Summary of the Methodology and Results of the 2019 Bruce A and Bruce B Probabilistic Safety Assessments

OCTOBER 2022

Prepared by: Rob McLean, Senior Technical Specialist, NSAS 3APR2023

Verified by: Umeir Mian, Senior Technical Engineer, NSAS 3APR2023

Digitally signed by Jimena Nunez
Date: 2023.04.03 15:11:03 -04'00'

Approved by: Jimena Nunez, Section Manager, NSAS

Table of Contents

Page

1.0 PURPOSE

The purpose of this document is to summarize the methodology and results of the 2019 probabilistic safety assessment which provides a comprehensive and integrated assessment of the risks at the Bruce A and Bruce B stations. The probabilistic safety assessment is prepared to comply with Bruce Power's internal risk management governance and CNSC Regulatory Document RD-2.4.2. This document summarizes the results of the probabilistic safety assessment for public disclosure.

2.0 INTRODUCTION

CNSC Regulatory Document RD-2.4.2 "Probabilistic Safety Assessment (PSA) for Reactor facilities" was written to provide the requirements and guidance for conducting PSA by Canadian nuclear utilities. PSAs are used by regulators and operators a like in assessing the adequacy of plant design and operation as compared to other societal risks, identifying areas of dominant risk and optimizing the use of resources. PSAs have been performed at the Bruce Power stations since the early 1990s and risk considerations were included in their original designs.

Bruce Power uses two internationally recognized risk metrics to assess the risk of potential accidents at its stations:

(a) Severe Core Damage Frequency (SCDF), a measure of the likelihood of releasing radioactive material from the fuel into containment, and
(b) Large Release Frequency (LRF), a measure of the potential for release of radioactive material to the environment from containment.

These metrics are quantified in Level 1 and Level 2 PSA respectively, with the results expressed as a frequency of occurrence per year. These metrics ensure that public and environmental risk from the operation of nuclear stations is understood, and compliance with prescribed safety goals ensures that public safety is maintained.

Bruce Power's internal safety goals and administrative targets for these risk metrics are provided in Table 1. It is noted that the 2018 PSA results submitted to the CNSC by Bruce Power meet the safety goal in all cases at both Bruce A and B.

Table 1 – Bruce Power Safety Goals and Administrative Limits[1]

Safety Goal (application)	Average Risk (per year)	
	Administrative Target	**Safety Goal**
Large Release (per unit)	10^{-6}	10^{-5}
Severe Core Damage (per unit)	10^{-5}	10^{-4}

3.0 SCOPE

As required by RD-2.4.2, Bruce Power has used PSA to assess the risk from internal and external events, for reactors both at-power and during the outage state. This includes determination of severe core damage frequency for internal events (at-power and outage) internal fires, internal floods, high winds/tornadoes and seismic (Level 1 PSA). Large release frequency is also assessed for internal events at-power, internal fires, high winds and seismic[2] (Level 2 PSA). Each of these studies was executed with methodologies and codes accepted by the CNSC.

An extensive screening of external hazards is performed as part of RD-2.4.2 compliance to determine those hazards (e.g., internal fires, seismic) which require more detailed PSA to characterize the risk. Other hazards such as avalanches and forest fires are screened using internationally accepted qualitative and quantitative methods.

Additionally, sources of radioactivity other than the reactor core are assessed for the potential to impact public safety. Assessments of stored fuel on site, and the irradiated fuel bays are made. Also, intermediate operation states between at-power and outage are considered. The risk metrics identified are representative of a single reactor unit. Multi-unit impacts (the ability of another operating unit to cause a transient (negative) or provide aid (positive) is implicitly considered in the PSA.

---

[1] The goals and targets are expressed in scientific notation. They represent the very low predicted frequency of core damage or large release events. For comparison, annual frequencies of 10^{-4}, 10^{-5}, 10^{-6} can be expressed as a probability of occurrence of one in 10,000, one in 100,000 and one in 1,000,000 per year. Meetings these limits ensures that the risk from reactor operation is kept to an acceptably low level.

