POINT LEPREAU NUCLEAR GENERATING STATION

Probabilistic Safety Assessment

SUMMARY REPORT
0087-03610-0002-001-PSA-A-02

For Information

Available Upon Request

Template # 0139 Rev. 5 2019-08-30

0087-03610-0002-001-PSA-A-02
REGISTERED 2021 DEC 16

Document Approval

The document has been electronically approved through E-form # 1705732 on this date 2021-12-14.
The following approvals are required prior to issue.

Role	Name
Author	Daniel F. Basque
Reviewer	Andre Jean
Document Owner (Approved by)	Will Higgins
Process Owner (Approved by)	Jennifer Lennox

Revision Record

The following is the latest revision record for this document.

Rev. #	Date	Page	Section	Comments
2	2021-10-04			Update to reflect latest work in PSA.

Classification Statement

Proprietary usage

This document has commercial value to NB Power. Hence, without our prior written approval, it must not be copied or distributed to a third party.

A copy of this document may be obtained from NB Power provided an agreed fee (specific for this document and available upon request) is paid to NB Power.

Requests should be made to the Process Owner/Document Owner noted in the "Document Approval" section, at Point Lepreau Nuclear Generating Station, P.O. Box 600, Lepreau, New Brunswick, Canada E5J 2S6.
(Tel. 506-659-2220)

Executive Summary

Point Lepreau Nuclear Generating Station's highest priority is the safety of its workers and the public. It is operated daily to the highest nuclear safety standards and is held to rigorous requirements by the national nuclear regulator. When the plant was being designed and sited at Point Lepreau, guidelines and early regulatory documents provided an expectation that certain systems achieve specific reliability targets which is included within the design basis of the plant. During original plant construction, analytical tools called safety design matrices (SDMs) for various postulated accidents considered within the design basis were developed using simplified hand-drawn models. The intent of the safety design matrices was to identify if there were areas where the plant and operators would benefit from design improvements.

During subsequent years, the international community continued to develop techniques for probability-based assessment. As methodologies matured and were adopted more widely, PSA became a tool of choice for nuclear power plant operators to integrate many different aspects of design and operation to assess the likelihood of causing damage and incurring a large radiological release. The aim is to examine opportunities for improvement to design, maintenance and operations where it makes sense to do so. However, the difference between the earlier safety design matrices and PSA is that the latter now extends examining plant response from design basis accidents to a broader view of accidents beyond the design basis where all levels of plant defenses have failed. Although highly unlikely, when such occurs, consequences could be severe and are referred to as "severe accidents". These are defined as a condition where there is extensive physical damage to multiple fuel channels leading to loss of core structural integrity.

In the early 2000's when NB Power was considering life extension, it committed to the Canadian Nuclear Safety Commission (CNSC) to perform a PSA for PLNGS following international guidelines and best industry practice. This would ensure that the full range of potential accidents would be considered and opportunities for plant improvement identified for possible inclusion in the refurbishment outage scope. The objective was to make the plant more robust and provide a reasonable higher degree of safety for its workers and the public. That first PSA was completed in 2008, was submitted to the CNSC and was, accepted. Many modifications were made to the plant as a result, which was expected, since the plant was not originally designed to deal with severe accidents. The plant is now far more robust in dealing with severe accidents.

Executive Summary, Continued

To meet current regulatory requirements, NB Power is required to update its PSA on a periodic basis. As part of that scope of work, all potential external hazards and their combinations were re-examined. In response to the CNSC Integrated Action Plan [4] three particular hazards; earthquakes, tsunami and high winds were reassessed using latest methodologies and knowledge. PSA methodologies were adjusted as necessary in response to those assessments as well as evolution in regulatory guidance, standards and industry practices. Since the original PSA, two versions were submitted, the latest updates being completed in stages with the final work completed and submitted to the CNSC in 2021. This report provides a summary of the results of the PSA in addition to how it was carried out.

It is important to note that a PSA is an assessment tool that provides a risk-informed assessment that is complementary to other traditional evaluation techniques such as deterministic safety analysis, engineering analysis, etc. It is not intended to replace those evaluation techniques but rather provides further insights from a quantitative risk perspective. PSAs are limited in what they can practicably model and, therefore, it is important to understand those limitations so that PSA-related information is used in the correct context within decision making in an operating nuclear power plant.

Overall plant safety is provided by combination of the station's programs and procedures, training effectiveness, equipment maintenance practices, work control, configuration management, system and equipment monitoring and corrective action, and emergency procedures and abnormal condition response. PSA is one of many tools that provide a measure of, or indicator of, safety but given its limitations cannot be considered in isolation of other measures or deterministic safety analysis. It is a complementary tool and in itself does not provide safety per se.

While a PSA also provides a quantitative estimate of plant risk, the limitations of PSA modeling and content means that care must be taken in interpreting results and trying to derive meaningful insights from a PSA. It also limits the usefulness of such estimates in an absolute value sense. Quantitative risk estimates from PSA can be compared to safety goals based on international targets; however, their value is primarily in considering them as a "measuring stick" to determine the size of a safety improvement that may be identified from the PSA to resolve potential plant vulnerability.

Executive Summary, Continued

International expert consensus is that it is through the act of performing a PSA, developing event sequences and evaluation that one develops insights into possible vulnerabilities of a nuclear power plant and where it may be worth investing in safety-related improvements. The PSA developed for Point Lepreau Nuclear Generating Station considered all hazards to which the plant may be susceptible including internal hazards (that is, internal equipment failures, internal fires and internal floods) and for seismic events (i.e., external hazard). All other external hazard and combinations of hazards have been screened out from further detailed analysis using PSA.

In all cases and regardless of how the results are presented, safety goals related to PSA are met for Point Lepreau Nuclear Generating Station.

Table of Contents

List of Figures

List of Tables

1.0 Introduction

Nuclear power plants are designed and built with layers of protection against accidents. A probabilistic safety assessment (PSA) is an analytical technique for integrating many different aspects of design and operation to assess the likelihood of damaging a particular facility, in this case a nuclear power plant, and incurring a large radiological release. A PSA can also be used to develop an information base for analyzing plant-specific and generic issues.

It is important to note that a PSA is an assessment tool that provides a risk-informed assessment that is complementary to other traditional evaluation techniques such as deterministic safety analysis, engineering analysis, etc. It is not intended to replace those evaluation techniques but rather provides further insights from a quantitative risk perspective. PSAs are limited in what they can practicably model and, therefore, it is important to understand those limitations so that PSA-related information is used in the correct context within decision making in an operating nuclear power plant. Examples of limitations include:

- Software and computational limitations that limit the size of models and quantification capability. For example, only human errors of omission[1] are included in modeling and not human errors of commission[2], the latter having a large number of possible combinations and permutations; and,
- The effectiveness of programs such as periodic inspection programs to detect and resolve piping degradation is prior to failure is not readily modeled in a PSA. Industry operating experience data for piping failures is instead utilized in the models as being representative. Another example includes heavy lift programs and procedures that, if not effective, could potentially result in failure of important equipment caused by falling heavy equipment if a failure occurs with a crane or rigging. These types of programs cannot be reasonably modeled in a PSA.

As discussed further in *Section 6.1*, overall plant safety is provided by the combination of the station's programs and procedures, training effectiveness, equipment maintenance practices, work control, configuration management, system and equipment monitoring and corrective action, and emergency procedures and abnormal condition response. PSA is one of many tools that provide a measure of, or indicator of, safety but given its limitations cannot be considered in isolation of other measures or deterministic safety analysis. It is a complementary tool and in itself does not provide safety per se.

[1] An error of omission is when an operator fails to perform a particular action as specified by a procedure
[2] An error of commission is when an operator takes an action not included in a procedure and exacerbates the postulated accident.

1.0 Introduction, Continued

While a PSA also provides a quantitative estimate of plant risk, the limitations of PSA modeling and content means that care must be taken in interpreting results and trying to derive meaningful insights from a PSA. There is far more value to an operating nuclear power plant in considering quantitative risk estimates in the context of system configuration management to identify the relative change in risk as a result of equipment degradation or changes to availability of equipment.

International expert consensus is that it is through the act of performing a PSA, developing event sequences and evaluation that one develops insights into possible vulnerabilities of a nuclear power plant and where it may be worth investing in safety-related improvements.

1.1 PSA Terminology

The PSA consists of Level 1 and Level 2 assessments for internal events at-power and in the shutdown state, and for other events at power. The sub-sections below provide further information related to PSA terminology and content.

1.1.1 Level 1 PSA

A Level 1 PSA consists of the identification and quantification of accident sequences, component data and human reliability. It includes an analysis of plant design and operation with emphasis on the accident sequences that lead to core damage, their basic causes, and their frequencies. It does not investigate the frequency or mode of containment failure or the consequences of radionuclide releases. Internal hazards such as process system failures, internal fires and internal flooding, and external hazards such as earthquakes, are included.

1.1.2 Level 2 PSA

A Level 2 PSA consists of an analysis of the physical processes of an accident and the response of containment in addition to the analysis performed in a Level 1 PSA. It predicts containment failure modes and the frequency and inventory of radionuclide releases to the environment at the containment boundary using severe accident analyses.

1.1.3 Internal Hazards

In general terms, internal hazards are those hazards that originate from sources located on the Point Lepreau Nuclear Generating Station site both inside and outside plant buildings.

1.1.3.1 Internal Events

Internal events are a subset of internal hazards and represent any event that progresses from failure of a structure, system or component. These are events which, if not mitigated, could lead to core damage and/or external plant releases. Typically, internal initiating events are abnormal conditions generated within the plant, as the result of a failure of some process function, due to equipment failure or human error.

1.1.3.2 Internal Fires

For internal fire events, internal causes include failure of equipment identified as potential ignition sources (active or passive components that are energized and/or contain combustible material), sparks from hot work such as welding and cutting, and human error. Fires induced by outside sources such as lightning, terrorist attack, earthquake or external flood are beyond the scope of this event. Earthquake-induced plant equipment fires are treated in seismic assessments. Failure of components containing significant combustible material due to seismic events is also addressed as part of the seismic assessment.

1.1.3.3 Internal Floods

Floods affecting plant safety could be due to sources outside the plant or inside the plant. Internal floods may result from component failures, or from the incorrect operation of equipment or systems within the plant. Internal floods may occur, for example, as a result of a rupture of a pipe or a vessel, or be caused by leakage from a component that is incorrectly assembled or is left in a disassembled state following maintenance An internal flood may potentially lead to core damage by first causing the failure of the systems that maintains heat sink, and then by potentially contributing to some failures of engineered systems that are designed to mitigate such events.

1.1.4 External Hazards

External hazards are those events that originate externally to the plant, such as earthquakes, hazards that might cause flooding of the site, and extreme winds that may cause damage to plant structures and the systems and components within. Because of the broad-ranging effects these external hazards may have on a nuclear power plant, these are also referred to as a “common cause” or “common mode” initiator. In other words, the event itself can cause failures of redundant components and systems, and thereby reduce the number of mitigating systems available to bring the plant to a safe and stable state following failure of a safety-related process system.

All external hazards, whether man-made or naturally-induced, which may be viewed as a potential common-mode failure mechanism for Point Lepreau Nuclear Generating Station, were reviewed and screened (see *Section 5.0* for further details) to determine if they require further detailed PSA analysis. The scope and extent to which external hazards are screened and evaluated have received regulatory acceptance.

1.2 Objectives

Consistent with the foregoing in *Section 1.0*, the objectives of a PSA are:

- To provide a systematic analysis, to give confidence that the design will align with fundamental safety objectives in International Atomic Energy Agency N-SF-1 [1] to protect people and the environment from harmful effects of ionizing radiation
- To provide confidence that small changes of conditions that may lead to a catastrophic increase in the severity of consequences will be prevented
- To provide assessment of the probabilities of occurrence for the severe core damage states, and assessments of the risks of major radioactive releases to the environment. Severe core damage is defined as a condition where there is extensive physical damage to multiple fuel channels leading to loss of core structural integrity. Risks of major radioactive releases could include small and/or large releases
- To provide site-specific assessments of the probabilities of occurrence, and the consequence of external hazards
- To identify plant vulnerabilities and systems for which design improvements or modifications to operational procedures could reduce the probability of severe accidents, or mitigate their consequences

1.2 Objectives, Continued

- To assess the adequacy of emergency operating procedures. PSA insights should be used as part of the system for maintaining the emergency operating procedures as these procedures are subject to improvement throughout a nuclear power plant lifetime
- To provide insights into the severe accident management program. Level 2 PSA can support severe accident management programs, i.e. the development, implementation, training and optimization of accident management strategies and measures
- To demonstrate that a balanced design has been achieved, which can be demonstrated if no particular feature or postulated initiating event make a disproportionately large or significant uncertain contribution to the overall plant risk, and the first two levels of defence-in-depth as per International Atomic Energy Agency INSAG-10 [2] bear the burden of ensuring nuclear safety.

Assessment of the adequacy of plant design and operation is achieved by identifying potential accident sequences that dominate nuclear safety risk and establishing which features of the plant contribute most to the dominant accident sequences. These plant features may be potential hardware failures, common-mode failures, human errors during testing and maintenance, or procedural inadequacies leading to human errors.

1.3 Scope

The integrated report provides a technical summary of all potential hazards that can contribute to damaging the reactor core or result in a large radiological release. The integrated report also includes sensitivity, uncertainty and importance analysis. This report evaluates the plant for the following scenarios:

- Potential core damage and subsequent releases from internal events occurring while the reactor is at power, i.e. it considers the challenges to reactor core control, fuel cooling and containment of radioactive material
- Potential core damage and subsequent releases from internal events occurring while the reactor is in a shutdown state including loss of outage heat sinks
- Potential severe core damage and subsequent releases from seismic events occurring while the reactor is at full power
- Potential severe core damage and subsequent release from internal fires occurring while the reactor is at full power
- Potential severe core damage and subsequent release from internal floods occurring while the reactor is at full power

1.3 Scope, Continued

All potential external hazards to which the Point Lepreau Nuclear Generating Station site may be susceptible have been evaluated based on screening criteria to determine if additional hazards should be included in the detailed analysis of PSA. In addition, evaluating the outcomes of state-of-the-art seismic hazard assessment, probabilistic tsunami hazard assessment and a high wind hazard assessment that was performed in response to the Canadian Nuclear Safety Commission Integrated Action Plan [4]. Further details are provided in *Section 5.0.*

Seismic events, internal fire, and internal flooding have not been evaluated for shutdown conditions for the reasons described below, as well as being quantitatively screened out following guidance from ASME/ANS RA-Sb-2013 [17]:

- A seismic PSA for shutdown conditions was not performed as the risk from a seismic event is similar if the plant is at-power or in outage; the accident progression is slower when the plant is in outage, giving more time for operator action; and the time at risk while the plant is in outage is small compared to the time the plant is at power. Seismic PSA for shutdown conditions was quantitatively screened out.
- An internal fire PSA for shutdown conditions has not been performed. The evolution of an accident for this scenario is also slower than when the reactor is at power and there is more time for operator actions to mitigate the event. Also, some of the equipment that operates at full power is shut down and does not form an ignition source. The plant also has hot work programs in place to limit the potential for fires and other risk control measures are in place for managing transient combustibles. Internal fire PSA for shutdown conditions was also quantitatively screened out.
- An internal flood PSA for shutdown conditions was not done as the overall risk of severe core damage due to flooding is low. The low risk of severe core damage due to flooding is due to the low initiating event frequency, the physical separation of the Group 1 and Group 2 systems and the separation of odd and even equipment. These factors are the same from at-power and outage operation. Internal flood PSA for shutdown conditions was also quantitatively screened out.

1.4 Organization of Summary Report

In addition to the general information presented in this introductory section, the summary report provides:

(a) A short description of the Point Lepreau Nuclear Generating Station (*Section 2.0*)
(b) A brief description of the enhancements made to Point Lepreau Nuclear Generating Station to deal with events and accidents beyond the original design basis (*Section 3.0*)
(c) A discussion of the results of updated external hazard assessments (*Section 4.0*)
(d) A high level overview of the other types of hazards that were considered as part of PSA and their screening criteria (*Section 5.0*)
(e) An overview of PSA methods and acceptance criteria (*Section 6.0*)
(f) A discussion of the main results from the PSA (*Section 7.0*)
(g) A description of emergency response capabilities should an unlikely nuclear accident occur (*Section 8.0*)
(h) The approach used to estimate public health risk in the event of a very unlikely severe accident (*Section 9.0*)

2.0 Plant Description

The Point Lepreau Nuclear Generating Station (PLNGS) is a CANDU-6 heavy water moderated, pressure tube reactor design with on-line fuelling capability. PLNGS is owned and operated by New Brunswick Power Corporation. The station was commissioned in 1982 and was placed into commercial operation in February of 1983.

The station is designed for commercial base load operation. It contains a turbine generator set delivering an electrical output of 705 MW(e) with steam supplied from a CANDU-PHW (pressurized heavy water) type nuclear power plant. Some electrical power is consumed to operate equipment within the station. A net output of 660 MW(e) is available to the NB Power electrical distribution grid.

