versus per reactor LRF also does not change the insight that internal fire dominates the risk in this example. Nevertheless it is important to consider differences in modeling approach, conservatism, uncertainty and station aggregation to ensure a complete understanding of the PSA results for different hazards, and the figure provides a means to communicate this information.

Additional ways of presenting PSA results to facilitate risk insights are provided in Appendix A. The appendix includes examples with increasing amounts of detail and with broader scope. The second figure in the appendix presents a template for describing all factors that affect LRF for a site, including non-reactor sources of radioactive material, the effect of uncertainties, the impact of multiple units on a site, and the relative risks associated with different categories of hazards.

## 5 Conclusions

This report has described how the whole-site risk of NPPs is evaluated in the Canadian regulatory framework. The report presents information used by utilities and the CNSC to confirm that the risk of Canadian NPPs is limited to a reasonable level, as required by the NSCA. The report also describes the role of PSA and PSA goals in assessing whole-site risk, and describes methods for documenting and communicating PSA results to convey whether the goals are met as well as safety insights from PSA.

The key conclusions of this report are:

- The level of safety and reasonableness of the whole-site risk associated with a nuclear power plant site are evaluated using qualitative and quantitative information grouped into 14 Safety and Control Areas and 73 sub-areas.
- The actual risk to the public and environment associated with operation of Canadian NPPs has been negligible, based on the measured releases of radioactivity to the environment.
- The predicted risk associated with the continuing operation of Canadian NPPs is evaluated based on predicted releases during normal operation, abnormal occurrences, design basis accidents and beyond design basis accidents.
- Only low probability beyond design basis accidents have the potential to release large quantities of radioactive material to the environment. The risk associated with such accidents is evaluated using PSA techniques taking into account mitigating factors such as post-Fukushima design enhancements and emergency management improvements.
- PSAs performed for Canadian NPPs with multiple units are Multi-Unit PSAs in that they explicitly account for the presence of multiple units in a station, even though results are typically expressed on a per reactor basis.
- PSA results for different hazard categories for single and multi-unit stations can be documented in a way that provides meaningful insights into the margins to PSA goals, into the hazards that dominate risks, and into how the risk changes when results are expressed on a per station basis compared to a per reactor basis. Examples are shown in Figure 3 and in the additional examples shown in Appendix A.

In summary, whole-site risk is not expressed as a single number or a series of numbers. Consistent with the requirements of the Canadian regulatory framework, whole-site risk comprises qualitative and quantitative information that facilitates a value judgment of the reasonableness of risk. This information includes quantitative information on the risks of large releases of radioactivity expressed on both a per reactor basis and a per station basis for stations comprising multiple reactor units.

## References

- [1] J. Vecchiarelli, K. Dinnie and J. Luxat, "Development of a Whole-Site PSA Methodology", CANDU Owners Group report COG-13-9034 R0, February 2014.
- [2] CNSC REGDOC-3.6, "Glossary of CNSC Terminology", December 2016.
- [3] M. Binder, Presentation "Managing a Regulatory Agency", University of Ottawa, E-DOCS-#4653998, March 12, 2015.