[2] RD-2.4.2 allows for low risk contributors to not require formal PSA on the basis of screening and bounding analysis. This is done in a systematic manner which is also formally reviewed and accepted.

4.0 RISK ASSESSMENT

PSA provides a methodical and analytical approach to quantifying and comparing risks, both their frequency and consequence, helping Bruce Power to decide on how best to operate, maintain and invest in the plant to uphold adequate levels of safety.
PSA answers the following three questions:

(a) What can go wrong? (hazard identification)
(b) How likely is it to happen? (frequency analysis)
(c) What are the consequences? (consequence analysis)

By answering these questions, risk metrics can be compared to regulatory requirements and internal governance which serve as representations of adequate public safety.

5.0 SUMMARY OF PROBABILISTIC SAFETY ASSESSMENT METHODOLOGIES AND RESULTS

Bruce Power conducts PSA for internal and external events to characterize and assess risk. A summary of the approach and results for each study is provided in the following sections.

5.1 Level 1 At-Power Internal Events PSA

Internal events are events that occur due to failure of a structure, system, component or human error from the normal operation of the plant. Failures that lead directly, or in combination with other failures, to damage to fuel in the reactor are considered. The major elements of the Level 1 PSA for internal events are:

- **Initiating Event Identification and Quantification** - Events which may challenge plant operation and require intervention from mitigating systems are identified (e.g., loss of offsite power, steam generator tube ruptures). Frequencies of occurrence for these events are determined based on observed events at the Bruce Power site, similar CANDU reactors, and internationally. Initiating events that originate in the accident unit, another unit, or impact multiple units are included.
- **Accident Sequence Analysis** - Potential sequences of events which lead to fuel damage and potential severe core damage are systematically identified based on postulated failures of the plant and operator responses.
- **System Fault Tree Analysis** - The specific ways systems may fail to function for specific accidents are identified. The impact of failure of unitized systems and systems which are shared between units (such as electrical power and service water) are considered.
- **Human Reliability Analysis** - The human errors due to operators failing to respond or responding incorrectly to an event are identified and quantified.

- **Reliability Parameter Estimation** - Data is used to quantify failures by incorporating station-specific failure probabilities for the components in the systems and structures.
- **Probabilistic Safety Assessment Model Integration and Quantification of Accident Sequences** - The resulting probabilistic safety assessment model developed in the previous steps is evaluated to quantify the risk for a number of fuel damage events, including severe core damage.
- **Uncertainty, Sensitivity and Importance Analysis** - Statistical uncertainty in the risk results is determined, along with the sensitivity of the results to specific modeling assumptions. Dominant contributors and risk-significant systems, structures and components are identified.

The resulting Level 1 at-power internal events severe core damage frequency at Bruce A is 3.18E-06/reactor-yr (three in one million), and at Bruce B is 2.78E-06/reactor-yr (three in one million). These both meet the Bruce Power safety goal of 1E-04/reactor-yr (one in ten thousand).

5.2 Level 2 At-Power Internal Events Probabilistic Safety Assessment

The Level 2 PSA takes accident sequences of the Level 1 PSA as inputs, and evaluates the capability of containment to prevent a core damage event from releasing radionuclides to the public. Both single unit and multi-unit impacts are considered in the Level 2 probabilistic safety assessment. The major elements of the Level 2 probabilistic safety assessment for internal events are:

- **Plant Damage State Definition and Bridging Event Tree** - The output of the Level 1 analysis is used to characterize plant damage states representing the extent of core damage and containment states needed to populate the Level 2 probabilistic safety assessment.
- **Containment System Fault Tree Analysis** - Fault trees are developed that model the ways that containment systems can fail.
- **Containment Event Tree Development** - Event trees are developed that model the ways containment is impacted by the consequences of severe accident progression and phenomena.
- **Containment Branch Point Quantification** - Probabilities are assigned to failures induced by the phenomena (e.g., hydrogen burns, overpressure) which may occur during a severe accident.
- **Severe Accident Progression Analysis** - The severe accident analysis code MAAP4-CANDU is used to perform consequence analysis to determine the extent of damage, the success of mitigation, and the potential for containment failure induced by the accident sequence.
- **Release Categorization and Source Term Analysis** - Releases are quantified and categorized on the basis of the source term (amount of radioactive material released)

and containment impairments or failures. Both the amount of radioactive material released and the timing of the release are important to categorization.