The layout and design of the unit is similar to the Gentilly-2 unit constructed in Quebec, Wolsong-Units 1 to 4 in Korea, Embalse-1 in Argentina and, Cernavoda 1 and 2 in Romania.

The CANDU reactor uses heavy water as a moderator and as a coolant inside the heat transport system. The fuel is natural uranium supplied in the form of bundles loaded into and removed from the reactor during on-power operation. A closed loop heat transport system transfers the heat from the fuel to the boilers, producing light water steam in the secondary side of the boilers. The turbine cycle is similar to that used for other plants of this type.

2.1 Site Arrangement

The general location of the Point Lepreau Nuclear Generating Station site is shown in **Figure 1**.

2.2 Buildings and Structures

The station consists of the following buildings and structures:

- Reactor building (1)
- Service building (2)
- Turbine building (3)
- Auxiliary service building (5)
- Fresh water pump house (206)
- Salt water pump house (26)
- Switchyard
- Administration building (4)
- Solid radioactive waste management facility (not shown in Figure 2)
- High pressure emergency core cooling system building (7)
- Secondary control & emergency power building (6)
- Sewage treatment plant (200)
- Emergency filtered containment vent building (39)
- Standby generator 3 complex (14 to 19)
- Emergency mitigating equipment storage building (224)
- Fire truck building (42)
- Simulator, training, office and information complex (204)
- Supplemental office administration and projects building (203)

The site layout is shown in **Figure 2** (corresponding Building ID# above)

The reactor building contains the nuclear reactor and associated equipment including the boilers. Its outer structure forms a containment boundary designed to confine any accidental release of radioactivity within the building. The containment structure is a pre-stressed concrete building comprising three structural components: a base slab; a cylindrical wall; and a hemispherical dome. It is designed to contain an internal pressure of 124 kPa(g). An impermeable lining is provided to minimize leakage during potential overpressure transients. An inner dome at the top of the reactor building, together with the building perimeter wall, forms a storage tank that contains water for boiler make-up, the containment dousing system and the emergency core cooling system. The typical layout of the reactor building for a CANDU-6 plant is provided in **Figure 3**.

2.2 Buildings and Structures, Continued

The turbine building complex consists of a turbine hall, an auxiliary bay and a two story auxiliary service building. The main structure is approximately 96 m long, 61 m wide and 38 m high with respect to its base and 23 m above grade level. The turbine hall houses the turbine generator set, power distribution rooms and instrument air supply. A water treatment plant that produces demineralized water, which provides make-up to various systems, two standby diesel generators and auxiliary boiler are located in the auxiliary service building.

Pressure relief panels are provided to ensure that internal and external walls are not blown down in the event of a break in a pipe carrying high energy steam or water. Twenty-three (23) panels are located below the operating floor and face south. Forty-three (43) panels are located above the operating floor and are divided between the north, west and south directions.

Steam line of defense wall and doors are installed to minimize the potential for steam ingress into the service building should a main steam line failure occur in the turbine hall, which could adversely affect the main control room and emergency egress routes.

The service building is designed to accommodate two similar reactor units and contains service areas that would be common to both units, such as, main control room, change room, stores, workshops and laboratories, as well as areas that would be repeated at each unit. These latter areas contain equipment and systems directly associated with the operation of the reactor, such as spent fuel storage bays, spent fuel storage bay cooling and purification, shield cooling, moderator purification, emergency core cooling.

2.3 Systems and Functions

2.3.1 Reactor Core

The reactor comprises a cylindrical calandria vessel with 380 fuel channels and an array of reactivity control devices. The calandria vessel, which is filled with a heavy water moderator, is positioned so that the longitudinal axis of the cylinder is horizontal. The fuel channels penetrate the calandria horizontally and are arranged in a square lattice, when viewing the reactor from either end. The fuel channel consists of a calandria tube, which is part of the calandria vessel, a pressure tube, which contains the fuel, and the fuel itself. The space between the calandria tube and the pressure tube is known as the gas annulus. It is filled with flowing carbon dioxide gas and is maintained by spacers located along the length of the channel. This annulus gas system provides the capability to detect a small leak from a pressure tube so that operator action can be taken to shut down the plant and depressurize the system before a rupture occurs.

2.3.1 Reactor Core, Continued

End shields, which are an integral part of the calandria vessel, provide shielding at each end of the reactor to permit personnel access to the fuelling machine vaults when the reactor is shut down. The tube sheet that contains the heavy water is the moderator end shield, and the tube sheet that forms the outer face of the calandria is called the fuelling machine tube sheet. The fuel channels penetrate the end shields and are supported by them.

The calandria vessel is located inside a steel lined concrete reactor vault, which is filled with light water. The water provides additional shielding and also maintains the calandria shell at essentially constant temperature.

2.3.2 Reactor Process Systems

2.3.2.1 Primary Heat Transport System

The heat transport system circulates pressurized heavy water through the fuel channels to remove the heat produced in the fuel. This heat is transferred to ordinary light water in the boilers located inside the reactor building. The light water in the boilers, which is at a lower temperature and pressure, produces the steam to drive the turbine-generator. During shutdown periods, the shutdown cooling system is used in conjunction with the heat transport system for removing decay heat from the fuel.

The heat transport system includes the four circulating pumps, four reactor inlet headers and four reactor outlet headers, feeder pipes to and from each fuel channel, the primary side of the boilers, and a pressurizer. System pressure control is normally provided by the pressurizer. Inventory control is provided by the feed and bleed system. Water chemistry is closely controlled to limit the build-up of active corrosion products. Close attention is given to minimizing the escape of heavy water from the system and to the collection of heavy water liquid or vapour that does escape. Overpressure relief is provided by liquid relief valves.

In the event of a break in one loop of the primary heat transport system that discharges cooling water, an emergency core cooling system (see *Section 2.3.5.4* for further details) can inject water to maintain the fuel cool.

2.3.2.2 Moderator System

The moderator system is also in direct contact with the reactor. The moderator water inside the calandria vessel, surrounding the fuel channels, is essential to sustain the fission process in that it is responsible for slowing down the neutrons produced by fission to the thermal energy range in which further fissions will occur with a higher probability. Under normal conditions the moderator system removes the heat that's produced inside the calandria. Under emergency conditions it could function as a heat sink capable of limiting the extent of damage to the core.

A moderator cover gas system is provided in the pressure relief pipes above the moderator, to provide the calandria with normal pressure regulation, and to limit deuterium concentration in the calandria pressure relief pipes. The pressure of the cover gas also helps in ensuring sufficient cooling of the moderator water.

If a severe accident occurs, moderator make-up can be provided by an external portable water source via a hose connection point.

2.3.2.3 Shutdown Cooling System

The shutdown cooling system is connected to the Primary Heat Transport System and removes heat from the fuel under shutdown conditions. Under normal shutdown conditions operation of the shutdown cooling system allows maintenance to be performed on the heat transport pumps and boilers. Under abnormal, or accident conditions the shutdown cooling system can be used as a back-up heat sink.

2.3.2.4 Shield Cooling System

The end shields are horizontal, cylindrical shells enclosed at each end by tubesheets, and spanned horizontally by 380 lattice tubes. They contain biological shielding material in the form of carbon steel balls and demineralized light water. The function of the shield cooling system is to circulate, cool and purify the water used as a biological shield in the shield tank (calandria vault) and the two end-shields. The shield cooling system at Point Lepreau Nuclear Generating Station is directly connected to the calandria vault and provision is provided for overpressure relief during postulated accident conditions and for make-up from an external water source via a system referred to as the calandria vault make-up system. The shutdown cooling system comprises two sets of pumps and heat exchangers.

2.3.3 Plant Control

The Point Lepreau Nuclear Generating Station has a consistent performance record of outstanding electricity generation and safe operation. This record is attributable to good design and construction practices coupled with prudent operating strategies. Automated plant control is a key ingredient of this success.

This section describes the instrumentation and control philosophy, design and equipment for the Point Lepreau Nuclear Generating Station.

The plant is automated to require a minimum of operator actions during all phases of operation. A dual redundant computer system is central to the instrumentation and control systems. All major control loops use the two computers as direct digital controllers, giving a redundant and highly reliable system that is powerful and flexible. Conventional analog control instrumentation is used on smaller local loops.

The first principle of plant control is to provide safe and efficient operation of the plant, safeguarding worker and public health, and producing a secure return on the economic investment for the owner. This entails operation within specified design parameters and regulatory limits.

2.3.3.1 Two-Group Separation Philosophy

The Point Lepreau Nuclear Generating Station design uses group separation to minimize the possible consequences of events that could cause widespread damage, and to provide defence-in-depth. Each group contains equipment to shut down the reactor, remove decay heat, and monitor the reactor status. The Group 1 and Group 2 systems are physically separated. The safety system grouping is shown in **Table 1**.

2.3.3.2 Main Control Room

The main control room contains the unit control panels, station common systems and electrical services panels, an operator's desk with two printers, and a fuel handling machine control console.

To satisfy the operator's need for a pleasant working environment, the main control room is spacious enough to eliminate claustrophobic effects and to allow easy movement about the control panels.

The main control room instrumentation design and layout is based on the philosophy of having sufficient information displayed to allow the unit to be controlled safely from the main control room. To achieve this goal, all indications and controls essential for operation (startup, shutdown, and normal operation) are located on the main control room panels. Also located there are controls for any systems requiring attention within 15 minutes of an alarm occurrence. For systems not requiring attention within 15 minutes, local control is provided.

Most information is presented to the operator via the station computer system. However, sufficient conventional display, annunciation and indication of plant variables is included to allow the plant to be properly run with the reactor shut down and both computers out of service.

2.3.3.3 Secondary Control Area

If the main control room becomes uninhabitable or inoperable for any reason (e.g., due to smoke, seismic event, fire or toxic fumes), a secondary control area remote from the main control room is provided with sufficient display and control instrumentation to allow the plant to be shut down, monitored, and maintained in a safe shutdown condition including the assurance of adequate fuel cooling.

The original intent of the secondary control area was to cater for a catastrophic seismic event in which all of the main control room and its associated equipment become unavailable. Therefore, all of the equipment in and operated from, the secondary control area is seismically qualified. In addition, two separate seismically qualified routes (lights, anchored equipment, etc.) are available for control room operators to reach the secondary control area. In keeping with the two group approach, the secondary control area has all Group 2 equipment. It also contains seismically qualified controls for Emergency Core Cooling, a Group 1 system.

In addition, the secondary control area is permanently manned when the primary heat transport system is above 100ºC so that prompt action can be taken to control the reactor should the main control room become uninhabitable.

2.3.3.4 Overall Plant Computer Control

Digital computers are employed for station control, alarm annunciation and data display. Direct digital control is used for such functions as regulating reactor power, heat transport pressure and inventory, boiler pressure, boiler level, moderator temperature and fuelling machine operation. The system consists of two nearly identical independent digital computers: DCCX and DCCY. Each computer is capable of complete station control. In the event of a failure or stall of one computer, control is transferred to the other computer. As a result the dual computer system assures the very high reliability required for the station control.

All functions essential to the operation of the plant are incorporated in both computers. Typical duplicated functions are:

Reactor power control, including protective functions for stepback (fast reduction in power using mechanical control absorbers) and setback (slower reduction in power using mechanical control absorbers or liquid zone controllers for spatial control):

- Plant load control
- Boiler pressure control
- Boiler level control
- Heat transport pressure and inventory control
- Moderator temperature control
- Alarm annunciation
- Data display on monitors

Other functions, not essential to plant operation, are resident in one computer only. One such function is fuelling machine control.

2.3.4 Balance of Plant Process Systems

2.3.4.1 Steam Generators

The main role of the primary heat transport system is to transport the heat generated in the fuel channels to the steam generators (also referred to as boilers). The role of the steam generators is to transfer this heat and boil the light water on the secondary side. The steam generated is then used to drive the turbine generators to convert the thermal energy to electrical power. After passing through the turbine the steam condenses. The condensate is returned via the feedwater system to the steam generators to continue the process.

In the event that engineered normal or emergency water sources for maintaining steam generator level are not available, connection points have been provided to supply water to the steam generators from external portable water sources.

2.3.4.2 Steam System and Steam Relief

The key function of the steam system is to transport the steam produced in the boilers to the turbine where the thermal energy is converted into mechanical energy. The steam relief system protects the steam generators from overpressure and is also used for rapid cooling of the primary heat transport system when needed.

Four atmospheric steam discharge valves with a total capacity of ten percent of main steam flow are installed on the four main steam lines. Sixteen main steam safety valves with a total nameplate capacity of 115 percent of main steam flow are also installed on the main steam lines. Ten condenser steam discharge valves with a total capacity of 100 percent of main steam flow are connected to the condenser steam discharge lines that bypass the turbine. These valves function as:

(a) a poison-prevent turbine bypass system by dumping steam to the main condenser when the turbine is tripped
(b) boiler pressure control support

2.3.4.3 Feedwater System

The function of the feedwater system is to provide a continuous supply of feedwater to the boilers to maintain the desired water level in the steam generators. Steam output from the steam generators is transmitted to the turbine-generator set, is condensed with cool water from the condenser cooling water system, and that condensate is then returned to the steam generators via main feedwater pumps to be boiled again.

In the event that all main feedwater pumps are not available, the reactor power is reduced and feedwater is pumped from the deaerator to the boilers using the auxiliary electrical or steam-driven feedwater pumps.

2.3.4.4 Secondary Side Piping Leak Detection System

The function of the secondary side piping leak detection system is to provide enhanced protection to the main control room against the potential consequences of a pipeline break. This is done by monitoring sections of the main steam, feedwater and reheater drains piping for small leaks, and alerting station personnel before the leak can develop into an unstable piping failure.

2.3.5 Safety Systems

2.3.5.1 Design Philosophy

Special safety systems are incorporated into the plant to preserve, to the maximum extent practicable, the various barriers to the release of radioactive elements from the site in the case of postulated incidents in which normal plant control systems fail to provide sufficient response to deal with significant plant transients.

The safety systems perform three essential safety functions:

- To automatically detect the event and shutdown the reactor
- To keep the fuel cool
- To limit radioactive releases to the environment

2.3.5.2 Shutdown System 1

The purpose of shutdown system 1 is to rapidly and automatically shut the reactor down and so prevent failure of the primary heat transport system due to overpressure, excessive fuel temperature, or fuel break-up. It can maintain the reactor in a suitable subcritical state indefinitely, or for a period long enough to permit the protective shutdown system to be supplemented reliably. Shutdown system 1 consists of 28 cadmium shutoff rods and is the primary method of quickly terminating reactor operation when certain parameters enter an unacceptable range.

2.3.5.3 Shutdown System 2

Similar to shutdown system 1, shutdown system 2 also designed to rapidly and automatically shut the reactor down when certain events occur. Shutdown system 2 performs its function by injecting a solution of gadolinium nitrate under high pressure into the moderator to rapidly bring the reactor sub-critical and terminate reactor operation.

2.3.5.4 Emergency Core Cooling

The function of the emergency core cooling system is to provide cool light water to the primary heat transport system for fuel cooling and inventory makeup, if the primary heat transport system is breached creating a loss of coolant accident. During specific plant outage situations, the emergency core cooling system provides heat sink coverage on a manual initiation basis. The emergency core cooling system does not operate during normal plant operating conditions but is in a standby mode.

2.3.5.5 Containment Systems

Containment is the concrete building or shell that houses the reactor and other equipment that contain radioactive material. Its function is to prevent or limit the escape of radioactivity to the environment.

The containment building cannot be completely sealed during normal operation due to requirements to transfer process fluids, to provide building ventilation, and to provide for personnel and materials access for testing, maintenance, inspection, fuelling and operations support activities. Thus, a number of sub-systems are required to permit building access and automatic isolation of the building penetrations which service the above functions. These sub-systems include: an automatic isolation system, a dousing system, access airlocks, fuel transfer mechanism, atmospheric control panels and local air coolers. A simplified diagram of the containment envelope is provided in **Figure 4**.

The containment building performs a dual function:

- Protect the reactor and other equipment housed inside it from the external environment
- Protect the external environment (including the public) from radiation contained inside it

The external environment and public are protected by logic that automatically closes the containment isolation valves if reactor building pressure increases beyond a certain setpoint or if radiation is detected in the reactor building ventilation or vapour recovery ducting. Dousing and local air coolers serve as part of the containment pressure control during accident conditions.

During plant refurbishment, the pressure reducing capability of containment was enhanced through installation of an emergency filtered containment venting system that provides additional protection of structural integrity during a very unlikely severe accident. This system has special filters that allow the building to be depressurized while minimizing radioactive release. In addition, passive autocatalytic recombiners were installed to manage possible hydrogen production following an accident.

2.3.6 Safety Support Systems

2.3.6.1 Emergency Water Supply

The emergency water supply system ensures that there is sufficient water available to establish an adequate heat sink, for decay heat removal, independently of the normal cooling water systems. The system is seismically qualified to provide long term heat removal capability. The system consists of two electric motor-driven main pumps which supply water to the emergency water supply distribution system from an on-site reservoir.