- [4] T. Jamieson, Presentation "The Role of Research and Development Information in Supporting a Safety Case", Ottawa, E-DOCS-#5102290, Nov. 2, 2016.
- [5] CNSC Public Website, <http://www.nuclearsafety.gc.ca/eng/resources/educational-resources/feature-articles/how-does-the-cnsc-define-safety.cfm>
- [6] CNSC REGDOC-2.5.2, "Physical Design – Design of Reactor Facilities: Nuclear Power Plants", May 2014.
- [7] NUREG-2201, "Probabilistic Risk Assessment and Regulatory Decisionmaking: Some Frequently Asked Questions", September 2016.
- [8] CNSC, "Regulatory Oversight Report for Canadian Nuclear Power Plants: 2016", in CMD 17-M15, June 16, 2017.
- [9] Bruce Power Report B-REP-0700-00008 R00, "2015 Environmental Monitoring Program Report", May, 2016.
- [10] OPG Report N-REP-03442-10015 R001, "2015 Results of Environmental Monitoring Programs", July 12, 2016.
- [11] NB Power Report ACR-07000-2015 Rev. 1, "Environmental Protection - 2015", April 27, 2016.
- [12] CNSC REGDOC-2.4.2, "Probabilistic Safety Assessment (PSA) for Nuclear Power Plants", May 2014.
- [13] CNSC CMD 17-M37, "Follow-Up on the August 2016 Commission Proceedings on the Anonymous Letter", August 1, 2017.
- [14] D. True, "Addressing Uncertainty: The Hobgoblin of Risk-informed Decision-making", Presentation to RIC 2015, March 10, 2015, <https://www.nrc.gov/public-involve/conference-symposia/ric/past/2015/docs/abstracts/trued-t6-r1-hv.pdf>