- **Level 1/Level 2 Integration** - The models are integrated to incorporate the frequency contribution of the Level 1 probabilistic safety assessment so an overall large release frequency can be quantified.
- **Uncertainty, Sensitivity and Importance Analysis** - Statistical uncertainty in the risk results is determined, along with the sensitivity of the results to specific modeling assumptions. Dominant contributors and risk-significant systems and components are identified.

The Level 2 at-power internal events large release frequency at Bruce A is 7.40E-07/reactor-yr (seven in ten million), and at Bruce B is 5.0E-07/reactor-yr (five in 10 million). These both meet the Bruce Power safety goal of 1 E-05/reactor-yr (one in one hundred thousand).

5.3 Level 1 Outage Probabilistic Safety Assessment

The outage probabilistic safety assessment characterizes outages by definition of plant outage states, which represent the outage configurations. This is based on the availability and alignment of heat sinks and the guaranteed shutdown method used. The outage probabilistic safety assessment starts with the reactor already in a shutdown state, and is characterized by slower accident progression than an at-power reactor. The elements of the outage probabilistic safety assessment are:

- **Plant Operational State Identification** - Discrete states of the outage are defined based on the status and configuration of the heat transport system, moderator system and the guaranteed shutdown state. The duration in each state is determined based on outage experience.
- **Initiating Event Identification and Quantification** - This involves identification of outage-specific initiating events, in addition to the initiating events already identified for at-power probabilistic safety assessment and the quantification of their frequency of occurrence.
- **Accident Sequence Analysis** - The progression of the abnormal operational occurrence, or accident due to failure of mitigating systems and actions is identified.
- **System Fault Tree Analysis** - The specific ways that systems may fail to provide their mitigating function for specific outage accidents are identified. The impact of failure of unitized systems and systems which are shared between units (such as electrical power and service water) are considered, along with the potential outage configurations of these systems.
- **Reliability Parameter Estimation** - Data is used to quantify system failure by incorporating station-specific failure probabilities for the components in the mitigating systems.
- **Human Reliability Analysis** - The human errors due to operators failing to respond or responding incorrectly to an accident in an outage unit are identified and quantified.

- **Probabilistic Safety Assessment Model Integration and Quantification of Accident Sequences** - The resulting probabilistic safety assessment model developed in the previous steps is evaluated to quantify the outage risk for a number of fuel damage events, including severe core damage.
- **Uncertainty, Sensitivity and Importance Analyses** - Statistical uncertainty in the outage risk results is determined, along with the sensitivity of the results to specific modeling assumptions. Dominant contributors to the outage results and risk-significant systems and components are identified.

The Level 1 outage internal events severe core damage frequency at Bruce A is 1.01E-5/reactor-yr (one in one hundred thousand), and at Bruce B is 7.80E-06/reactor-yr (eight in one million). These both meet the Bruce Power safety goal of 1E-04/reactor-yr (one in ten thousand).

5.4 Fire Probabilistic Safety Assessment

The Fire PSA characterizes risk to the plant from fire scenarios induced by fixed and transient ignition sources, with the potential to propagate and damage other plant equipment, cabling and fuel sources.