A sub-system of emergency water supply known as the boiler make-up water system automatically injects water under gravity from the dousing tank to the boilers when certain conditions exist. Later, water can be supplied via emergency water supply pumps. Ensuring an adequate supply of boiler inventory provides assurance that thermosyphoning will remain effective for the primary heat transport loop whose integrity remains intact.

The emergency water supply pumps are located in a pump house situated approximately 210 m from the reactor building. They take suction from the on-site fresh water reservoir, which is separate and remote from the intake structure for normal cooling water supply, with an emergency connection from the fire protection system and an additional make-up connection from the Hanson Stream reservoir connected into the pump suction pit.

The pumps are normally powered from the emergency power supply system, which is comprised of two fixed diesel generator sets. However, if emergency power supply is not available, the pumps can also be powered via switching from a portable diesel generator that can be deployed on demand. If the emergency water supply pumps are not available for any reason, a connection point is provided in the pump house to supply water from a portable diesel pump that can also be deployed on demand.

2.3.6.2 Emergency Power Supply

The emergency power supply system provides an alternative source of electrical power for certain safety and safety support systems and instrumentation when the normal source of supply is unavailable.

The emergency power supply system comprises two redundant, seismically qualified, and functionally independent power supply trains. Each train consists of a 4.16 kV diesel generator set and associated switchgear as required to distribute high voltage to the appropriate loads.

In the event that the emergency power supply diesel generators are not available for any reason, connection points have been installed to provide power from a portable diesel generator unit that can be deployed on demand. The portable unit can provide power to essential motorized valves and ensure that the plant can be cooled and controlled in a stable state.

2.3.7 Other Support Systems

2.3.7.1 Electrical Power Systems

The electrical system for Point Lepreau Nuclear Generating Station is similar to those found in any large power station, with modifications introduced to satisfy the increased reliability requirements for nuclear power systems, including the need to support equipment for decay heat removal after station shutdown. This results in a more selective bus arrangement and more standby and redundant equipment. There are four distinct classes of power (Classes IV, III, II and I) each with a higher degree of reliability, and emergency power supply (see *Section 2.3.6.2*).

Class IV power is the main site electrical power supplied from a combination of the provincial electrical grid and the station generating unit transformers; class III power is the backup supply to class IV and includes two standby generators and an installed spare; class II is an alternating current power system to supply control and monitoring systems and is uninterruptible as it is supplied by class I power via inverters; class I is a uninterruptible direct current power system to supply control and monitoring system since it is a battery backup supplies.

The two Class III standby generators located in the auxiliary service building are also supplied with fire water in the event that normal cooling sources are lost for any reason. The installed spare standby generator (i.e. standby generator 3) is located outside of the auxiliary service building in its own complex.

2.3.7.2 Service Water Systems

Service water systems provide cooling water for various loads. The service water systems for Point Lepreau Nuclear Generating Station consist of the following:

- Condenser circulating water system. This system supplies the sea cooling water required by the steam turbine condenser (see *Section 2.3.4.3*). The system is supplied with traveling screens and a screenwash system in its pump house to ensure that no large debris causes a blockage at the intake. In the event of a break of expansion joints for this system in the turbine hall, flooding logic will activate to isolate the condenser cooling water system to prevent further sea water ingress.

- Raw service water system. The raw service water system supplies sea water to the recirculating cooling water heat exchangers located in the basement of the turbine hall. In addition, it supplies water to other heat exchangers which do not have a credited safety function in the PSA (lube oil heat exchangers, seal oil heat exchangers, air extraction system heat exchangers, turbine auxiliary recirculating cooling water heat exchangers, and the boiler blowdown mixing chamber). Any pressure boundary failures of the raw service water system will also activate the turbine building flooding logic to isolate the building from further sea water ingress.

- Recirculating cooling water system. The recirculating cooling water system is a closed loop of treated demineralized water supplying cooling to all equipment for which salt water is unsuitable.

- Turbine auxiliaries recirculated cooling water system. The turbine auxiliary recirculating cooling water system is also a closed loop, treated, demineralized water system. The system supplies cooling to various turbine related equipment which cannot tolerate cooling by either sea water or the higher pressure of the main recirculating cooling water system. These cooling loads include the hydrogen, stator water and fire resistant fluid coolers. In addition, the turbine auxiliary recirculating cooling water system cools the thrust bearings of the main condensate pumps, and various bearings and glands of the high pressure heater drains pumps and reheater drains pumps. The turbine auxiliaries recirculated cooling water system is not credited as a safety function in the PSA.

2.3.7.2 Service Water Systems, Continued

- Instrument air compressor cooling system. The instrument air compressor cooling system is a closed loop system. Its purpose is to supply low-pressure cooling water to the instrument air compressor coolers. The instrument air compressor cooling system is designed to transfer 0.4 MW of heat from the instrument air compressor coolant heat exchangers during normal operation. Heat is removed by the instrument air compressor cooling system to the recirculating cooling water loop via heat exchangers.

- Demineralized water system. This system provides a source of demineralized water through treatment of fresh water drawn from the Hanson Stream reservoir. Water provided from this system has a controlled chemical composition. The major usage is loads which are sensitive to corrosion.

- Domestic water system. This system is designed to supply hot and cold treated water to the plant. Typically, it supplies loads in the plant, administrative building, the simulator, training, office and information complex building, construction stores, washrooms, laundry, emergency eyewash stations and safety showers.

2.3.7.3 Instrument Air System

The instrument air supply is a support system providing compressed air. This compressed air is used for various plant activities including operating valves and inflating airlock seals. Certain key loads are supplied by compressed gas from bottles, to ensure operability in the event of failure of the normal supply.

2.3.8 Spent Fuel Bays

The spent fuel bays are located adjacent to the reactor building, to minimize the distance of spent fuel transfer. Cranes are used in both spent fuel bays for movement of fuel and access to certain portions of the reception bay can be accomplished by the service building hall crane (100 ton capacity).
The spent fuel bay complex is divided into two separate bays as follows:

- Reception bay (including the flask loading area)
- Main storage bay

These areas are entirely separate, with an underwater flow restrictor and with partition walls to provide atmospheric separation.

2.3.8 Spent Fuel Bays, Continued

The storage area of the bay has sufficient capacity for 10 years accumulation of spent fuel and for temporary storage of one full reactor core of the fuel. Additional spent fuel storage, beyond the ten year capacity, has been provided in dry concrete canisters in Phase II of the Solid Radiation Waste Management Facility.

The reception bay and flask loading area is located at the end of the main storage bay in the crane hall portion of the service building. Spent fuel is received via the spent fuel transfer tunnel in the reception bay. Here any failed fuel, which has been canned in the reactor building, is held in temporary storage. All other fuel is transferred directly to the main bay for storage. The flask loading area is provided to allow underwater loading of spent fuel into shipping flasks for transfer to other sites.

The spent fuel bay is a reinforced concrete tank. The inner surface of the fuel storage bay walls is lined with a white fibreglass reinforced epoxy coating, except for the floor and 0.5 m up the walls, which are covered with a stainless steel liner. Underdrainage is provided for the bay.

There are two essentially separate, but interconnectable, cooling and purification systems: one system provided for the main storage bay and the other for the spent fuel discharge and reception bays. The storage bay system is designed primarily to remove decay heat, whereas the removal of radioactivity dictates the flows in the system for the other bays. The design intent is to provide operational flexibility to meet varied purification demands without unnecessary duplication of equipment.

Decay heat from the spent fuel in the storage bay is removed by recirculating the bay water through a heat exchanger. The flow from the bay originates from skimmers at the bay water surface. A fraction of the flow is passed through a filter and then passed through ion exchangers.

The flow from the fuel discharge and reception bays, which also originates from skimmers, is normally passed through a heat exchanger, purification flow is passed through a filter, and then an ion exchanger before being returned to the flask filling area of the reception bay. The design intent is to maintain a positive flow of water into the fuel discharge bay.

Fuel bay outlets are located near the water surface to prevent draining of the bay in the event of a pipe rupture. Piping from fuel bay inlets near the bottom of the bays is routed directly up above the bay surface outside the bays and is equipped with siphon breaks to prevent siphoning of the bay water should a pipe rupture occur.

3.0 Dealing With Beyond Design Basis Accidents

3.1 Introduction

Design basis accidents are events that are not expected to occur during the lifetime of Point Lepreau Nuclear Generating Station but, in accordance with the principle of defence-in-depth, are considered in the original design of the plant. Beyond design basis accidents are those events with low probabilities of expected occurrence, which are more severe than design basis accidents and could lead to severe accidents involving significant core damage, challenges to the integrity of the containment barrier, and, eventually, to the release of radioactive material. Beyond design basis accidents were only considered in a very limited fashion in the original design and safety basis of the plant through analytical tools referred to as Safety Design Matrices, but as lessons learned from world nuclear events have been considered and addressed, the design of the plant and its safety basis has evolved to demonstrate capability to withstand a much broader range of beyond design basis accidents. As such, probabilistic safety assessment evaluates the likelihood and consequences of both design basis and beyond design basis accidents.

In response to the accident at the Fukushima Daiichi power plant in Honshu, Japan, caused by the March 11, 2011, Tohoku, Japan, earthquake and subsequent tsunami, the Canadian Nuclear Safety Commission established a task force to review safety of nuclear power plants in Canada and their capability to withstand events beyond the design basis. A task force report [3] provided thirteen recommendations to further enhance safety of Canadian nuclear power plants, with a particular emphasis on:

(a) The capability of Canadian plants to withstand external hazards comparable to those that triggered the Fukushima Daiichi nuclear accident
(b) Emergency preparedness and response in Canada
(c) The effectiveness of the Canadian Nuclear Safety Commission regulatory framework
(d) International collaboration

An increased focus on capability, analysis and accident management to deal with hazards and events well beyond the design basis has developed nationally and internationally, and improvements are being made to enhance the safety of nuclear facilities. This has prompted NB Power to examine:

- The design approach and modifications that have been implemented at Point Lepreau to mitigate beyond design basis accident scenarios
- External hazard assessments which have been performed for the hazards to which the site is susceptible
- Relevant accident analysis that has been performed

3.2 Principles for Beyond Design Basis Events

A set of principles has been developed and agreed to by all Canadian utilities to guide their response to the Fukushima Daiichi accident and to reassure the public. The objective is to practically eliminate the potential for societal disruption due to a nuclear incident by maintaining multiple and flexible barriers to severe event progression through application of the following principles:

- Actions and defenses will focus on stopping accident progression prior to a severe accident
- Multiple barriers to event progression and multiple means to supply water or electricity will be used to ensure adequate defence
- Methods and actions to initiate heat transport system cooldown and maintain fuel cooling will be a primary and early priority
- Actions to maintain containment integrity will be utilized to minimize radioactive releases
- Containment venting will be controlled through a filtered system
- Necessary systems, structures and components will be confirmed to survive rare yet credible conditions for external hazards
- Irradiated fuel bay water levels will be maintained sufficiently above the top of the fuel to mitigate high radiation fields, hydrogen production, and fuel damage
- Emergency mitigating equipment will be robust, readily available, easily deployable within required timeframes, and have adequate redundancy
- Canadian utilities will utilize a common philosophy for the prevention of a beyond design basis accident

The Canadian industry responded with diligence and urgency to understand and address the lessons learned from the events of Fukushima Daiichi. The response has quickly provided additional real physical barriers to a very low probability, high consequence event such as seen at Fukushima Daiichi, thereby reducing the risk of adverse effects to the public and the environment.

These principles are voluntary but nevertheless reflect the genuine aspiration of the participants to apply them, to make every effort to achieve the overall objective, and to be held accountable for decisions in this regard. NB Power has committed to its Canadian utility peers to abide by the above principles. Modifications to the plant that cater to beyond design basis accident or severe accident conditions have been implemented with these principles in mind.

3.3 Design Philosophy

The standard Point Lepreau Nuclear Generating Station processes related to plant modifications have been developed to stipulate a high degree of rigour to ensure consistency with the design basis of the station. When developing modifications related to beyond design basis accident conditions, alternate strategies may be appropriate in some cases, provided that the original design basis of the station is preserved.

The overriding objective is to ensure that modifications undertaken to manage and/or mitigate beyond design basis accident conditions will:

- Ensure that station functionality is not compromised under design basis conditions
- Deliver the required functionality with high confidence under the anticipated beyond design basis accident conditions.

In general, this functionality will prevent or mitigate significant adverse consequences, such as fuel and/or core damage and/or significant radiological releases.

As the overriding objective suggests, NB Power has adopted a balanced approach to managing the consequences of low frequency, high impact event sequences that are not considered in, and lie outside of, the design basis of the station. As a result of the foregoing, NB Power has installed a number of complementary design features to ensure that the above objective can be met and so that a flexible response capability is achieved and maintained to prevent and/or mitigate severe consequences of a postulated nuclear accident.

3.4 Complementary Design Features

The following is a list of complementary design features added to the Point Lepreau Nuclear Generating Station design since 2008 to deal with a potential beyond design basis accident and/or severe accident:

- Emergency filtered containment venting system
- Calandria vault make-up system from an external water source
- Passive autocatalytic hydrogen recombiners
- Installation of a severe accident sampling and monitoring system
- Seismic upgrades to key equipment to improve the robustness of the plant to withstand earthquakes larger than the original design
- Installation of various connection points to allow water to be admitted from external pumped water sources (i.e. towable diesel-powered water pump or fire trucks)
- Installation of various connection points to allow repowering critical electrical buses in the event of a total station blackout (i.e. via towable diesel-powered electrical generators)
- Procurement of portable water pump and portable diesel generators
- Installation of an on-site diesel fuel storage and dispensing system for the portable equipment
- Procurement of auxiliary equipment such as hoses, fuel transfer trailer, and a debris clearing vehicle to ensure a clear path for deployment of portable pumps and generators
- Improved water level measurement and management, and pressure monitoring, in the reactor building
- Installation of a submarine-style door over the inside penetration of the personnel airlock to allow more water to be added to key systems to restore or maintain heat sinks

The towable pumps and generators, and any supporting auxiliary equipment, is referred to as “emergency mitigating equipment”. NB Power performs routine drills to ensure that emergency mitigating equipment can be deployed within the timeframe required to terminate accident progression or to mitigate any further consequences.

4.0 External Hazard Assessments

4.1 Introduction

In accordance with *Section 3.0* above, lessons learned from the accident at Fukushima Daiichi have prompted regulatory agencies around the world to require nuclear operators to re-examine external hazards to which their sites may be susceptible. In Canada, these requirements and expectations have been documented in the Canadian Nuclear Safety Commission Integrated Action Plan [4] on the lessons learned from the Fukushima Daiichi accident, which has been enacted on utilities through various Fukushima action items. The Fukushima action items (FAI) that relate to re-evaluating external hazards include FAI 2.1.1 to re-evaluate the hazards and FAI 2.1.2 to evaluate the impact on the design protection of the plant and to establish plans and schedules, where necessary, to close any gaps. The external hazards to which Point Lepreau may be most susceptible, and for which the Fukushima Action Plan specifically required reevaluation, are:

- Seismic hazard (e.g., earthquakes)
- High wind hazard (e.g., hurricanes, extratropical cyclones, etc.)
- Tsunami hazard.

These are discussed further in the sections below.

4.2 Seismic Hazard Assessment

4.2.1 Introduction

The seismic hazard characterized for the Point Lepreau site is based on numerous geologic and seismic hazard studies that have been conducted in the site region since the previous seismic hazard analyses for the site were performed in the 1970s and 1980s. The approach to this assessment was to conduct a site-specific probabilistic seismic hazard assessment to characterize ground motion hazard at the site in terms of peak horizontal ground acceleration and response spectral accelerations at selected structural response frequencies (periods) and for a range of probabilities of exceedance appropriate for evaluating seismic safety during the design life of the Point Lepreau Nuclear Generating Station.

The probabilistic seismic hazard assessment involved compilation of an earthquake catalog for the region surrounding the site and identification and characterization of regional seismic source zones and local seismic sources. The results of paleoseismic studies in the region were incorporated in the seismic source characterization. Ground motion models applicable to the hard rock conditions of southeastern Canada were selected using the most recent published

4.2.1 Introduction, Continued

literature and through discussions with experts. Probabilistic seismic hazard analyses were conducted for peak ground acceleration and response spectral accelerations (Sa) covering the frequency range of importance to nuclear power plant design and performance.

4.2.2 Geological and Tectonic Setting

Understanding the geology, structure, tectonic setting and seismicity of a region facilitates the identification of potential seismic sources and provides a context for developing tectonic models of crustal deformation that can be used to characterize the seismic potential of individual geologic structures and source zones. The Point Lepreau Nuclear Generating Station site is located in the Northern Appalachian Orogen, which extends from the Gulf of St. Lawrence to the Atlantic Ocean, and is an area that has experienced a long and complex geologic and tectonic history.