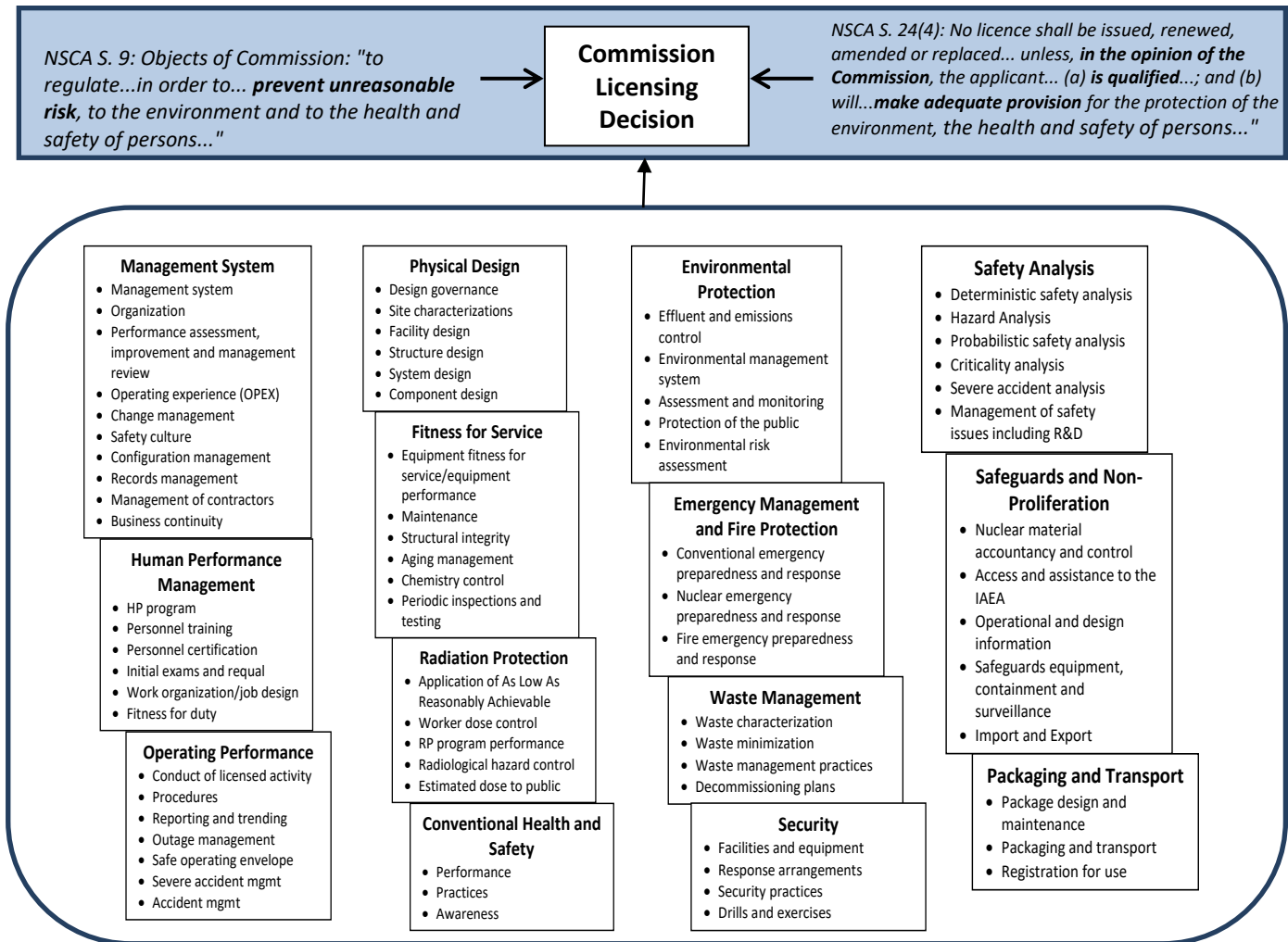
**Table 1 - Typical PSA Results**

NOTE: The results in this table are representative of a Canadian multi-unit NPP but do not correspond to a specific station.

| Hazard Category  | PSA Results<br>(per reactor per year) |                |
|--|---------------------------------------|----------------|
|  | SCDF                                  | LRF            |
| <b>INTERNAL EVENTS</b>   |                                       |                |
| At Power   | 5E-6                                  | 7E-7           |
| During Shutdown  | 1E-6                                  | - <sup>1</sup> |
| Flood  | 5E-7                                  | - <sup>1</sup> |
| Fire   | 4E-6                                  | 2E-6           |
| Total for Internal Events  | 1.8E-5                                | 2.7E-6         |
| Margin to PSA Goal   | Factor of 5.6                         | Factor of 3.7  |
| <b>EXTERNAL EVENTS</b>   |                                       |                |
| Seismic Events<br>(up to 1 in 1,000 y frequency)                     | <1E-8                                 | <1E-8          |
| Extremely Unlikely Seismic Events<br>(up to 1 in 10,000 y frequency) | 1E-6                                  | 4E-7           |
| High Winds<br>(up to 1 in 1,000 y frequency)                         | <2E-6                                 | <2E-7          |
| Extremely Unlikely High Winds<br>(up to 1 in 10,000 y frequency)     | 7E-6                                  | 7E-7           |

**NOTES:**

1. In this example set of results, a dash (-) in the table indicates that the result was not quantified because the contribution to risk is very low. For Flood events, the SCDF may be about an order of magnitude less than for other hazard categories, so the LRF will also be a small fraction of that for other hazard categories.