The approach is similar to the internal events PSA with the exception that the failure of equipment is due mainly to postulated fires rather than the random failures of equipment. Figure 1 outlines the internal fire PSA methodology. Tasks 1 to 3 involve the identification of components and equipment that could either cause or be impacted by a fire. Qualitative screening is performed in Task 4 to rule out areas of the plant which do not have one or the other (and hence cannot be consequential to plant risk). This allows analytical resources to be focused on plant areas of the most risk. Task 5 employs plant logic to determine what failures could arise from fire damage, using the Level 1 at-power internal events probabilistic safety assessment as the basis, and Tasks 6 and 12 support the quantification of fire scenarios such that preliminary screening can be performed on low-risk areas of the plant. Tasks 8 through 11, model the actual impact of the postulated fires on plant equipment based on its location, heat intensity, and potential for mitigation. This detailed modelling of the fire hazards and the effects on electrical circuits impacted by them is a key element of the Fire probabilistic safety assessment. With these impacts known, the model is then quantified and documented in the remaining tasks, with appropriate treatment of human reliability and uncertainty/sensitivity assessment. The quantified model provides insight into probabilistic safety assessment metrics due to fire, as well as the relative importance's of different fire initiator types, operator responses and equipment.

Level 1 Fire severe core damage frequency at Bruce A is 6.10E-06/reactor-yr (six in one million), and at Bruce B is 2.97E-06/reactor-yr (three in one million). These both meet the Bruce Power safety goal of 1E-04/reactor-yr (one in ten thousand). Level 2 Fire large release frequency at Bruce A is 5.37E-06/reactor-yr (five in one million) and at Bruce B is 7.72E-07/reactor-yr (seven in ten million). These both meet the Bruce Power safety goal of 1E-05/yr (one in one hundred thousand).