4.2.3 Seismicity

An earthquake catalog of seismicity from 1568 to 2011 for the region surrounding Point Lepreau Nuclear Generating Station was developed for this study. The primary source of data for the project catalog is the Central and Eastern United States Seismic Source Characterization for Nuclear Facilities Project catalog [5] that includes earthquakes from 1568 through the end of 2008. The catalog is appropriate to use for this project because it merged all the relevant continental, regional, and local catalogs for instrumental and historical earthquakes, and was compiled for a Senior Seismic Hazard Analysis Committee Level 3 study [34]. Preparation of the catalog involved extensive research of literature on specific earthquakes, use of uniform moment magnitude that is consistent with ground motion models, and formal treatment of uncertainties in estimates of moment magnitude.

To the west-southwest of the Point Lepreau site, an increased level of historical seismicity has been recognized in the area of Passamaquoddy Bay, which is located approximately 25-30 km southwest of the site. The project earthquake catalog included 33 earthquakes within this area. The largest earthquakes that have occurred in the Passamaquoddy Bay area are the October 22, 1869, magnitude 5.47 earthquake and the March 21, 1904, magnitude 5.73 Eastport earthquake [6]. The 1869 event was located approximately 61 km west-southwest of the site based on felt intensities. This type of information provides a valuable input to the seismic hazard assessment modeling.

4.2.4 Paleoseismicity

Because the record of historical and instrumental seismicity only represents several hundred years of earthquake history in the region, one part of the new methodology for the updated hazard assessment included a "paleoseismology" study. This involved field work by recognized experts to identify evidence of large earthquakes that may have occurred since the ice age and how long ago that may have occurred. There is no observable evidence prior to the ice age since glaciers scoured the earth and erased any such evidence.

The field work identified evidence of three large earthquakes in the past that have affected the Point Lepreau region. Expert interpretation is that these earthquakes have occurred about 1,000, 4,000, and 12,000 years ago in the Passamaquoddy Bay area, centered near the epicenter of the 1904 event. Based on this information, it was estimated that earthquakes occurring in the Passamaquoddy Bay region as a result of the Oak Bay fault could be a magnitude 6.0 earthquake every 1000 years or so; a magnitude 6.5 event every 5000 years or so; and, a magnitude 7.0 event every 10,000 years or so.

This information was used to modify the seismic hazard and resulted in an increase of the hazard estimates for very rare, large earthquakes. The Point Lepreau Nuclear Generating Station design basis includes a magnitude 6.0 earthquake occurring about 20 kms from the plant once every 1000 years or so. The Passamoquoddy Bay area is 25-30 kms southwest of Point Lepreau Nuclear Generating Station, therefore, it should be expected that the original design basis for Point Lepreau Nuclear Generating Station is appropriate. However, the consequence of locating evidence of even larger earthquakes within the study region has modified our understanding of larger earthquakes that could occur less frequently and which are considered beyond the design basis of the plant.

4.2.5 Results

A summary of the results of the comprehensive probabilistic seismic hazard assessment was made available to the public in December of 2014 on the NB Power corporate website in parallel with it undergoing a third party expert review. As this study was to lay the foundation for performing a more detailed probabilistic safety assessment, hazard curves were presented for both the mean and median values and for other percentiles. The study identified the following:

Design basis - When comparing the hazard at a 1000 year return period to our design, the response spectra was significantly lower than the design spectra at frequencies lower than 10 Hz. That is to say it is bounded by the existing design, indicating that design margins have increased in the area of interest. The design spectra was however slightly exceeded at higher frequencies, but based on industry knowledge, high frequency aspects of an earthquake do not damage plant structures and equipment because their natural frequencies are lower, tending to be more in the range of 2-8 Hz and 1-10 Hz respectively.

4.2.5 Results, Continued

Beyond design basis - Although the hazard assessment showed that the earthquake magnitudes for more frequent earthquakes that might occur over the lifetime of the Station is lower than previously predicted, the magnitudes of very rare earthquakes that are unlikely to occur over the lifetime of the plant are larger than historically regarded as credible. To fully assess the potential implications of these larger earthquakes, NB Power committed to the Canadian Nuclear Safety Commission to perform a full seismic PSA.

Third party experts have completed their review of the Point Lepreau Nuclear Generating Station seismic hazard assessment, which resulted in a slight reduction of the overall hazard as reported in 2014, and the final hazard assessment was submitted to the Canadian Nuclear Safety Commission at the end of June 2015. Seismic experts at Natural Resources Canada have completed their review and the Canadian Nuclear Safety Commission has accepted the seismic hazard assessment for use at Point Lepreau Nuclear Generating Station.

Table 2 provides the horizontal uniform hazard response spectra at various return periods from the hazard assessment. **Table 3** provides a comparison to previous studies. **Figure 5** provides a graphical representation of **Table 2**, and **Figure 6** provides a graphical representation of the seismic hazard for various percentiles expressed as the annual frequency of exceedance (inverse of return period) versus the magnitude of earthquake.

To provide perspective on how the new hazard assessment compares to the existing design basis of Point Lepreau Nuclear Generating Station, **Figure 7** provides an overlay of the 1,000 year curves. Experts and experience have indicated that earthquake frequencies above 10 Hertz (number of vibrational cycles per second) do not typically cause substantial damage to structures and equipment of nuclear power plants because their natural frequencies tend to be more in the range of, respectively, 2-8 Hertz (Hz) and 1-10 Hz (see Annex B.6 of [37] for further details). An exceedance above 10 Hz for the mean uniform hazard response spectra shown in **Figure 7** is not an issue for Point Lepreau Nuclear Generating Station in terms of existing plant design. In the vibrational frequency range that might cause damage to most structures and equipment (i.e. < 10 Hz or so), the new updated hazard assessment shows that the hazard is lower. In addition since the uniform hazard response spectra is estimated for hard rock condition, it is expected that if a seismic site response analysis (similar to that performed in *Section 4.2.6*) is also performed for an earthquake with a 1,000 year return period, the high frequency content of the hazard spectra will be even lower. This is positive from a safety perspective as the existing Point Lepreau Nuclear Generating Station design bounds the new hazard curve in the frequency range of most interest.

4.2.6 Seismic Site Response Analysis

During the course of the seismic hazard assessment work and evaluating its implications, it was realized by experts that the seismic hazard assessment results provided in **Table 2** and **Table 3**, and in **Figure 5** and **Figure 6**, represent the seismic vibrations felt in the hard rock well beneath the plant whereas it is of more interest to evaluate seismic risk by considering what seismic vibrations the buildings will actually "feel". Therefore, it was deemed appropriate to perform additional work to propagate the seismic vibrations upwards into the foundations of the buildings (called foundation input response spectra or FIRS) and then further upwards into the buildings at different floor elevations (called floor response spectra or FRS).

The additional study identified that the varying rock and soil layers between the competent rock beneath the plant and the building foundations result in an attenuation or "dampening" effect particularly for seismic vibrations in the frequency region of 8 Hz and greater (see **Figure 8**) and results in a mean peak ground acceleration of 0.344g that the buildings will "feel". **Figure 10** also shows the corresponding reduction in the site seismic hazard curve.

Since we are interested in beyond design basis earthquakes for seismic PSA, in accordance with industry practice and guidelines, only the seismic vibrations from an earthquake with a return period of 10,000 years are propagated upwards into the buildings. The seismic response predicted to be felt at the foundations of buildings (at elevation 25 feet above mean sea level) is shown in **Figure 9**, and demonstrated to NB Power that earlier margin assessments would need to be modified since the new hazard exceeded the hazard curves used in those earlier margin assessments. The Canadian Nuclear Safety Commission was formally informed of that fact and that safety objectives and methodology may need to be reconsidered. The margin assessment work is discussed further in *Sections 6.4* and 7.0.

Following a similar approach to the site seismic response analysis to evaluate the hazard felt at the foundations of buildings, it would not be appropriate to apply the hazard curve from **Figure 6** in further PSA evaluations since it represents the vibrations well below the plant. Therefore, revised seismic hazard curves for use in seismic PSA were prepared and are presented in **Figure 11**.

4.3 High Wind Assessment

4.3.1 Introduction

Note that in the context of high wind assessment described below, the word "missile" refers to an object (e.g. yard debris) that could be picked up and thrown by the wind.

The purpose of the high wind hazard assessment is to develop and document high wind hazards and fragility functions for structures, systems, and components at Point Lepreau Nuclear Generating Station. The work is divided into four volumes to document the information. The work uses a systematic, documented process that follows ASME/ANS RA-Sa-2009 [7] and United States Nuclear Regulatory Commission Regulatory Guide 1.200 [8]. In summary, the four volumes include:

1. Volume I presents an overview of the calculation organization and walkdown procedures, as well as the screening of structures, systems and components for inclusion in the wind pressure and missile fragility analyses. This screening uses information collected via the plant walkdown as well as plant documents and drawings.

2. Volume II is divided into two sub-volumes:
   (a) Volume IIA documents the tornado hazard analysis for the Point Lepreau Nuclear Generating Station site. This volume serves as input to the tornado missile plant model
   (b) Volume IIB documents the high wind hazard analysis

3. Volume III documents the three-dimensional tornado missile model of the plant that was built to produce the missile fragilities for key structures, systems and components. This volume also documents results of the missile source survey portion of the site walkdown and information related to the tornado missile modeling of the structures, systems and component information gathered during the site walkdown.

4. Volume IV documents the development of wind pressure fragilities for the buildings that house the safety-related equipment.

4.3.2 Methodology and Results

4.3.2.1 Walkdown

A site walkdown of the Point Lepreau Nuclear Generating Station site was conducted between December 11 and December 13, 2013 for the purposes of observing and documenting the structures, systems and components, as well as surveying and documenting the potential sources of wind-borne missiles. In total, 109 locations were considered in the walkdown and the majority of these locations were included in the tornado missile model using a volume approach.

4.3.2.1.1 Screening for Inclusion in Missile Fragility Analysis

In general, all of the targets are included in the missile fragility analysis unless it can be shown that there is no credible missile path to the target. It was concluded that there is no credible missile path when the structure, system or component under consideration is:

- Located below local grade (no risk from horizontal missiles) and located more than 50 feet (15 m) horizontally from any unprotected openings in the concrete slab floor above
- Located below grade where the only available missile paths are through openings protected by steel plate and which are further protected from vertical missiles by floor slabs of upper floors
- Protected by at least 1 foot (300 mm) of concrete or 1 inch (25 mm) of steel [9]
- Located below local grade (no risk from horizontal missiles), protected by steel grating overhead, and located at least 50 feet (15 m) from exterior missile sources
- Located below local grade in 3 directions, below multiple floor slabs, and more than 100' (30 m) from external missile sources (in the single above local grade direction)

4.3.2.1.2 Screening for Inclusion in Wind Pressure Fragility Analysis

A list of buildings and individual targets to be considered in the wind pressure fragility analysis was also developed. The process included:

1. Identifying structures housing safety-related targets
2. Identifying exterior safety related systems that may be exposed to direct wind loading
3. Identifying other structures in the proximity of the target that could fail and fall on to the target.

4.3.2.1.2 Screening for Inclusion in Wind Pressure Fragility Analysis, Continued

The complete list of targets and buildings identified for consideration in the wind pressure fragility analysis was then reviewed to determine whether the targets and buildings identified were vulnerable to failure by wind pressure. The following reasons were established as justifications for screening building and/or individual targets from the wind pressure fragility analysis:

- Building designed and constructed with walls and roof composed of a minimum of 1′ (300 mm) of reinforced concrete;
- Large water and fuel storage tanks are assumed to be not susceptible to failure from wind loading; and,
- Wind speed required to develop a full plastic moment in exhaust stacks shown to be greater than 418 km/h (the windspeed corresponding to the highest fragility calculation point).

4.3.2.2 Tornado Hazard Analysis

The tornado risk analysis methodology used a statistical approach that considers both broad regions and small areas around the plant. A basic subregion data set for the Point Lepreau site was identified and analyzed. Tornado hazard curves were developed using a code called TORRISK. TORRISK produces tornado hazard curves distinct from the missile risk analysis features of the tornado missile code (TORMIS). The TORRISK hazard curves provide control points to ensure that the tornado missile simulations track the site-specific hazard curve developed for Point Lepreau Nuclear Generating Station.

A homogenous tornado subregion around Point Lepreau Nuclear Generating Station was identified through statistical analysis of the Climat-Quebec (Que) tornado data set for Quebec (1985 – 2013), Atlantic Region Database of Verified Tornadoes (Atl) for New Brunswick, Newfoundland and Labrador, Nova Scotia, and Prince Edward Island (1954 – 2007), and the US National Weather Service (NWS) Storm Prediction Center tornado data set (1950 – 2012). The Que database did not include tornado length, width, or direction information; however, the Atl data did include such information for a few tornadoes. Due to the limited extent of the Que and Atl data, the development of a Point Lepreau Nuclear Generating Station subregion included US land area to develop sufficient inputs needed for tornado windspeed risk analysis. The subregion includes areas of high tornado risk within a broad area. The subregion contains 397,949 sq km (153,649 sq mi) of land and 424 tornado segments.

4.3.2.2 Tornado Hazard Analysis, Continued

Tornado strike definition on the Point Lepreau Nuclear Generating Station tornado hazard curves were applied as follows:

(a) A "point" strike curve, which assumes that the target is a geometric point in which a tornado strike corresponds to that point experiencing the specific wind speed. For example, with EF-Scale winds, the probability of a small target or point experiencing 225 km/h (140 mph) peak gust tornadic winds at Point Lepreau Nuclear Generating Station is about one event in 2,197,802 years.

(b) A union curve corresponding to an area target that envelops the modeled safety related targets at Point Lepreau Nuclear Generating Station. This envelope has 188,468 sq meters (2,028,715 sq ft). The probability that any ("union of all points") location in this envelope experiences 225 km/h (140 mph) wind speeds is about one event in 316,456 years. This risk is about 7 times greater than a single point target and it depends on the shape, orientation, and area of the plant envelope.

The point hazard curves at various percentiles for tornados are provided in Figure 13.

4.3.2.3 Non-Tornado and Straight-Line Wind Hazard Analysis

Three types of non-tornado extreme winds have been analyzed for the Point Lepreau Nuclear Generating Station site:

1. Thunderstorm Winds
2. Non-Thunderstorm Winds (Extratropical Storms)
3. Hurricanes

Thunderstorm and extratropical storms are different meteorological phenomena and research has shown that they generally have distinct distributions and that the most accurate method to develop extreme wind frequencies is by separate analysis of each.

4.3.2.3.1 Straight Winds

Straight winds include thunderstorm and extratropical storm winds. Wind data from four airport stations in New Brunswick and Nova Scotia were separated into thunderstorm and non-thunderstorm data sets and used to develop separate extreme value distributions for each storm type. The thunderstorm wind speed hazard curves were developed using a stochastic modeling approach where the maximum gust wind speed recorded on every thunderday was used to develop a distribution of thunderstorm wind gusts given the occurrence of a thunderday. The thunderday extremes were developed by combining the conditional distribution of thunderstorm maxima with a Poisson arrival rate model. The annual extratropical storm winds were obtained using the method of independent storms where all independent peak gust wind speeds that exceeded a 60 km/h threshold were used to define the distribution of maximum extratropical storm wind gusts given the occurrence of an extratropical storm.

The separate distributions were then combined as statistically independent processes to arrive at one final straight wind hazard model. Estimates of uncertainties associated with local terrain effects, anemometer response characteristics, height corrections, errors in the estimates of the parameters of the extreme value distributions and an overall modeling error, were combined with the best estimate models to develop a family of wind hazard curves. The final family of straight wind hazard curves, corrected for height and terrain, is given in **Figure 14**.

4.3.2.3.2 Hurricane Winds

The hurricane wind speed hazard curves were developed using a hurricane simulation model. The model used in the study is a slight variation of that used in to develop the ASCE 7-10 [10] hurricane wind speed contours. This slight variation of the model was used to develop the wind hazard curves given NUREG/CR-7005 [11]. A 1,300,000 year simulation was performed for Point Lepreau Nuclear Generating Station. Hurricane wind speeds for rarer events (i.e. less than 10^{-6}/yr) were obtained by extrapolating the results from the simulation. **Figure 15** shows the hurricane hazard curves. The hurricane winds contribute little to the overall wind hazard at Point Lepreau Nuclear Generating Station.

4.3.2.3.3 All Winds Combined

Straight winds and tornadic wind hazard curves were combined using statistical independence. The combined curves from all wind hazards are shown in **Figure 16**. Extratropical winds dominate the straight line winds. Extratropical winds dominate the wind speed exceedance risk until about 300 km/h at which point tornadoes begin to dominate. At 332 km/h, tornadoes contribute 61% of the exceedance frequency.

4.3.2.4 Missile Fragility Analysis

The purpose of the missile analysis is to develop the necessary inputs for analyzing safety-related structures, systems, and components, develop a time-dependent plant-specific missile population, and using these inputs to produce missile fragilities for the identified targets using the tornado missile methodology. The inputs developed for these calculations include documentation of the location, dimensions, characteristics, and exposure to potential wind-borne missiles for each of the identified structures, systems and components.