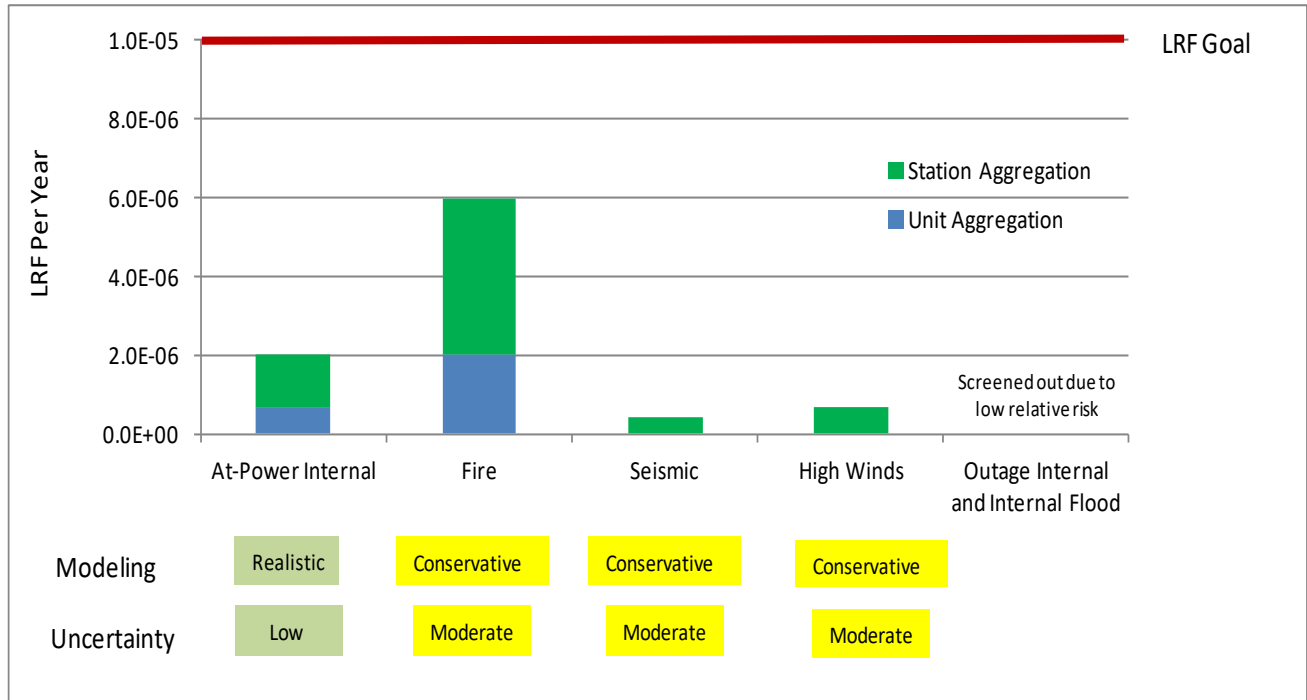


**Figure 1 - CNSC Safety and Control Areas**

SA = Satisfactory  
FS = Fully Satisfactory

| Safety and control area                  | Bruce A | Bruce B | Darlington | Pickering | Point Lepreau |
|--|---------|---------|------------|-----------|---------------|
| Management system                        | SA      | SA      | SA         | SA        | SA            |
| Human performance management             | SA      | SA      | SA         | SA        | SA            |
| Operating performance                    | FS      | FS      | FS         | FS        | SA            |
| Safety analysis                          | FS      | FS      | FS         | FS        | FS            |
| Physical design                          | SA      | SA      | SA         | SA        | SA            |
| Fitness for service                      | SA      | SA      | SA         | SA        | SA            |
| Radiation protection                     | FS      | FS      | FS         | SA        | SA            |
| Conventional health and safety           | FS      | SA      | SA         | FS        | FS            |
| Environmental protection                 | SA      | SA      | SA         | SA        | SA            |
| Emergency management and fire protection | SA      | SA      | SA         | SA        | SA            |
| Waste management                         | FS      | FS      | FS         | FS        | SA            |
| Security                                 | SA      | SA      | SA         | SA        | SA            |
| Safeguards and non-proliferation         | SA      | SA      | SA         | SA        | SA            |
| Packaging and transport                  | SA      | SA      | SA         | SA        | SA            |
| Integrated plant rating                  | FS      | SA      | FS         | FS        | SA            |

**Figure 2 - CNSC Staff Assessment of Canadian NPP Performance 2016 [8]**



**Figure 3 - Example PSA Results for Large Release Frequency**

NOTE: The results in this figure are representative of a Canadian multi-unit NPP but do not correspond to a specific station.

## Appendix A Additional PSA Results Presentation Approaches

PSAs produce a large amount of information that needs to be distilled and documented in order to effectively communicate the results and the risk insights. Section 4.3 of the main text presents one format for presenting PSA results. This appendix presents additional means of displaying PSA results to provide increasing levels of detail. These are examples only and are provided to illustrate that there is no one best way to present the results. The presentation should be tailored to the audience in a way that the results can be best understood, without being superficial or misleading.