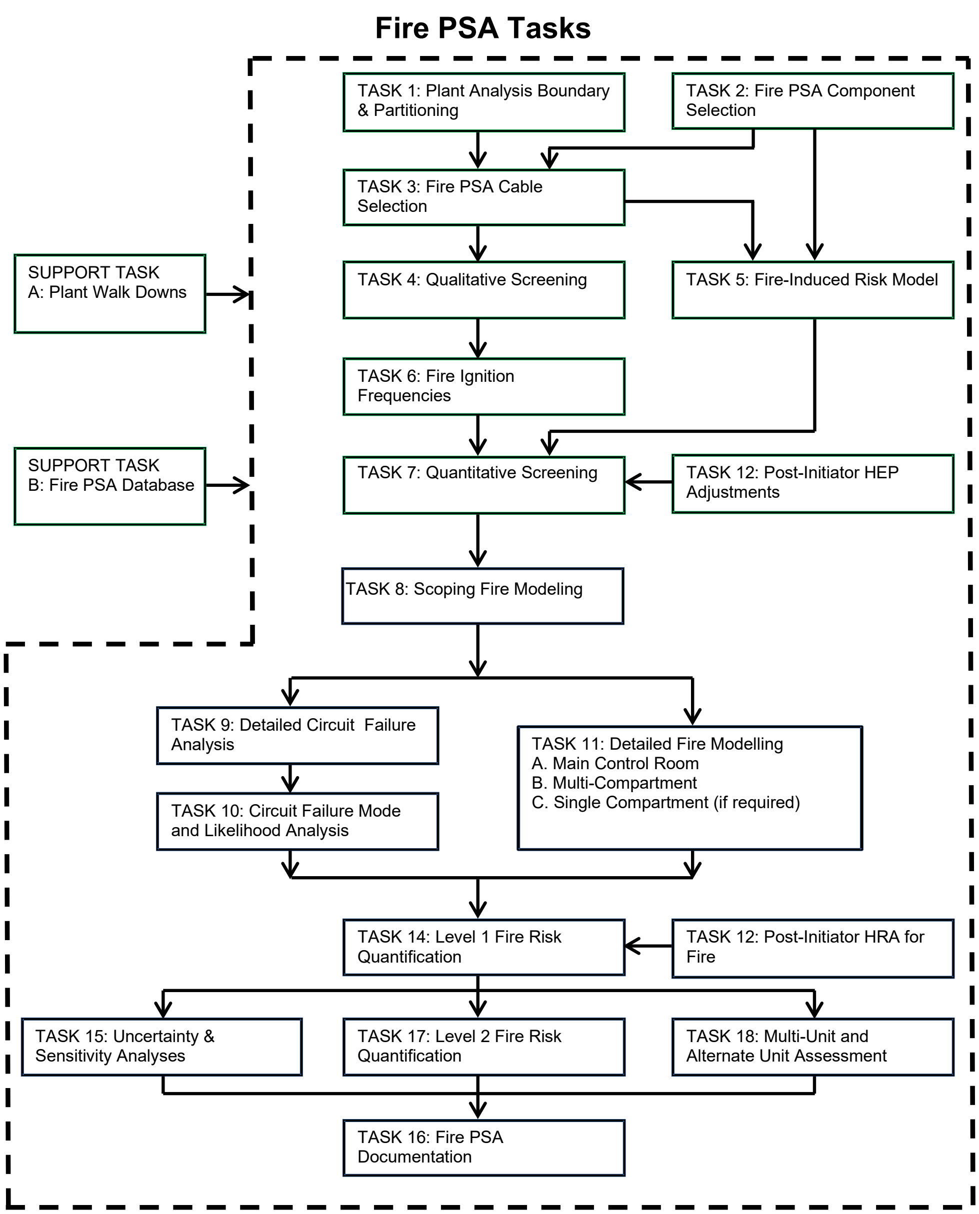

Figure 1 – Internal Fire PSA Methodology

5.5 Internal Flood Probabilistic Safety Assessment

The internal flood probabilistic safety assessment characterizes risk to the plant from flooding scenarios from sources in the plant. The critical sources considered are high volume and high flow service water systems. Again, the approach is similar to that taken in any probabilistic safety assessment study (see Figure 2). Tasks 1 to 3 identify flooding sources and targets potentially impacted by floods. Plant walk downs are conducted to confirm understanding of the plant layout and condition of systems, structures and components from a flood perspective. On this basis, qualitative screening is performed in Task 4, ruling out areas where no flood sources exist, or systems, structures and components of importance are inconsequentially impacted. Tasks 5 through 8 characterize flood scenarios on the basis of their consequences and impacts, and consider the potential for mitigating such hazards. Tasks 9 and 10 integrate and quantify the modelling of these flooding scenarios to arrive at an evaluation of core damage frequency due to internal floods. Tasks 11 and 12 were not necessary in the study at either Bruce A or Bruce B due to the low overall risk and confirmation of unit similarity during walkdowns.

Level 1 Internal Flood severe core damage frequency at Bruce A is 6.3E-08/reactor-yr (six in one hundred million), and at Bruce B is 8.0E-08/reactor-yr (eight in one hundred million). These both meet the Bruce Power safety goal of 1E-04/reactor-yr (one in ten thousand).