The tornado missile analysis results have been completed in accordance with United States Nuclear Regulatory Commission requirements [35 & 36]. A total of 23.808 billion tornado missile simulations have been performed for Point Lepreau Nuclear Generating Station. Each simulation consists of sampling and flying a missile for a simulated tornado strike on the plant. A total of 3,968 million tornado strikes on the plant were simulated as part of the tornado missile analysis with 6,000 missiles sampled per tornado strike. The missile impact fragilities are based on simulated tornado strikes on the plant and simulated tornado wind fields. Separate fragilities for straight wind hazards were not developed as the wind speeds from a tornado were considered bounding. A sample of the missile fragility output is provided in **Figure 17**.

4.3.2.5 Wind Pressure Fragility Analysis

An advanced code-based methodology has been applied in the development of the Point Lepreau Nuclear Generating Station wind pressure fragilities. The method applies the basic code-based approach with code and load-effect calculations. The methodology considers wind direction, terrain roughness, blockage, and structure enclosure state. The net load effects are modeled as a function of the envelope cladding fragility and overall structure fragility.

Wind loading effects include the aerodynamic forces produced by the dynamic pressure component of the wind flow, the associated atmospheric pressure change within the core. These wind loading effects may damage the building that the target is located in as well as the target itself. Structures may also collapse onto targets.

The analysis of fragility for a target depends on careful definition of failure modes and the potential interaction of individual failure modes. The interaction of failure mode effects (for example, external pipes experiencing wind and missile loads simultaneously) was considered in the modeling of the failure modes. **Figure 18** provides a sample of the wind fragility curves for one structure at Point Lepreau Nuclear Generating Station. All key safety-related structures were assessed in a similar manner.

4.3.3 Conclusion

A comprehensive high wind hazard and missile fragility assessment was performed to better understand the possible wind hazard based on state-of-the-art modeling and the latest experience and knowledge of winds. The results of the hazard assessment demonstrate that tornados pose a negligible hazard to Point Lepreau Nuclear Generating Station. Hurricanes also contribute little to the overall hazard compared to straight winds.

The design basis for the plant was established based on a 100 year return period for wind. An internal review of the protection of the plant against the equivalent wind speed from the hazard assessment did not reveal any changes required to the plant.

To deal with potential missile generation and the hazard caused by winds, and other weather-related events, Point Lepreau Nuclear Generating Station has in place a severe weather procedure that provides direction to plant operators to take a more and more defensive and safe posture with the plant to protect the public and our workers depending on the predicted winds, which includes potentially shutting down the plant before the weather event arrives.

4.3.4 Impact on Probabilistic Safety Assessment

The potential impact on PSA was assessed as part of the work done in *Section 5.0* considering a wind magnitude up to an equivalent of a 10,000-year event, two orders of magnitude beyond the design basis of the plant. The likelihood of each modeled wind event combined with wind pressure fragility and missile fragilities were assessed against the screening criterion. Based on the screening, all wind hazards were screened out from further detailed analysis via PSA.

4.4 External Flooding Hazard Assessment

Plant flooding from external sources was examined during the original plant siting of Point Lepreau Nuclear Generating Station. Flooding from the following sources was considered

- Rainfall
- Large astronomically induced tide
- Storm surge
- Wave run-up
- Tsunami

4.4 External Flooding Hazard Assessment, Continued

The probable maximum storm was used to determine the adequacy of safety-related structures to runoff flooding. This storm is based on a rational consideration of the simultaneous occurrence of the maximum conditions that contribute to a storm. The maximum probable storm hyetograph is based on a total of 21 inches (530 mm) of rain falling over a six hour duration. This hyetograph represents an envelopment of maximized intensity-duration values obtained from all types of storms. During the maximum probable storm, it is assumed that the capacity of the plant's drainage system will be temporarily exceeded and the storm runoff may be assumed to be overland flow. Considering the extreme case in which the entire storm runoff is directed over the plant area platform to the sea, the maximum depth of overland flow is predicted to not exceed six inches (15 cm). Point Lepreau Nuclear Generating Station has experienced a number of storms that have resulted in minor flooding in some parts of the station such as the underground tunnel that leads from the condenser cooling water pump house to the turbine building, and elevation -5 feet of the turbine building. No plant transients and thus no challenge to nuclear safety existed in such cases. Plant staff was able to deal with the clean-up, efforts have been undertaken to reduce water ingress from certain areas, and a greater importance has been placed on the maintenance of building sump pumps.

4.4.1 Tsunami Hazard Assessment

4.4.1.1 Introduction

When discussing tsunamis, it is important that when referring to the height of a tsunami, it can be referenced as "peak-to-trough" (i.e. from the valley between waves to the peak or highest crest of a wave), or it can be referenced from mean sea level, which is about half of the height from "peak-to-trough". Making this distinction is important so that when different tsunami events or studies are compared, or if the height of the tsunami is compared to a particular height on land that is referenced to mean sea level, the height of the tsunami is not misrepresented and an "apples to apples" comparison is made.

Mean sea level can be considered as the average half-way point between low and high tides.

Another term that is used often is called "runup". Runup is defined as the level of land inundation above still water level, or how high the water will run up on land as the tsunami washes ashore. This level is typically referenced to mean sea level.

4.4.1.1 Introduction, Continued

The generation of a tsunami requires a source, or something that causes a large displacement of water in the ocean such as a subduction-type earthquake or an underwater landslide. The displacement of water caused by the underwater event generates waves with a very long wavelength and which can travel at a very high rate of speed. In the deep ocean waves can travel upwards of 800 kilometers per hour. The waves can also be far apart from several minutes to several hundreds of minutes. As the tsunami moves towards shore and the depth of water shallows, the energy of the tsunami drives the waves upwards, effectively amplifying their height. The height of those waves and how far inland the tsunami can travel is governed by many factors including how much energy is left in the tsunami after the irregular shape of the ocean floor breaks up or reduces the energy.

During the 1970's when the site for construction of Point Lepreau Nuclear Generating Station was originally selected, the potential for tsunamis was considered. At that time, assessments and historical information led to the conclusion that a storm surge from a maximum probable hurricane would be larger than a potential tsunami and such a storm surge would not overtop the Point Lepreau peninsula even when considering wave action generated by wind.

In 2012 the Geological Survey of Canada—a division of Natural Resources Canada—issued a preliminary tsunami assessment of the Canadian coastline [32], which included identifying possible tsunami hazards that might be generated from earthquakes and underwater landslides occurring in the Atlantic Ocean. This preliminary assessment refers to the height of a tsunami from "peak-to-trough". The assessment was generic in nature in that it did not consider effects on particular facilities or building structures or how high those structures might be above mean sea level, and simply assumed that a tsunami with a height of 1.5 metres (0.75 m above mean sea level) had "damage potential" and a tsunami with a height of 3 metres (1.5 m above mean sea level) could have "significant damage potential".

In contrast to the tsunami thresholds used in the 2012 preliminary assessment [32], the grade level of most buildings at Point Lepreau is 13.7 m above mean sea level, well above the tsunami threshold values used by the Geological Survey of Canada. The lowest point is the sea water intake (condenser cooling water) pump house, which is at about 7.62 m above mean sea level. In its review of the preliminary assessment, NB Power noted that the assessment indicated the hazard for the Atlantic coastline was not well constrained, that it formed a good framework for further study and recommended further study to understand site-specific effects of a tsunami. On that basis, NB Power contracted experts to perform a full probabilistic tsunami hazard assessment for the Point Lepreau region to determine if there is a hazard to be concerned about or not. As a result, a state-of-the-art probabilistic tsunami hazard assessment was performed using the latest modeling simulations, data and state of knowledge regarding tsunamis, how they are formed and how they move towards Point Lepreau.

4.4.1.2 Methodology and Results

Overall, performing the tsunami hazard assessment involved three key pieces of work:

1. Field work to find any historical evidence of tsunamis that may have inundated southern New Brunswick
2. Through detailed models, simulate the generation of tsunamis from various possible sources in the Atlantic Ocean, how they move towards the Bay of Fundy and Point Lepreau and their potential size
3. Perform probabilistic modeling to determine the likelihood of those tsunamis.

4.4.1.2.1 Paleotsunami Investigation

NB Power hired one of the foremost experts in the world to perform field work referred to as a paleotsunami investigation, which involved investigation of peat bogs, marshes, river beds and lake edges from southeastern Maine to as far east as Walton Lake and north to the Keswick and Nashwaak Rivers (see **Figure 19**). The field work involved excavating pits and taking borehole samples to find any evidence of a large tsunami that might have come ashore at any time after the ice age, which were also carbon dated to determine when those may have occurred.

Figure 20 provides an example of what the field study is looking for as a result of excavation, and shows a typical finding of tsunami deposits at Taylor's Bay on the southern coast of Newfoundland caused by a 1929 tsunami generated by an underwater landslide at the Grand Banks.

Figure 21 provides the results of bore hole logs for Upper Duck Pond on Campobello Island. The bore hole logs provides an indication of deep deposits that could be carried by a tsunami onto shore and how long ago that may have occurred. Core logs similar to those presented in **Figure 21** were collected in many areas of the study area.

The results of the field work for the study region surrounding Point Lepreau showed that there is no evidence to suggest that tsunamis have inundated the study sites since 2350 years Before Present (B.P.) or B.C. 400, and possibly since 4290 years B.P. or B.C. 2340. Therefore, it is unlikely that a tsunami with a runup more than 2-4 m have struck the study region during the past 2300 years or so.

4.4.1.2.2 Deterministic Simulation of Tsunamis

Using state of the art 3-dimensional modelling, which is referred to as deterministic simulation, the most likely transatlantic sources of tsunamis were identified (see **Figure 22**). These included:

- Earthquake sources that are far away, such as the Puerto Rico Fault in the Caribbean and the Iberia fault zone in the Atlantic Ocean just west of Spain and Portugal;
- Earthquakes that may be close by including the Oak Bay fault that runs through Passamoquoddy Bay; and,
- Underwater landslide sources such as landslides along the continental shelf at the mouth of the Gulf of Maine, and landslides caused by flank collapse of the Cumbre Vieja volcano on Las Palma in the Canary Islands.

Based on prior geological studies of how often such events might occur and detailed modelling of the above events, the generation of tsunamis and how they would propagate or move towards North America and Point Lepreau were simulated and analyzed. Underwater features and irregularities in the ocean floor (called bathymetry), including those along the North American continental shelf, in the Gulf of Maine and Bay of Fundy were accounted for in terms of their ability to break up the energy of a tsunami (see **Figure 23**).

To obtain an accurate simulation of the effect bathymetry (or the irregular features of the ocean floor) may have on the tsunami, a nested spherical grid was used in the models. As shown in **Figure 24**, the grid resolution was several kilometers, but as the tsunami wave moved towards the Bay of Fundy, and then closer to Point Lepreau, the model included a finer and finer resolution (see **Figure 25**) to provide better simulation of what is happening with the tsunami as it approaches shore.

Assuming a tsunami is generated by a source across the Atlantic Ocean that moves towards the Bay of Fundy, when it contacts the continental shelf the waves are amplified and driven upwards. However, at the same time Georges Bank and Browns Bank (see **Figure 23**) removes a great deal of the energy. The much deeper Northeast Channel allows more of the tsunami energy to move into the Gulf of Maine. As what's left of the tsunami moves further into the Bay of Fundy, Grand Manan Island causes a further shadowing effect, which helps to protect the Point Lepreau Nuclear Generating Station. **Figure 27** shows the results of the deterministic 3-D modeling for a very large earthquake occurring along a subduction fault at the Puerto Rico trench, which could drive tsunami waves northwards towards the Gulf of Maine and Bay of Fundy. **Figure 27** shows the bathymetric effects as the tsunami strikes the continental shelf and drives the wave height upwards. The continental shelf, Georges Bank and Browns Bank removes much of the energy of the tsunami as it travels further northward into the Gulf of Maine and mouth of the Bay of Fundy.

4.4.1.2.2 Deterministic Simulation of Tsunamis, Continued

The detailed tsunami modeling for Point Lepreau was done at various tide levels—low tide, mean sea level and high tide. This was done to see what affect tidal level might have on the tsunami and how large it could potentially be. The results show that, generally, for the higher the tide, the larger the tsunami could be and the lower the tide, the smaller the tsunami will likely be as more energy is removed by the bathymetry of the Bay of Fundy as it moves up the bay.

Based on geological studies, earthquake sources that were modelled were varied in strength or magnitude to see what affect it would have on tsunami generation. Some of the earthquake magnitudes were as large as the Great Tohoku Earthquake that occurred on March 11, 2011, just east of Japan. The simulations show that the largest plausible tsunami caused by an earthquake across the ocean might result in a runup of 6.3 metres. This is not enough to reach any structure at Point Lepreau Nuclear Generating Station, even at its lowest point.

Potential underwater landslides result in the largest simulated tsunamis that might affect the Bay of Fundy. For the Cumbre Vieja volcano on Las Palma in the Canary Islands, it was assumed that various volumes of material would rapidly slide off the mountain (called a flank collapse) and into the ocean causing large waves and tsunami. Our experts considered 20, 40 and 80 cubic kilometers of material collapsing into the ocean. The volume of the landslide correlates to the size of a potential tsunami. Even for the worst-case plausible volcano collapse of 80 cubic kilometers, by the time the energy of the tsunami is dissipated by Georges Bank, Browns Bank and the bathymetry of the Gulf of Maine and Bay of Fundy, the highest water level at Point Lepreau Nuclear Generating Station is estimated to be about 7.2 meters at high tide. This is still not enough to reach any structure or cause damage to the plant.

In considering underwater landslides along the continental shelf, several locations were selected along the shelf. For most locations, a great deal of the tsunami energy is broken up Georges Bank and Browns Bank. Therefore, another event was modelled at the location of the Northeast Channel where very little of the tsunami energy travelling into the Gulf of Maine would be affected. Using geological data and evidence of underwater landslides from various literature sources, a maximum plausible volume for the landslide was established at about 165 cubic kilometers of material. Again, various landslide sizes were considered in the study to see what effects there might be on the generation of tsunami. Considering the largest plausible landslide at the Northeast Channel, it could potentially generate a tsunami at high tide with a water level of 8.3 meters. This height of water could contact the condenser cooling water pump house at Point Lepreau Nuclear Generating Station but is not high enough to wash over the peninsula, overtop site and affect our ability to control and cool the reactor using emergency water sources.

4.4.1.2.2 Deterministic Simulation of Tsunamis, Continued

Earthquakes caused by the Oak Bay fault at Passamoquoddy Bay did not result in any significant tsunamis and were generally less than 1 metre in height, similar to the worst case tsunamis that might be caused by meteorological conditions.

4.4.1.2.3 Probabilistic Modeling of Tsunamis

It has been confirmed through the detailed 3-D simulations that most events that could generate tsunamis will not affect Point Lepreau. Only one postulated and very large underwater landslide along the continental shelf occurring in a specific location at the Northeast Channel might result in a tsunami that could contact our condenser cooling water pump house. How often is that likely to occur? Existing scientific studies estimate how large and how often these have occurred in the past at various locations along the continental shelf. Using that information as an input, experts indicate that the likelihood of that event occurring is very rare and the likelihood of large earthquakes in Puerto Rico or in Iberia is much more likely, and if they generate a tsunami it is unlikely to affect the plant.

Figure 28 shows the mean hazard curves assuming the tsunami occurs coincident with a very high tide.

The mean Annual Frequency of Exceedance (vertical axes in **Figure 28**) is a term that helps us to determine the likelihood of a tsunami of a certain size, and in this graph it is expressed as the run-up at Point Lepreau Nuclear Generating Station above tide level. If the inverse of the Annual Frequency of Exceedance is calculated, the result is an average time period (or return period) that the tsunami might occur. High astronomical tide at the Point Lepreau peninsula is about +4.0 metres relative to mean sea level. To determine the total mean likelihood of a tsunami from all potential transatlantic and local sources (i.e. black solid line) contacting the condenser cooling water pump house, which is at an elevation of 7.62 metres above mean sea level, the tsunami runup would need to be 3.62 metres above the high astronomical tide level. Therefore, on **Figure 28**, 3.62 metres has an Annual Frequency of Exceedance for the total hazard (all sources) of about $1x10^{-5}$/yr or around a 100,000 year return period. Note that the worst case tsunami from an underwater landslide that results in a total water height of 8.3 m (from the 3-D simulations discussed above), has a predicted return period of about 500,000 years from **Figure 28** when considering the landslide hazard curve only (i.e. the blue dashed line)

4.4.1.2.3 Probabilistic Modeling of Tsunamis, Continued

One could also use the same logic to consider over-washing the rest of the plant at 13.7 metres (4 meters high astronomical tide level + 9.7 metres on **Figure 28**) as about $4x10^{-8}$/yr or around a 25,000,000 year return period. However, the caveat to this estimated return period is that there is no evidence of tsunamis that large ever having affected the Bay of Fundy. Given that the 3-D simulations of worst-case plausible tsunami events does not overtop site, NB Power believes that the likelihood of overtopping the whole site is more an artifact of the probabilistic model rather than reality and the hazard, therefore, is considered negligible.