Figure A-1 is similar in layout to Figure 3 but in this case the black horizontal bar represents the per reactor per year LRF calculated without accounting for the presence of other units. The additional information in the figure provides the following additional insights for this example set of results:

- The proximity of the black line to the unit aggregation value for Internal Fire indicates that fire events that lead to LRF are typically events that affect only single unit, because there is little difference between the single unit result and the result taking into account the impact of and on other units.
- The proximity of the black line to zero for seismic and high wind events indicates that external events that contribute to the LRF typically affect all four units.

Including the additional information in the figure helps to understand the extent to which a given hazard affects only a single unit or multiple units in its contribution to LRF. This insight would be used to evaluate additional mitigating provisions should such provisions be required.

Figure A-2 demonstrates a method to provide even more comprehensive information. This figure places Figure 3 in the main text into a broader context and summarizes additional aspects of the whole-site risk of large off-site releases. Figure A-2 is adapted from an approach developed for the Electric Power Research Institute and described in Reference [14]. The key features of this figure are:

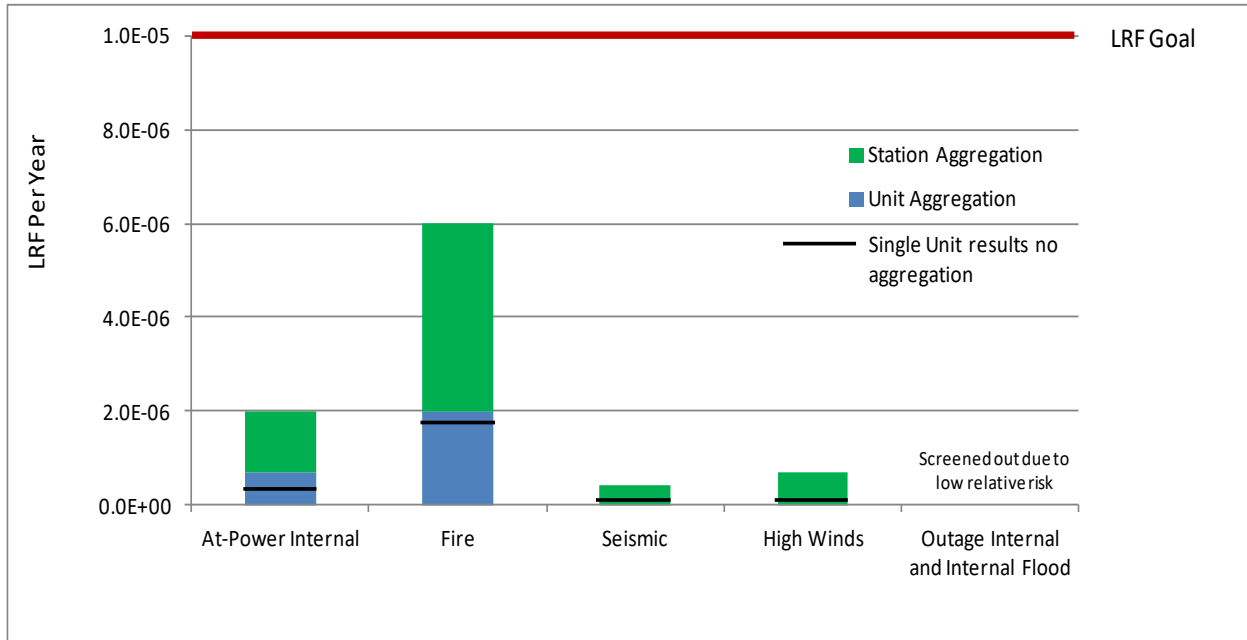
- It incorporates Figure 3 and includes text that summarizes the implications of the PSA scope, methodology, conservatisms and results.
- It shows whether PSA goals are met, and margins to the goals, for the full spectrum of internal events.
  - It provides a means to discuss potentially significant hazards not assessed with PSA. In this example, events associated with spent fuel bays are addressed through deterministic safety analysis and are in the process of being screened to determine which spent fuel events, if any, for which a PSA would provide additional safety insights.
- For external events, the figure provides a means to show that:
  - In this example, unlikely external events (those with frequencies up to 1 in 10,000 years) are small contributors to LRF. These results are shown in the embedded figure.
  - The section on Safety Margin includes results of sensitivity analysis for external events with frequencies less than 1 in 10,000 years. The purpose is to confirm that there isn't a significant increase in SCDF or LRF for frequencies just beyond 1 in 10,000 years. In this example, the SCDF for seismic events does not increase significantly until the severity increases beyond that associated with