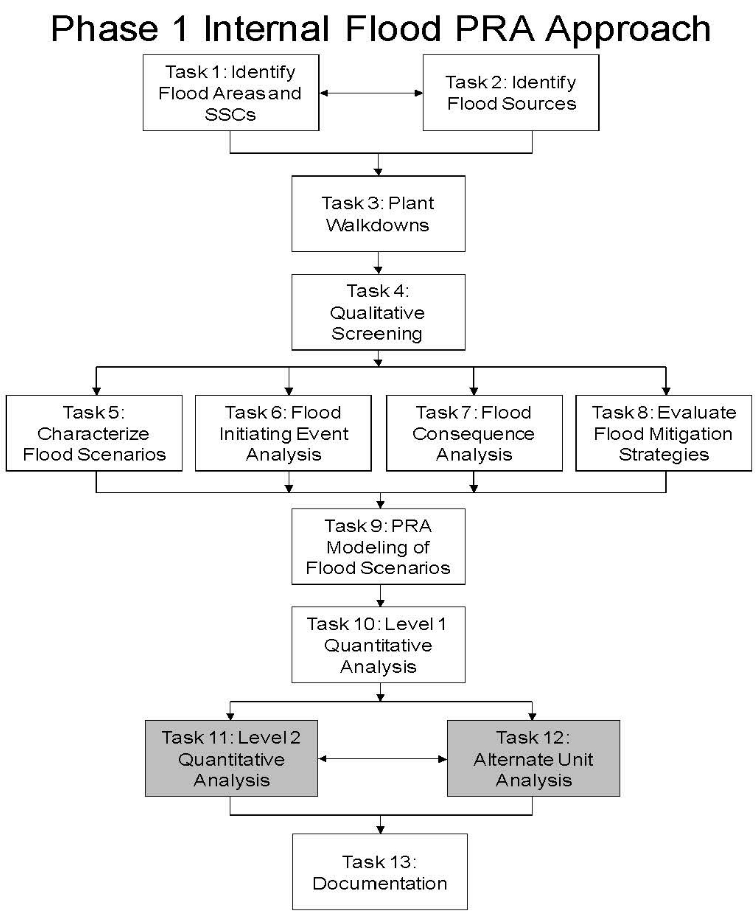

Figure 2 – Internal Flood Probabilistic Safety Assessment Methodology

5.6 Seismic Probabilistic Safety Assessment

The seismic probabilistic safety assessment characterizes risk to the plant from seismic events. Figure 3 shows the Seismic probabilistic safety assessment methodology. The seismic probabilistic safety assessment starts in Task 1 from a characterization of the seismic hazard at the Bruce Power site. The response of the plant and the necessary systems credited to ensure a safe shutdown are modelled in Task 2. An iterative process is then taken in Tasks 3 through 6 to characterize, model and confirm the response of plant equipment and structures to different magnitude of seismic hazards. This involves a review of plant records starting with their seismic design specifications and functions to confirm the design and ending with a confirmation of anchorages and structures in the field. Finally, seismic risk is quantified, using the Level 1 at-power internal events probabilistic safety assessment as the basis, to arrive at an evaluation of severe core damage frequency due to seismic events.

Level 2 quantification is performed in a conservative bounding manner. Since the Level 1 Seismic probabilistic safety assessment assumes correlated impacts to all four units given a seismic event likely impacts all four units, it is assumed that all seismic severe core damage events would result in multi-unit challenges to the containment function. It was confirmed that the containment structure and components have a very low likelihood of failure (seismic fragility) for the same range of seismic events as considered in the Level 1 probabilistic safety assessment and an estimated seismically-induced containment failure was determined. Large release frequency is therefore estimated to be no higher than the calculated severe core damage frequency.

Level 1 seismic probabilistic safety assessment severe core damage frequency at Bruce A is 7.64E-07/reactor-yr (seven in ten million), and at Bruce B is 6.40E-07/reactor-yr (six in ten million). These both meet the Bruce Power safety goal of 1E-04/reactor-yr (one in ten thousand). As noted above, these two values are both taken as conservative estimates of the large release frequency for both stations, and both meet the Bruce Power safety goal of 1E-05/reactor-yr (one in one hundred thousand).