So far the potential for tsunami runup has been discussed. However, the phenomena of a tsunami also includes drawdown--that is, how far will water withdraw from the shoreline as it rushes out when a tsunami is first coming onto shore. The concern was whether or not such a drawdown could damage condenser cooling water pumps even if the tsunami did not contact the pump house. Therefore, the detailed study also includes estimates of the water levels during drawdown and its likelihood. **Figure 29** provides an example for the case where the initial Bay of Fundy water level is at mean sea level. Following review by system specialists at Point Lepreau Nuclear Generating Station, it was concluded that more tsunamis equivalent to a 10,000 year return period the pumps will be undamaged from drawdown caused by a tsunami.

4.4.1.3 Conclusions

A detailed study of potential tsunamis generated in the Atlantic Ocean and how they might affect the Point Lepreau Nuclear Generating Station site was performed. The detailed study indicates that the hazard, and therefore, the risk to the plant is low. Only one simulated worst-case plausible tsunami indicated that one low-lying building, the condenser cooling water pump house, could be contacted by a tsunami caused by a landslide and is considered to be a very rare event. Even if that were to occur, the reactor cooling capability through emergency services and back-ups will not be affected. In conclusion, the probabilistic tsunami hazard assessment has demonstrated that Point Lepreau can be considered a “dry site” due to its high elevation. The existing design protection for Point Lepreau in terms of tsunami hazard is considered adequate.

Even though the detailed study does not indicate a significant hazard for Point Lepreau, one of the lessons learned from the accident at Fukushima Daiichi is to not put too much faith in analytical models and studies. We still need to deal with the unknown, the “what if”? As a result, for additional protection, Point Lepreau Nuclear Generating Station has put in place a tsunami procedure that provides direction to plant operators to take a more and more defensive and safe posture with the plant to protect the public and our workers depending on the nature of the tsunami advisory, warning or alert, which includes potentially shutting down the plant before the tsunami arrives.

4.4.1.4 Impact on Probabilistic Safety Assessment

The probabilistic tsunami hazard assessment has demonstrated that tsunamis are not a significant concern for Point Lepreau, and both the run-up and the drawdown due to tsunami hazards can be screened out from further detailed analysis. As a result, no further external flooding probabilistic safety assessment is needed to evaluate vulnerabilities or identify plant improvements when considering tsunami hazards.

5.0 Assessment of Other External Hazards

5.1 Introduction

In support of confirming the PSA scope at Point Lepreau Nuclear Generating Station, a comprehensive evaluation and screening of external hazards was performed based on a list of all potential external hazards compiled from a variety of sources. Screening criteria were established; events were evaluated against the screening criteria to determine if the events were risk significant; and, for those events not screened out, bounding analysis was performed to determine if further detailed analysis for the event is warranted via PSA.

5.2 Methodology

The first step to assess external hazards is identification of the hazards and several sources are available which provide lists. The following documents were used for the identification of external hazards:

1. Canadian Nuclear Safety Commission C-6 Revision 1 [12]
2. Canadian Nuclear Safety Commission REGDOC 2.4.1 [13]
3. United States Nuclear Regulatory Commission NUREG/CR-2300 [14]
4. International Atomic Energy Agency-TECDOC-1341 [15]
5. International Atomic Energy Agency-TECDOC-1487 [16]
6. American Society of Mechanical Engineers ASME/ANS RA-Sb-2013 [17]

The most inclusive list is ASME/ANS RA-Sb-2013 [17]. However, two additional potential hazards were added to this list, namely, i) electromagnetic interference from telecommunications equipment, and ii) events in other reactors on the site. As Point Lepreau Nuclear Generating Station is a single unit site, the second item does not apply.

The screening methodology is in line with international practice and, more specifically, with ASME/ANS RA-Sb-2013 [17].

5.2 Methodology, Continued

Once the comprehensive list of external hazards was identified (see **Table 4**), the next step was to determine whether the events can be screened out. Two types of screenings have been used:

1. Preliminary screening
2. Bounding analysis

The preliminary screening is a qualitative method and the bounding analysis is quantitative. Each identified hazard is screened, and if the hazard is screened out, then no further detailed analysis via PSA is required. The preliminary screening has five associated criteria whereas the bounding analysis had two criteria to be applied.

- Preliminary screening:
  Criterion 1: The hazard is of equal or lesser damage potential than the events for which the plant has been designed. This requires an evaluation of plant design bases in order to estimate the resistance of plant structures and systems to a particular external event.

  Criterion 2: The hazard has a significantly lower mean frequency of occurrence than another event, taking into account the uncertainties in the estimates of both frequencies, and the event could not result in worse consequences than the consequences from the other event.

  Criterion 3: The hazard cannot occur close enough to the plant to affect it. This criterion must be applied taking into account the range of magnitudes of the event for the recurrence frequencies of interest.

  Criterion 4: The hazard is included in the definition of another event.

  Criterion 5: The hazard is slow in developing, and it can be demonstrated that there is sufficient time to eliminate the source of the threat or to provide an adequate response.

- Bounding Analysis:
  Criterion A: The hazard event has a mean frequency $<10^{-5}$ /year, and the mean value of the conditional core damage probability[3] is assessed to be $<10^{-1}$.

  Criterion B: The core damage frequency, calculated using a bounding (demonstrably conservative) analysis, has a mean frequency $<10^{-6}$ /year.

[3] Conditional core damage probability is defined as the probability that core damage will occur assuming that an initiating event has occurred.

5.2 Methodology, Continued

Based on the international screening criteria, following ASME/ANS RA-Sb-2013 [17], five hazards have been further analyzed and were the subject of a bounding analysis. These five hazards were:

- Aircraft impacts
- Biological Events (e.g., Zebra Mussels)
- External flooding including:
  - Extreme rainfall events
  - Tsunamis from any tsunamigenic source
- Extreme winds including:
  - Tornadoes
  - Hurricanes
  - Straight winds
- Transportation accidents

Examination of combination of hazards has also been conducted.

The screening methodology for the wind hazard bounding analysis multiplies the frequency of the winds at various speeds by the mean damage probability (from wind pressure or missile fragility calculations) that is applicable to that structure and its contents, and then compares the results to Criterion A and B above. If none of the criterion can be met such that the event can be screened out in that initial comparison, then further measures are considered to meet one of the criteria.

International Atomic Energy Agency Safety Series Guide SSG-3 [18] states in paragraph 6.20, "*In order to eliminate specific hazards from the high wind category, it should be proven that the climatic conditions specific to the location of the plant support the assumption that these hazards are not sufficient to damage the plant (e.g. hurricanes in a non-coastal area). Wind hazards with a certain potential for damage should be screened out only when it is demonstrated that the frequency of exceedance of a particular wind velocity is negligible*." Therefore, specific wind hazards may be eliminated (screened out) in the wind hazard category if it is determined that the hazards are not sufficient to damage the plant's critical structures, systems and components and adversely affect reactor control, heat sinks or containment integrity.

The screening methodology involves calculating the total failure frequency for various targets (i.e. buildings) caused by tornados, hurricanes or straight winds as a result of wind pressure and wind-generated missiles. The result of the screening demonstrated that no further detailed analysis of wind events using PSA was required.

5.3 Combination of External hazards

The potential combination of external hazards included categorization has been examined in the following manner:

1. Coincidental hazards, which are hazards that occur simultaneously without a common mechanism. For example, an earthquake shortly after an aircraft crash or vice versa. Mathematically, these are independent events.
2. Consequential hazards, which are hazards that have a causal relationship. These combinations are possible only if the first condition has been fulfilled – therefore, the order is very important. For example, an earthquake can cause rail line derailment, but not vice versa.
3. Correlated hazards, which are hazards that originate from the same parent event. For example, a rail accident and toxic gas release can occur as a result of the same parent event – rail line derailment. However, there may be circumstances where there is some potential for one event to influence another.
4. Not applicable hazards: These are hazard combinations that:
    - Cannot physically occur at the same time; or,
    - Are not correlated and cannot occur coincidentally or consequentially. For example, soil failure cannot cause an earthquake.

These hazards are screened out.

Coincidental hazards are screened out if the frequency of the combination hazards is less than the limit of 10^{-6} events/year. The frequency of combination hazard is calculated by the multiplication of the frequency of one hazard by the probability of the other hazard occurring at the same time ($F_{comb} = F_{Event\ A} \times P_{Event\ B}$).

The frequency of the consequential hazards is estimated by multiplying the frequency of the initial event (Event A) by the subjective probability value P_{comb} ($F_{comb} = F_{Event\ A} \times P_{comb}$). P_{comb} can be chosen based on the likelihood of the combination events to happen: Likely (1.0), possible (0.1), unlikely (10^{-2}) or highly unlikely (10^{-4}). The combination is screened out if the combination frequency is less than 10^{-6}.

The frequency of the correlated combination hazards is calculated by multiplying the annual frequency of the parent event and the conditional probabilities of the child events ($F_{comb} = F_{parent} \times P_A \times P_B$).

The assessment concluded that there are no combinations of external hazards that warrant further detailed analysis using PSA for the Point Lepreau site. All external hazard combinations have been screened out.

5.4 Conclusion

A comprehensive evaluation of all potential external hazards and external hazard combinations that might affect the Point Lepreau Nuclear Generating Station site has been performed. The latest hazard information, including a state-of-the-art probabilistic tsunami hazard assessment and high wind assessment, has been considered in the context of preliminary and bounding analysis screening criteria to determine if any further detailed analysis through PSA is necessary. Seismic hazard has always been included in scope of the PLNGS PSA. The additional assessments have shown that there are no additional external hazards requiring further detailed analysis. High winds and external flooding including tsunami external hazards have been screened out and do not require a PSA.

6.0 Overview of PSA Methods

Risk assessment is based on the idea that the product of the frequency of occurrence of an event and the consequence of the event represents a useful and meaningful quantity. This product is defined to be the risk from the event and is expressed in units of consequence per unit of time.

Risk assessment provides a means of quantifying the degree of safety inherent in a potentially hazardous activity as well as a common basis for comparing the relative safety of dissimilar types of activities and industrial processes. One of the principles of the risk assessment process is that the larger the numerical value of risk for a particular event or combination of events, the more important the event is to safety. Thus, measures to reduce calculated risk improve the level of safety. PSA represents the process by which risk is quantified, leading to the identification of the dominant contributors to risk. If necessary, the dominant contributors can be used to create strategies to reduce risk and improve safety.

6.1 Safety Goals

There are two safety goals for the Point Lepreau Nuclear Generating Station PSA:

1. Core Damage Frequency (CDF)
2. Large Release Frequency (LRF)

A core damage accident results from a postulated initiating event followed by failure of one or more safety system(s) or safety support system(s). Core damage frequency is a measure of the plant's accident preventive capabilities and is quantify by summing the frequencies from all event sequences that can lead to significant core damage.

Large release frequency is a measure of the plant capability to contain radionuclides within the containment envelope and therefore a measure of the risk to society and to the environment due to the operation of a nuclear power plant. Large release

frequency is quantified by summing the frequencies of all event sequences that can lead to a release to the environment of more than 10^{14} becquerel of Cs-137. The quantitative safety goals are described below (extracted from *REGDOC-2.5.2*).

For PLGS the safety goals are stated in **Table 10**.

The safety goals are consistent with IAEA guidance provided in SSG-3 [18], which states:

"*The objectives for core damage frequency in Ref. [4] are (a) 1×10^{-4} per reactor-year for existing plants and (b) 1×10^{-5} per reactor-year for future plants*" (footnote 3, page 10),

and,

"*The objective for large off-site releases requiring short term off-site response is 1×10^{-5} per reactor-year for existing plants*." (footnote 4, page 11).

The safety goal represents the high level of tolerable risk exposure above which action shall be taken to reduce risk. The administrative goal represents the desired objective towards which the facility should strive, provided that measures to further reduce *risk* are cost effective, such as when benefits are comparable to, or greater than, the cost of implementing the measure.

The safety goals pertaining to Severe Core Damage are intended to help the nuclear facilities make routine decisions relating to changes in plant operation, configuration or procedures. For proposed changes significantly affecting the integrity of containment (either directly or indirectly) a further assessment against the Large Release safety goal is required.

It is broadly recognized by PSA practitioners that the greatest safety value in performing a PSA is not in the comparison of risk estimates against predefined safety goals. Rather, what is important are the insights coming from the PSA; understanding of changes in risk; development of event sequences and what they tell us; looking at short cutsets for weaknesses in defense-in-depth; identification of vulnerabilities including single point vulnerabilities; and, identifying the areas to improve that most benefits risk reduction. Regardless, most regulatory frameworks tend to focus on quantitative safety goals and the comparison of risk estimates against those goals. Therefore, it is necessary to ensure that Canadian utility operator response is consistent in terms of actions that are taken when either safety goal or administrative goal targets are exceeded. The approach described in **Figure 30** is applied at PLGS.

6.2 Crediting Emergency Mitigating Equipment in PSA

Following direction by the Canadian Nuclear Safety Commission to include portable emergency mitigating equipment (see *Section 3.4*) in PSA to evaluate the benefits, the Canadian industry as a whole has done so as part of the baseline models where necessary. Taking credit for portable emergency mitigating equipment and associated strategies in PSA is justifiable for the following reasons:

- PSA is a probabilistic assessment and, unlike deterministic safety analysis that follows a single/dual system failure approach, all systems are considered to have a certain probability of failure.
- The purpose of PSA is to evaluate credible combinations of failures and the possible mitigating measures to evaluate plant vulnerabilities for the full range of accidents and their consequences. Risk estimates of core damage or large release are also provided that can be compared to safety goals. However, to limit costs, sometimes conservative assumptions are made, such as assuming the failure of Group 1 systems and equipment following a seismic event by not including them in the models.
- If the combination of modelled system or equipment failure results in a very unlikely progression to a severe accident, plant procedures and guidelines are in place to deploy emergency mitigating equipment to mitigate the consequences, which is the purpose of emergency mitigating equipment.
- Robust emergency mitigating equipment at PLNGS has been procured, and deployment of the portable equipment has been drilled to ensure that critical performance objectives have been demonstrated so that we have a high degree of confidence that all postulated accidents scenarios can be effectively mitigated or terminated.
- Emergency mitigating equipment has been designed to be an effective mitigating measure under severe accident conditions that can be credited in PSA. While there may be no international consensus on emergency mitigating equipment modeling in PSA, the emergency mitigating equipment has been included in the PLNGS PSA where appropriate in accordance with methodology submitted to, and accepted by, the CNSC.
- Emergency mitigating equipment has been credited as recovery actions instead of being incorporated directly into event tree models. This results in using more conservative (i.e. higher) probability of failure values.
- PLNGS is well aligned with other Canadian utilities and compliant with CNSC-accepted PSA methodologies by crediting emergency mitigating equipment in PSA.

6.3 Internal Hazards PSA Methods

The goal of a Level 1 PSA is to identify occurrences at the plant that can cause a transient that would challenge fuel cooling, establish the plant response and identify what systems can be credited to mitigate the event. Depending on the success or failure of the mitigating systems the event may lead to a successful outcome or to a plant damage state or damage to the reactor core.

A key component of a PSA for a power reactor is to identify a list of potential plant operating states, considering steady state at-power operation, planned shutdown evolutions, standard power manoeuvres and standard start-up evolutions. The plant operating states should be specified on the basis of actual operational experience and according to plant practices and procedures. Potential states were systematically reviewed and combined into the following plant operational states

- At-Power
- Shutdown with the heat transport system full
- Shutdown with the heat transport system drained

Typically, the first PSA study completed for a station will be the Level 1 internal events PSA for the at-power plant operating state. Much of the effort of this study is in constructing models of what mitigating systems can be credited for a given transient, and how the mitigating systems can fail. In PSAs for other types of initiating events, e.g., internal fire, internal flood and seismic, much of the effort is associated with determining the impact these events have on the mitigating systems.

In the Level 1 PSA, the goal was to quantify the frequency of core damage. Once the core has been damaged, there is the potential for radioactive material to be released from the fuel into containment. The Point Lepreau Nuclear Generating Station design includes robust positive-pressure containment system (described in *Section 2.3.5.5*) to prevent the release of any radioactive material in the station from being discharged into the environment.

The Level 2 PSA studies the system failures and accident phenomena that might result in a release to the environment, and the timing and magnitude of the release. This information is combined with the Level 1 PSA model to quantify the frequency of possible large radiological releases. A simplified overview of the PSA process is presented in **Figure 31**.

The descriptions of the methodology for the various studies in the following subsections reflect different requirements for the different studies. At Point Lepreau Nuclear Generating Station, the PSAs for outage, seismic internal fires and internal flooding are built upon and integrated with the at-power internal events PSA model.

6.3.1 Level 1 At-Power Internal Events PSA

In fulfilment of PSA objectives as stated in *Section 1.2*, the Level 1 internal events PSA includes estimation of the overall severe core damage frequency that results from plant failures, as well as the frequency of accident sequences that result in serious economic consequences. The analysis consists of identifying the applicable initiating events, determining the response of plant systems during the event progression (using event trees and fault trees), and quantifying the detailed accident sequences, with special emphasis on sequences which lead to core damage, their basic causes and their frequencies. Internal events were determined and analyzed for both at-power and shutdown conditions.