frequencies lower than 1 in 30,000 years, confirming the robustness of the plant. Similarly, for high wind events, the SCDF only doubles, and remains small, even when events with frequencies as low as 1 in 100,000 years are considered. These results are representative of a multi-unit CANDU NPP and demonstrate the robustness of the NPP to even more extreme but unlikely postulated external events.

- The figure provides a means to illustrate the risk-dominant hazard category and whether it changes when results are expressed on a per station basis compared to a per reactor basis. In this example, internal fires dominate the risk profile. Although the PSA goals are met in this example, the figure draws attention to the risk-dominant hazard category and would prompt consideration of whether further safety improvements are warranted.
- For stations of similar but not identical design, such as Bruce A and B, the bar chart in Figure A-2 could be adapted to show PSA results for the "A" and "B" stations side by side, facilitating an understanding of the differences in results between the two stations. Similarly for Pickering, which has 2 operating "A" units and 4 operating "B" units in one station, the figure provides a means to distinguish results for the two "sides" of the plant.

Overall, Figure A-2 is a means to present PSA results in a way that provides a broader range of risk insights on a single page. The figure illustrates the change in risk insights when results are expressed on a per station basis compared to a per reactor basis. It provides a means to discuss the sensitivity of PSA results to a change in cutoff frequency for external events, and it also provided a means to integrate discussion of hazards not assessed with PSA with discussion of PSA results.



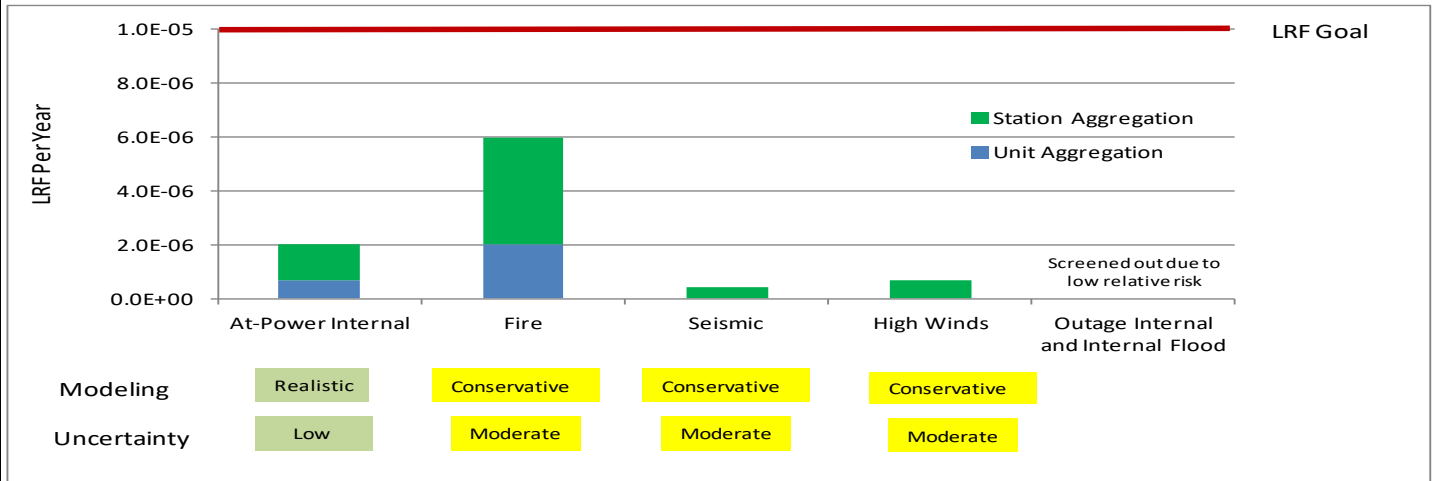
**Figure A-1 - Alternative Presentation of Aggregated PSA Results**

### Example Whole-Site PSA Results for Large Release Frequency

**Purpose**

The purpose is to summarize the safety assessment based on the Large Release Frequency (LRF), defined as the frequency of accidents causing a release to the environment greater than  $10^{14}$  Becquerels of Cs-137.