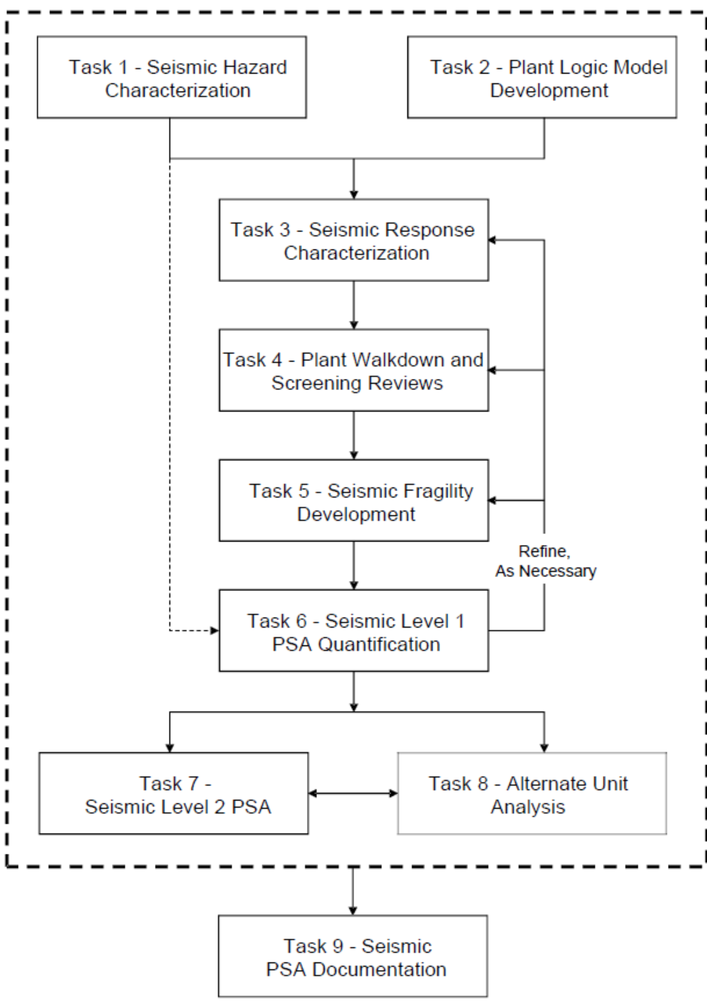

Figure 3 – Seismic Probabilistic Safety Assessment Methodology

5.7 High Winds Probabilistic Safety Assessment

The High Winds probabilistic safety assessment characterizes risk to the plant from tornado and straight line wind events. Figure 4 shows the High Winds probabilistic safety assessment methodology. A site walkdown was conducted to understand the layout of the stations, the potential for missile generation from equipment on site, means to protect the stations from winds and missiles. Task 1 developed a spectrum of wind hazards for both tornadoes and straight line winds based on the site location and meteorology. This was used to determine the potential generation of missiles in Task 2. The output of both these tasks were combined in Task 3 in consideration of the fragility of the plant structures, systems and components that could be impacted by wind itself or by wind-generated missiles. Task 4 developed the plant response to the failures induced by the hazard, and the convolution of these consequences and frequencies developed previously was quantified in Task 5, resulting in evaluation of core damage frequency for high winds, using the Level 1 at-power internal events probabilistic safety assessment as the basis.

Similar to the evaluation of Level 2 risk in the seismic study, severe core damage frequency is used as a demonstrably conservative bound on large release frequency for High Winds on the assumption that the majority of severe core damage frequency from High Winds affects multiple units.