There are innumerable different plant configurations that can be achieved owing to equipment duty cycling, maintenance and testing. There are also numerous evolutions required to move the plant from one configuration to another. For the purposes of the PSA, two bounding states are considered: the at-power (or running) state, and the shutdown state. The at-power state is discussed below. The shutdown state is addressed below in *Section 6.3.2*.

In accordance with REGDOC-2.4.2 [24], all methodologies for PSA at Point Lepreau Nuclear Generating Station have received regulatory acceptance.

6.3.1.1 Determination of Initiating Events

To ensure a comprehensive PSA it is necessary to address credible scenarios that may be encountered during the life of the plant. The identification of those various scenarios was the first stage in the assessment and is the foundation for all subsequent analysis work. To provide the necessary confidence that the set of scenarios chosen for analysis is complete and exhaustive, master logic diagrams have been employed for the systematic review of the plant for initiating events, which generates a comprehensive set of scenarios for the internal events PSA.

In summary, the systematic review for initiating events was divided into these stages:

- Identify distinct sources of radioactive material within the plant
- Identify mechanisms whereby radioactive material can be displaced from its normal location
- Identify initiating events; failures of the plant which may result in specific displacement mechanisms
- Group the initiating events in preparation for subsequent analysis; and,
- Assign a frequency to each initiating event group

The comprehensive list of initiating events selected for the Level 1 internal events PSA, at-power and shutdown conditions, are listed in **Table 5**.

6.3.1.2 Determination of Initiating Event Frequencies

Initiating event frequencies are established for all internal events. To distinguish between the various methods of calculating the frequencies, a numeric code is added in the "Initiating Event Code" column to identify the frequency derivation methodology as follows:

1. Frequency derived from operating experience
2. Frequency derived from pipe data calculations
3. Frequency derived from fault tree analysis

6.3.1.3 Event Progression

After the initiating events are identified (and before event tree development can begin), the safety functions necessary to prevent core damage (e.g., removal of heat) are defined. Based on these initiating events and functions, the safety and/or safety-related systems required to perform the functions are identified, along with any required support systems, such as service water, instrument air or electric power. Success criteria for each of these systems, necessary for the performance of the safety function, are then defined. For a particular system, typical success criteria may include the number of pumps required to operate and when they are required to operate, so that the safety function can be performed. Event progression, represented in the PSA as an accident sequence, is considered terminated when a sustainable and stable end state is reached.

Accident sequences are grouped into categories known as plant damage states (PDSs). The plant damage states are listed and described in **Table 6**. Severe core damage accidents are beyond design-basis accidents in which a rapid or late loss of the structural integrity of the reactor core occurs. Severe core damage accidents are characterized by plant damage states PDS0, PDS1 and PDS2. A loss of core structural integrity results from a loss of heat sinks leading to core damage involving multiple fuel channel failures and core disassembly. The core structure is defined as the calandria/end shield assembly. Core deformation accidents are those in which core structural integrity is maintained but fuel channel deformation occurs as a result of fuel heat being removed by moderator as a heat sink as opposed to coolant flow in the heat transport system. This type of accident is characterized by plant damage states PDS3 and PDS4. PDS5 represents an end-state where emergency core cooling is successful but not entirely effective, yielding wide-spread fuel damage. Limited fuel damage scenarios are represented by plant damage states PDS6, PDS7 and PDS8. PDS9 and PDS10 represents a release of radioactivity and tritium inside containment.

6.3.1.4 Event Trees

Once the initiating event and mitigation systems or functions are identified, event trees are developed depicting various possible sequences that could occur after the initiating event, by modeling combinations of mitigating system success or failure. Each sequence is considered terminated when a safe state is achieved (sustainable heat sink), when a plant damage state has been reached, or when the sequence of events is deemed to have a sufficiently low probability of occurrence (falls below the selected truncation limit).

6.3.1.5 Human Reliability Analysis – Post-Initiation

Post-accident human actions typically pertain to activities performed by reactor operators stationed in the main control room, and which take place after the onset and annunciation of an initiating event. Post-accident tasks are divided into diagnosis (perception, discrimination, interpretation, diagnosis and decision-making) and post-diagnosis (execution) tasks, both of which are intended to implement mitigation measures for ensuring or maintaining adequate fuel cooling. Post-accident operator actions are required in the following cases:

- Failure of the automatic actuation of the mitigating systems
- The automatic actuation of a mitigating system was successful, but its continuing operation requires operator action (e.g., the start-up of emergency water supply pumps after dousing tank inventory is exhausted)
- There are no design features for automatic mitigating action

Post-accident operator actions are generally modelled in the event trees as separate decision branch points (top events) and are usually placed just before the top event of the associated system requiring manual initiation. Post-accident human errors included in event trees are those actions, which are considered to be key or critical actions and failure to perform these actions could lead to core damage.

6.3.1.6 Mitigation Systems

To estimate the event sequence frequencies, the success and failure probabilities are determined for each branch point on the event trees. This requires the identification and quantification of the important contributors to failure of each of the systems identified by the event tree development. Fault tree modelling and evaluation is the main tool used to derive the failure probabilities of the mitigating systems. Fault tree analysis is also used to derive the frequencies of some initiating events. Fault trees are constructed for all front-line mitigating systems and support systems.

6.3.1.6.1 Fault Trees

Fault tree analysis is a deductive method of failure analysis, which focuses on one particular undesired event (e.g., a system functional failure) and provides a method for determining causes of this event. The undesired event constitutes the top event in the fault tree diagram constructed for the system and corresponds to some particular system failure mode. The fault tree top event is an event that appears in the event tree.

A fault tree is a logical representation of the ways in which a specified undesirable event may occur. The Boolean solution of the fault tree defines the combination of events that can lead to system failure. The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that can result in the occurrence of a predefined undesired event or system failure.

For mitigating systems, if a front-line or containment system interfaces with support systems such as electrical power and/or service water, then models were developed for the required support systems and integrated with the front-line systems. System reliability analysis includes pre-initiation human reliability analysis, specifically, pre-initiation human reliability analysis (described briefly in *Section 6.3.1.6.3*). Dependent failures arising from system interdependencies and component common-cause failures are also modelled (see *Section 6.3.1.6.2* below).

6.3.1.6.2 Common Cause Failures

The reliability requirements of many systems are such that the design of these systems incorporates redundant channels or trains. When a system design includes two or more redundant trains of equipment, each of which is capable of performing the system function, the possibility of dependent failure exists. Dependent failure is an overall term applied to events that can cause multiple components to be unavailable because they are coupled in some fashion. In particular, dependent failures can affect the redundant trains in a system simultaneously and cause overall system failure. It is essential to carry out dependent failure analysis for systems incorporating redundancy since dependent failure is often a significant contributor to the overall system failure probability.

Dependent failures can be classified into two main types: explicit and implicit. Explicit dependencies are clearly identified as to the specific or shared cause of failure and are modeled and quantified in the system fault tree analysis. These include three main areas:

6.3.1.6.2 Common Cause Failures, Continued

- Functional dependencies - redundant trains of equipment relying on common support services (e.g., cooling water, electrical systems)
- Physical interactions - physical phenomena which can impact multiple components such as the external events (fire, flood, seismic)
- Human interactions - pre-accident human errors in the testing or maintenance of component groups are addressed in human reliability analysis

The implicit dependencies are the "residual" causes of multiple component failures. These are known as common cause failures. Generally, the root causes of such failures are related to environmental conditions that locally affect component groups, common design faults, or additional human interactions that are not identified in the human reliability analysis. The modeling is implicit in the sense that the common cause failure events incorporated in the fault tree encompass a variety of potential causes that are not explicitly stated. In some cases, causes such as environmental factors can be modeled explicitly if sufficient data are available to do so. Where such information is not readily available, these causes are included in the domain of common cause failures.

The unified partial method for determining beta factors used in the common cause failure was adopted for the PSA.

6.3.1.6.3 Human Reliability Analysis – Pre-Initiation

Pre-Initiation actions occur prior to an accident and are associated with maintenance, test, calibration and repair errors which degrade system availability. They can be referred to as pre-accident human actions/errors. Prior to an initiating event, plant personnel can affect availability and safety by inadvertently disabling equipment during calibration, testing, or maintenance. This type of human error can occur and not be detected until the system is required to operate following an initiating event, or until the next test of the system.

The benefits of testing and maintenance are modelled by the selection of repair times, and test and maintenance intervals in the equipment unavailability calculations. The factors which degrade system availability are modelled as test and maintenance outages based on the associated downtime. The pre-accident human actions (errors) are explicitly incorporated as basic events in the fault trees for mitigating systems or initiating events.

6.3.1.6.4 Model Integration

Once the event trees and fault trees are developed, they are linked to determine the frequencies with which various plant damage states can occur based on those grouping of sequences with similar consequences. **Figure 32** provides a graphical representation of the linking. The linked models are then converted into a "master fault tree" for quantification.

6.3.1.6.5 Quantification

Accident sequence quantification is the process of quantifying the endpoint frequency of the plant success/damage states and determining the minimal cutsets. A minimal cutset is the combination of faults representing the minimum number of basic faults necessary for the event to occur.

The objective is to create a fault tree that includes all the decision branch points, which lead to the accident sequence under study. The frequency estimate for the sequence takes into account any modelled failures that are common between systems. Accident sequence quantification yields an estimate of the frequency of releases into containment for individual accident sequences by the solution of the event tree top logic and the sequence fault tree. Frequencies of the cutsets resulting in severe core damage are summed to obtain the overall core damage frequency of the plant.

6.3.1.6.5.1 Event Sequences

Accident sequence quantification is performed on each sequence of all event trees as described in *Section 6.3.1.4*. Each event sequence is a unique path in the event tree and consists of an initiating event followed by a series of failed and/or successful mitigating systems and post-accident operator actions. These failure and success events are either gates or basic events in the accident sequence quantification master fault tree. Quantifying a sequence consists of solving a specific fault tree that represents the combination of failure and success events for a sequence.

6.3.1.6.5.2 Recovery

Recovery analysis deals with the probabilistic evaluation of recovery actions and is an essential component of the accident sequence quantification process. All sequences from each event tree are quantified for preliminary cutset results. After the preliminary cutset results are obtained, recovery analysis is performed. The results obtained after applying recovery are the final results that provide a realistic estimate of the plant damage frequency.

Recovery analysis is an iterative process. First, the dominant contributors to severe core damage are identified from the preliminary cutset results. Recovery factors are then applied to reduce the probability of the dominant contributors. The plant damage frequency, after the recovery factors have been applied, is re-evaluated and a second set of results is produced. Reviewing the dominant contributors of the second set of results may further identify recovery factors. This iterative process continues until no further recovery factors can be found or when an acceptable plant damage frequency is achieved.

There are different recovery factors that can be applied:

- Recovery actions - actions taken by the operator to recover from a sequence of events, which also include deployment and use of portable emergency mitigating equipment
- Common cause failure recoveries - re-evaluation or recalculation of common cause failure events identified as dominant contributors
- Human reliability analysis recoveries - accounting for dependencies when more than one operator action occurs in a sequence. Also, recalculation of human reliability analysis events for dominant contributors and performance shaping factors in light of postulated fires, floods and seismic events.

Recovery Actions

Operator recovery actions are actions that can be taken by an operator to recover from a sequence of events. For example, if both diesel generators fail during mission, a credit for restoration of off-site power can be taken whereas if both diesels fail to start no credit can be taken due to the limited window of time. Criteria for applying operator recovery actions must be determined, and recovery actions must be applied consistently and only to cutsets for which operator recovery actions are applicable. Recovery actions may apply to operator actions or hardware component failures. The existing operator actions in a cutset must be considered, when adding recovery actions, to determine any dependent factors and/or to assess the overall maximum credit of the operator recovery action.

6.3.1.6.5.2 Recovery, Continued

Common Cause Failures
The original common cause failure factors were determined using the beta factors estimated using the unified partial method (see *Section 6.3.1.6.2* above). The beta factor determination was revisited if a common cause failure was identified as a dominant contributor, and sometimes the common cause failure probability was re-calculated based on a re-assessment of the beta factor. Alternatively, the recovery common cause failure was calculated using an alpha method.

Human Reliability Analysis
Operator dependency becomes an issue when an event sequence contains two or more failed operator actions in the same location or by the same crew. If such a dependency is found in a sequence, the second operator action is recalculated using the standardized plant analysis risk human reliability analysis (SPAR-H) methodology. Human reliability analysis events identified as dominant contributors were recalculated using the technique for human error rate prediction (THERP) methodology.

6.3.2 Level 1 Shutdown State PSA

The shutdown state PSA addresses additional concerns to those that are addressed in the at-power PSA. These include simultaneous system unavailability during different phases of an outage, the importance of operator actions to restore safety functions, and maintenance restrictions to various mitigating systems while the plant is in a specified shutdown state. The PSA includes an assessment of the initiating events that can occur during a shutdown plant operating state.

6.3.2.1 Initiating Events

The systematic review of initiating events, including events in the shutdown state, and their associated initiating event frequencies are included in **Table 5**. Initiating event frequencies for the shutdown state based on operating experience were calculated using station outage time (equal to the lifetime of the station less the effective full-power years).

6.3.2.2 Event Progression

Shutdown state event progression is determined in a similar manner as for the at-power PSA, with the added requirement to establish the applicable shutdown plant operating state: shutdown with the heat transport system either full or drained.

6.3.2.3 Mitigation Systems

The mitigation systems and related fault tree analysis is also different for the shutdown state. System configurations are different due to different maintenance and testing regimes during an outage. The required mitigation functions and action times are also different since the reactor core is only emitting decay power as opposed to full power.

6.3.2.4 Quantification

Quantification of the shutdown state PSA is performed in the same manner as for the at-power PSA discussed in *Section 6.3.1.6.5*.

6.3.3 Level 2 At-Power Internal Events PSA

The Level 1 PSA estimated the core damage frequency. The results of Level 1 are the input for Level 2 which studies the progression of core damage sequences to estimate the frequency of radionuclide releases within containment.

6.3.3.1 Grouping of Level 1 Event Sequences

The plant damage state (PDS) PDS0 represents sequences involving a rapid loss of core structural integrity due to failure of the reactor to be shut down when required. The likelihood of such an event is very low. The existence of two shutdown systems, Shutdown System 1 and Shutdown System 2, with at least two effective trip parameters on both systems, together with the reactor regulating system (setback, stepback) leads to very low predicted failure frequencies. It is conservatively assumed that failure to shutdown leads directly to containment failure and therefore the result of PDS0 is included into the calculation for early containment failure as a direct contributor to external plant release category zero (EPRC0).

PDS1 and 2 are grouped together and represent a total loss of heat removal, resulting in a severe core damage state. The summed frequency of PDS1 and PDS2 is much higher than the frequency of PDS0. Given their high frequency and the extent of associated fission product release into containment, this category is by far the most important one. The PDS1 and PDS2 sequences are subdivided into at-power and shutdown conditions.

PDS3 and PDS4 are grouped together, representing those accident sequences for which a loss of emergency core cooling has occurred, but moderator is acting as a heat sink. The consequences of reliance on the moderator as a heat sink are not severe in term of fission product releases but some fuel damage in many channels can be expected and deformation of the pressure tubes will occur.

PDS5 through 10 are grouped together for the Level 2 work.

6.3.3.1 Grouping of Level 1 Event Sequences, Continued

For Level 2 analysis, PDS1 and PDS2 event sequences are grouped in broad categories related to either the similarities in the initiating event or similarities in the subsequent event progression. These broad categories include:

- In-Core loss of coolant accident
- Small loss of coolant accident
- Large loss of coolant accident
- Station blackout
- Containment bypass
- Shutdown state

The sequences assigned to each category are further subdivided based on similar plant conditions, such as the availability and configuration of mitigating systems, containment subsystems and the availability of support systems.

6.3.3.2 Severe Accident Analysis

The Level 2 PSA takes as an input the core damage sequences from the Level 1 PSA and calculates the frequency and timing of various modes of containment failure that may cause releases of radioactive material to outside of the containment boundary. The deterministic accident progression is evaluated using a computer code that models the severe accident phenomena and fission product behaviour for unique, representative combinations of failures that lead to a severe core damage accident and successful/unsuccessful action of the containment mitigating systems and of operator actions. The severe accident analysis was conducted using the MAAP5-CANDU computer code.

The representative postulated accident scenarios selected for severe accident analysis were:

- Station Blackout, with the loss of cooling systems due to the loss of electrical power to Group 1 and Group 2 equipment
- Small loss-of-coolant accident, with a loss of emergency core cooling, moderator cooling system and other safety-related systems
- Loss of shutdown cooling during a shutdown state, when the primary heat transport system is drained to the header level, combined with a loss of emergency core cooling and the loss of the moderator cooling system and other safety-related systems
- In-core loss of coolant accident, with a loss of emergency core cooling and potential moderator drain through the ruptured bellows of the ruptured fuel channel
- Containment bypass events with a loss of emergency core cooling and the loss of the moderator cooling system
- Large loss-of-coolant accident, with a loss of emergency core cooling, moderator cooling system and other safety-related systems

6.3.3.3 Containment Envelope

The containment envelope comprises the reactor building, sealed penetrations and closed and open penetrations. All open penetrations are part of the containment isolation system. An intact containment assumes that the reactor building perimeter wall is intact, and the main and auxiliary airlocks and irradiated fuel transfer room are closed and intact. Strictly speaking, all of the analysis tasks which deal deterministically with the accident progression from each plant damage state and the calculation of the frequency and magnitude of releases from containment can be classified as Level 2 PSA activities.