**PSA Results Summary**



Parametric Uncertainty

- Mean values represented in results

Modeling Uncertainty

- Low uncertainty for internal failures at power and during outage
- Conservative assumptions for fire initiating events
- Conservative modeling for external hazards seismic and high winds

Completeness Uncertainty

- Comprehensive scope/screening of internal and external reactor hazards. PSA performed for hazards not screened out.
- External hazards cutoff frequency 1E-4/a. Margins assessed for lower frequency events.
- Spent fuel events addressed deterministically and in the process of being screened for PSA.

Overall Results Characterization

- Individual hazard category results meet the LRF PSA goal of 1E-5 per reactor per year
- Sum of internal events LRF = 3.E-6/reactor-year, which meets the LRF PSA goal of 1E-5/a
- LRFs for seismic and high winds are small in comparison to aggregated internal events LRF

**Multi-unit considerations:** Fire hazard category dominates both single unit and multi-unit results.

Defence-in-Depth Characterization

- Defence-in-Depth improvements implemented or in progress based on Fukushima lessons learned, including fire protection improvements such as early smoke detection.

Safety Margin Characterization

- No vulnerabilities identified. No risk dominant sequences identified in Fire PSA.
- Seismic results do not increase significantly until severity exceeds that associated with 1 in about 30,000 year frequency.
- High wind SCDF only doubles and remains small even for event frequencies as low as 1 in 100,000 years.

Performance Monitoring

- Utility governance ensures potential design or operational changes are evaluated for impact on PSA results.
- Utility governance requires review if average or instantaneous PSA goals are exceeded.
- PSAs are updated every 5 years or sooner if major changes occur.

Integrated Decision-making Inputs

| PSA Goal Met? | Defence-in-Depth | Safety Margins                    | Multi-Unit Implications  | Performance Monitoring                          |
|---------------|------------------|-----------------------------------|--|---|
| Yes           | Confirmed        | Dominated by Fire hazard category | Fire still the dominant hazard category. No additional insights. | Annual average and instantaneous LRF monitoring |

Conclusions

- Individual hazard categories and the sum of results for internal hazards meet the LRF goal.
- Large margins for external hazards with frequencies 1 in 10,000 years or greater.
- Fire dominates LRF. Results credit EME and improvements in fire detection equipment. There are no risk-dominant sequences.

**Figure A-2 - Whole-Site PSA Results Summary**

## **Appendix B      Acronyms and Abbreviations**

|       |                                    |
|-------|------------------------------------|
| ALARA | As Low As Reasonably Achievable    |
| AOO   | Anticipated Operational Occurrence |
| BDBA  | Beyond Design Basis Accident       |
| CMD   | Commission Member Document         |
| CNSC  | Canadian Nuclear Safety Commission |
| COG   | CANDU Owners Group                 |
| DBA   | Design Basis Accident              |
| DSA   | Deterministic Safety Analysis      |
| EME   | Emergency Mitigating Equipment     |
| LRF   | Large Release Frequency            |
| MUPSA | Multi-Unit PSA                     |
| NB    | New Brunswick (Power)              |
| NPP   | Nuclear Power Plant                |
| NRC   | Nuclear Regulatory Commission      |
| NSCA  | Nuclear Safety and Control Act     |
| OPG   | Ontario Power Generation           |
| PSA   | Probabilistic Safety Assessment    |
| SCA   | Safety and Control Area            |
| SCDF  | Severe Core Damage Frequency       |