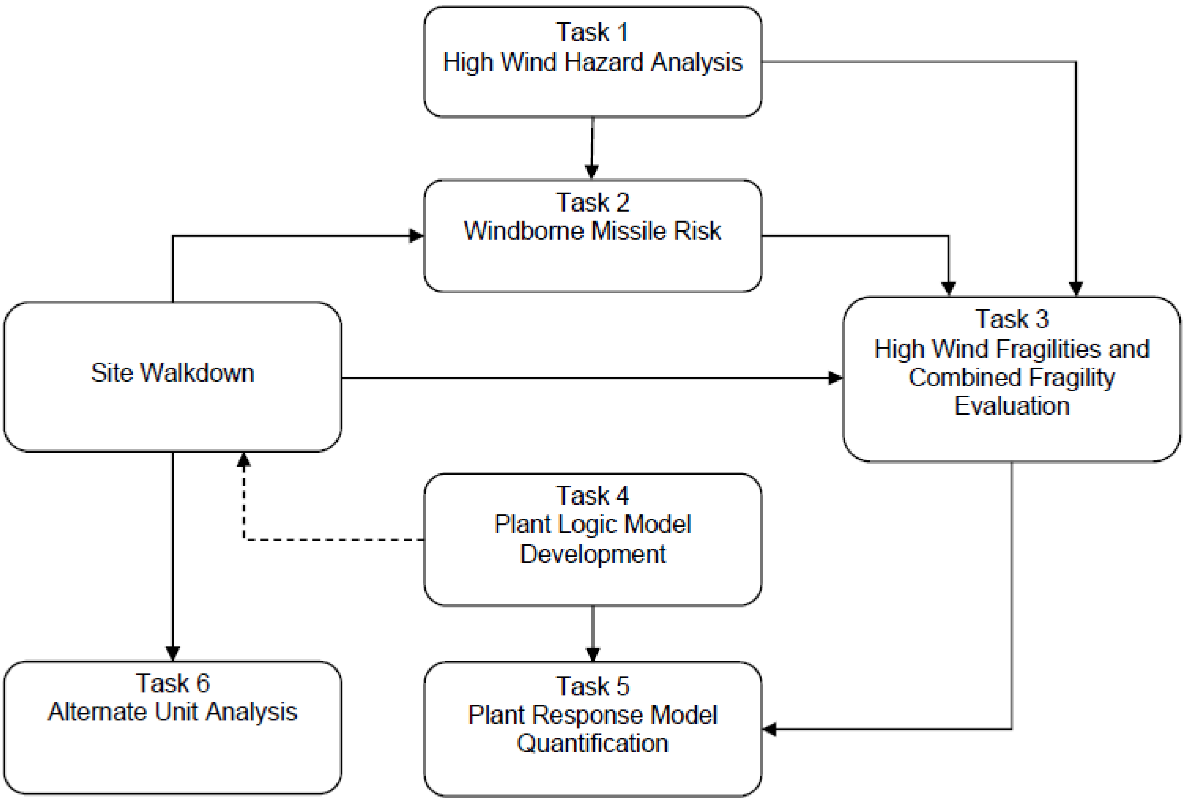

Figure 4 – High Winds Probabilistic Safety Assessment Methodology

Level 1 High Winds probabilistic safety assessment severe core damage frequency at Bruce A is 6.60E-07/reactor-yr (seven in ten million), and at Bruce B is 8.70E-07/reactor-yr (nine in 10 million). These both meet the Bruce Power safety goal of 1E-04/reactor-yr (one in ten thousand). As noted above, these two values are both taken as conservative estimates of the large release frequency for both stations, and both meet Bruce Power safety goal of 1E-05/reactor-yr (one in one hundred thousand).

5.8 Identification and Assessment of Plant Operating States

The assessments for Plant Operational States (POSs) for Bruce A and Bruce B were performed using industry standard methodology. Assessment was performed for other states where the reactor is expected to operate for extended periods of time and that are not covered by the at-power and shutdown PSAs, per REGDOC-2.4.2. The selection of POS involved the following steps:

- Develop criteria for POS selection;
- Review the Bruce A and B operating procedures to identify key features of planned shutdown evolutions and start-up evolutions;

- Apply the criteria for POS selection to the identified transition states. This step was supported by thermal-hydraulic analysis of unmitigated initiating events (IE) occurring at selected key operating states; and
- Recommend POS alignments for use in the PSAs,

The conclusions for both Bruce A and Bruce B are:

- The zero-power hot (ZPH) operating state, and transitions between Full Power and ZPH, can be grouped with the Full Power state and considered as part of the at-power PSAs;
- Extended power holds between Full Power and ZPH can be grouped with the Full Power state and considered as part of the at-power PSAs; and
- Cold pressurized and cold depressurized states outside of the guaranteed shutdown state (GSS) can be screened out of the PSA.

These assessments confirmed that all intermediate power states are effectively bounded by the existing at-power and shutdown studies, requiring no further assessment.

5.9 Identification and Assessment of Radioactive Sources Other than the Reactor Cores

Per the requirements of REGDOC-2.4.2, non-reactor sources of radioactivity on the Bruce A and Bruce B sites were identified and screened. The Western Waste Management Facility (WWMF) and Bruce A and Bruce B Irradiated Fuel Bays (IFB) were the only non-reactor sources of radioactivity requiring assessment. The Bruce A and Bruce B IFB assessments were completed following the methodology accepted by the CNSC. Each non-reactor source of radioactivity was screened from consideration and no further PSA assessment was required.

6.0 CONCLUSION

The Bruce Power probabilistic safety assessment studies have been conducted following methodologies accepted by the CNSC and meeting the requirements of CNSC Regulatory Document RD-2.4.2. The results of these studies demonstrate Bruce Power's compliance with internal governance for nuclear safety risk.