Containment system fault trees are treated the same as other mitigating system fault trees (see *Section 6.3.1.6.1*).

6.3.3.4 Level 2 Event Trees

Accident progression and containment event trees, also known as a Level 2 event trees, represent the accident progression from the end of the Level 1 event sequence to an end-state, either successful containment or an external plant release (see **Table 7**). A Level 2 event tree will credit Level 1 mitigation systems to slow down the event or alleviate the effect of the accident. Mitigation systems that are either known to be functional or not called upon to act in the Level 1 analysis can be credited. The event tree then proceeds to credit containment systems.

6.3.4 Internal Fire PSA

The internal fire PSA includes fires occurring within the plant at nominal power conditions. Fires occurring during the shutdown state are not considered (see *Section 1.3* for further details). The impact from fires on plant nuclear safety risk comes from the fact that fires are common cause initiators. In other words, the event itself can cause initiating events as well as failures of redundant components and systems, and thereby reduce the number of mitigating systems available to bring the plant to a safe and stable state.

The progression of a fire event from initiation to a severe core damage state is very complex, with a very high dependence on the types of components and their physical proximity to each other. The probabilistic safety assessment of external events starts with the identification of the basic cause of the event, and then examines historical or physical data to establish the sources and frequency of the event initiation. The physical layout and characteristics of the plant are studied to determine the impact of the initiating event on the systems that maintain the plant in a safe state. This identifies the systems that could be lost initially as a result of the event and as the event progresses, and the probability with which they may be lost. This information is used in conjunction with the modified internal event PSA models to quantify the plant damage and severe core damage frequencies.

6.3.4 Internal Fire PSA, Continued

The major elements of the internal fire PSA are as follows:

- Determination of fire compartments based on the general arrangement drawings, information about fire barriers, information concerning ignition sources and combustibles in the areas, existing fire related plant procedures and instructions, and other available design and operation information.
- Identification of fire characteristics in terms of fire ignition sources, combustibles, fire protection such as fire barriers, and the location of safety-related and PSA-credited components and cables.
- Qualitative screening analysis, which involves screening out fire compartments from further analysis based on qualitative evaluation. The qualitative evaluation focuses mainly on the location of safety-related systems and equipment.
- Qualitative ignition source screening and estimation of fire ignition frequency for each fire compartment based on the fire ignition frequency database developed for each fire ignition category.
- Quantitative screening analysis, which involves screening out fire compartments from further evaluation, based on the conservative evaluation of severe core damage frequency.
- Refining the results of some fire scenarios, by performing analysis to eliminate explicit conservatisms in the fire scenario.
- Detailed analysis of the potentially significant fire scenarios remained after the screening analysis. Local operator recovery actions are also credited if justified.

The internal fire PSA addresses Level 1 by evaluating fire-induced severe core damage and Level 2 by evaluating fire-induced external plant releases.

6.3.4.1 Identification of Plant Characteristics

The identification of plant characteristics in view of the internal fire PSA was performed mainly by two tasks: fire walkdown, and cable routing analysis. The purpose of the fire walkdown was to collect information necessary for the fire PSA and to confirm information already collected during previous work such as prior fire PSA or fire hazard assessment. A subsequent confirmatory walkdown for the screened in scenarios was performed and scenarios modified or updated accordingly as a result of the walkdown findings.

6.3.4.1 Identification of Plant Characteristics, Continued

The walkdown provides information for each room such as physical room data, ignition sources, combustible materials including transient combustibles, PSA-credited devices, manual and/or automatic fire detection/suppression, fire barriers, adjacent space evaluation considering the fire resistance rating for the barriers, openings of the room, room boundaries and cables and cable trays located in each room.

A separate cable routing analysis was conducted to define all cable and conductor routings from the power source, control or instrumentation device to each end device. The effort was performed for all devices that are considered in the internal fire PSA. The locations of all devices, trays, cables and conductors in each cable route of a device circuit were defined through the use of a cable and conductor routing analysis software program and updated by Point Lepreau Nuclear Generating Station staff. The result is a cable routing database that provides the information about the affected PSA-credited components due to fire-induced damage to cables in a certain room.

The Point Lepreau site was subdivided into areas called fire compartments for the purposes of screening and, if necessary, detailed analysis. Typically, a well-defined, enclosed room is labelled as a fire compartment. The areas within the plant boundary considered all rooms in buildings with the potential to affect normal plant operation, as well as outside areas with equipment.

6.3.4.2 Determination of Fire Scenarios

Fire scenarios are developed to delineate the path of how a fire could cause damage to the PSA-credited equipment or cables. Once the fire starts, it can grow and may propagate to other areas and targets (PSA-credited equipment or cables). These targets may be damaged during the process of fire growth or propagation, which would depend on their relative location with respect to fires. In the meantime, the fire could be detected and suppressed by an automatic suppression system or manually by maintenance personnel present at the event, firewatchers or fire brigade. The fire scenario analysis considers the interaction between the fire growth and the fire suppression and provides the scenario that could cause damage to a set of PSA-credited devices and cables. The results of this analysis would be the fire scenarios, the frequency of each fire scenarios, suppression and detection fraction (non-suppression probability) and the damage state that each fire scenario could cause.

6.3.4.2.1 Screening

There are two levels of screening in the internal fire PSA: qualitative and quantitative screening.

Qualitative screening is used to eliminate areas with an obviously low impact on plant safety from further analysis, without the use of PSA plant models. The main criteria for qualitative screening of fire areas and/or scenarios are as follows:

- Fire in the area does not cause demand for plant trip or shutdown
- Fire area does not have safety related equipment
- Fire does not propagate to other areas having safety related equipment
- Fire area does not have a credible fire source or significant amount of combustibles

Quantitative Screening of fire areas and/or scenarios is primarily based on the fire initiation frequency and analysis of the impact on plant safety using information from the PSA plant models. A fire location and/or scenario can be screened out for the following situations:

- The unavailability of the equipment/system in a location due to fire is substantially lower than the unavailability of the same equipment/system due to all other causes
- If the frequency of the reactor trip due to fire induced equipment failures is substantially lower than the reactor trip frequency from all other causes
- The severe core damage frequency of an accident sequence from a fire in the location under consideration is less than the screening threshold

The quantitative screening analysis using the Level 1 internal events plant model is performed as follows:

1. Compute initiating event frequency for all areas not screened out in qualitative screening
2. Assume all equipment and cables are damaged by fire in fire area/scenario;
3. Determine fire impact on mitigating system models, and determine which ones cannot be credited for reasons such as environmental qualification
4. Determine which internal event PSA event tree can be used, and modify accordingly
5. Perform accident sequence quantification for the fire scenario; calculate conditional core damage probability and severe core damage frequency for each fire scenario
6. Calculate the sum of the severe core damage frequency for quantitatively screened out scenarios.

6.3.4.2.1 Screening, Continued

The quantitative screening criterion in terms of severe core damage frequency has been made more stringent from once in 10,000,000 years to once in 100,000,000 years to satisfy the guidance in NUREG/CR-6850 [26], which limits the contribution of screened out fire compartments to less than 10 percent of the total internal events risk. Therefore, the single scenario risk criterion is set a value that is high enough to allow some screening but sufficiently low that all risk-significant fire compartments should be retained and adequately assessed. The sum of all screened out sequences is less than 8.78% of the internal fire severe core damage frequency.

6.3.4.3 Level 1 Internal Fire PSA

Internal Fire PSA only considers the at-power plant operating state, as discussed earlier (see *Section 1.3*).

6.3.4.3.1 At-Power State

The Level 1 internal fire PSA was performed for nominal power conditions at the level of fire scenarios developed for each of the fire compartments, which may include a single room or multiple rooms. All postulated scenarios that could occur in each fire compartment were systematically checked. The impact on nuclear safety from the fire scenarios was assessed based on the equipment damaged in each fire scenario by estimating the severe core damage frequency. The severe core damage frequency was quantified by applying the fire frequency, applicable location factor or severity factor of the fire scenario, the non-suppression probability, and screening conditional core damage probability for fire-induced damage state. Fire scenarios were screened out from further analysis if their screening severe core damage frequency was determined to be less than the screening threshold.

Fire scenarios that were not screened out during the quantitative screening are screened in for more detailed analysis. At this stage, the conditional core damage probability is revisited to obtain the best estimate for the severe core damage frequency. In the screening analysis, it is conservatively assumed that the fire will cause the worst possible consequence. In the detailed analysis, the fire-induced failure mode is reviewed and the actual failure mode due to the fire is considered. Also, depending on the results of the detailed fire modeling analysis, fire suppression probabilities were refined to obtain different estimates. Then the event tree developed for the internal events is modified, if necessary, to reflect the changes in the fire-induced damage.

6.3.4.3.1.1 Fire Event Progression

The detailed fire analysis is performed for each scenario by modifying an event tree created for Level 1 internal events. Each fire scenario event tree is created by identifying the systems that are unavailable as a result of the fire. For each fire scenario, a case file listing all components affected by the fire is created based on the cable routing information. All devices in this list are assumed to be unavailable due to fire or actuated spuriously as a result of the fire depending on the respective failure mode affecting the mitigation function. To identify an initiating event which best describes the fire scenario, the devices listed in the case file are made unavailable in the master fault tree for the Level 1 internal events and then all the tops in the tree are inspected. When the fire fails a mitigating or support system, which itself is an initiating event, accident sequence quantification is performed using the event tree pertaining to that initiating event. If, however, system failures do not result in an initiating event, detailed analysis is performed using the general transient event tree.

6.3.4.4 Level 2 Internal Fire PSA

The purpose of Level 2 internal fire PSA is to evaluate the external releases associated with at-power internal fire events, which is similar to that used for Level 2 internal events PSA. For large external releases, the Level 1 internal fire sequences leading to PDS1 and PDS2 are grouped, severe accident analysis is performed, accident progression event trees are developed, the containment envelope is defined, and then the event tree sequences are evaluated to determine the frequencies of all applicable external release categories. Level 1 sequences resulting in PDS0 (involving a rapid loss of core structural integrity due to failure tripping the reactor when required) contribute directly to large external plant releases.

6.3.5 Internal Flood PSA

Only flooding events within the plant are considered for the internal flood PSA as external flooding hazards have been screened out for further detailed analysis as discussed in *Sections 4.0* and *5.0*. Internal floods are defined as those events that result from the failure of the components that contain water, or water spills through incorrect operation of systems and/or components within the plant. Such a flood may occur due to the rupture or cracking of piping or vessel containing fluids, leakage past the gland or seal of a fluid system component that is incorrectly assembled or left in an open state following maintenance, or other causes such as spurious actuation of the firewater system. The flood events are of particular concern, because they are "common cause" initiators. In other words, the event itself can fail redundant components and systems, and thereby reduce the number of mitigating systems that are available to bring the plant to a safe and stable state.

An internal flood may potentially lead to severe core damage by first causing the failure of the systems that maintain the heat sinks, and then by contributing to failures of engineered systems that are designed to mitigate such events. In evaluating the flooding induced severe core damage frequency, the probability of coincident random equipment failures is considered, in addition to the initial damage caused by the flood itself.

Much of the methodology for quantifying the severe core damage frequency due to internal floods is similar to that for internal fires. The major tasks of the flood analysis are as follows:

- Collection of plant information required for flooding analysis as part of the flood walkdown
- Establish postulated flooding scenarios
- Qualitative screening analysis
- Quantitative screening analysis
- Detailed analysis of the potentially significant flooding sources and scenarios that are identified in the screening analysis

The internal flood PSA addresses Level 1 by evaluating flood-induced severe core damage and Level 2 by evaluating flood-induced external plant releases.

6.3.5.1 Identification of Plant Characteristics

The plant information that is required for the analysis includes the location of major flood sources, major piping, major equipment for safe shutdown, any potential flood barriers for preventing propagation, and the location of electrical and instrumentation equipment that may be affected by water. The information is collected mainly by review of documents and drawings.

The flood walkdown is conducted once the information for the internal flood PSA is collected by review of drawings and documents. The objectives of the plant walkdown are:

- to confirm the information already collected from documents/drawings,
- to collect additional information that could not be easily obtained from documents/drawings, and
- To help answer any questions that might have arisen in the review of the documentation.

From a plant walkdown, the analyst can gather information to determine if there are additional potential flooding sources that are not identifiable from plant drawings alone.

Information including flooding sources, pipe sizes, drainage features, equipment heights above floor level and general room or area information can be recorded in the walkdown checklist. The flood walkdown for these areas was initially performed in accordance with a walkdown plan. An updated flood walkdown was performed in each area considered by the postulated flood scenarios which could not be screened out to validate the assumptions of the case model. In addition, some pipe rupture frequency estimates were updated based on the most recent sources of information.

6.3.5.2 Determination of Flood Scenarios

The first step of the flooding analysis is to define flood areas by dividing the plant into physically separate areas where a flood area is generally viewed as independent of other areas in terms of flooding effects and flood propagation. An area is termed “independent” if flooding outside the area cannot intrude into the area without failure of an enclosing flood barrier. Having collected and compiled the necessary information, hazard scenarios for each flood area were constructed, considering the worst case impact on equipment in the area in order to calculate the respective flood frequencies, flooding flows rates, floodable volumes and flood levels.

6.3.5.2.1 Screening

There are two levels of screening in the internal flood PSA: qualitative and quantitative screening.

The qualitative screening analysis is to screen out flood areas from further analysis if they do not contain any susceptible equipment for safe shutdown, or if they do not contain any equipment that, if damaged, would lead to an initiating event. Also, flooding sources that do not have enough capacity to damage safe shutdown equipment or to lead to an internal event are screened out in this stage of the analysis.

The quantitative screening analysis is performed to screen out further areas based on the quantitative screening criteria of $1x10^{-7}$ events per year. In this step, the flood frequency for each flood area is estimated using conservative assumptions, bounding flood scenarios are developed, and the conditional core damage probability for the flooding scenarios is estimated. The severe core damage frequency is calculated by multiplying the frequency of sequence ending in a particular flood damage state by the conditional core damage probability. If the result is less than the screening threshold, then the flood scenario may be screened from further analysis.

6.3.5.3 Level 1 Internal Flood PSA

The areas addressed in the Level 1 internal flood PSA are the reactor building, service building, turbine building, and other miscellaneous buildings such as secondary control area, condenser cooling water building, emergency core cooling building, and on-site freshwater pump house.

6.3.5.3.1 At-Power State

The internal flood PSA assesses flooding events that could occur at power. It is assumed that in the event of any flood, the reactor is tripped and the plant is shutdown. Also, the analysis does not consider the plausible degradation of some mitigation functions as a result of the flood and the consequential impact if the plant remains at power, following a flood event.

6.3.5.3.1.1 Flood Event Progression

The detailed analysis deals specifically with the potential significant flooding sources and scenarios that remain after the screening analysis. The flooding frequency can be recalculated based on plant-specific data, and the impact of intermediate flooding growth stages within each area are assessed together with a more realistic evaluation of the capability of flooding damage to spread to adjacent areas. Local operator recovery actions, which are performed in areas that are not affected by flood, are credited. The potential that the flood could be also terminated due to its own effects (flooding can fail the very pumps that feed the flow) would be also accounted. Considering all the above factors, the detailed flood scenarios are developed, the flood-induced damage conditions are determined, and the conditional core damage probabilities for the flood-induced conditions are estimated. The severe core damage frequency for the flooding scenario is determined through multiplying the specific flood scenario frequency by the conditional core damage probability.

6.3.5.4 Level 2 Internal Flood PSA

The purpose of Level 2 internal flood PSA is to evaluate the external releases associated with internal flood events, which follows a similar approach as for Level 2 internal events PSA. For large external releases, the Level 1 internal flood sequences leading to PDS1 and PDS2 are grouped, severe accident analysis is performed, accident progression event trees are developed, the containment envelope is defined, and then the event tree sequences are evaluated to determine the frequencies of all applicable external release categories. Level 1 sequences resulting in PDS0 (involving a rapid loss of core structural integrity due to failure tripping the reactor when required) contribute directly to large external plant releases. However, the results from Level 1 were such that performing a Level 2 internal events PSA was unnecessary. The Level 1 severe core damage frequency was conservatively assumed to lead completely to large release.

6.4 Seismic PSA

Typically, the seismic strength for all structures and equipment that could terminate accident progression or mitigate the consequences of a postulated accident is evaluated. This included both Group 1 and Group 2 structures and equipment for the PSA-based seismic margin assessment work completed in 2008. However, for the most recent work to meet commitments to the Canadian Nuclear Safety Commission, the seismic PSA did not credit Group 1 equipment, which results in an overestimation of quantified plant risk. Provided that safety goals were met, this was deemed an acceptable approach with the intent to add Group 1 structures and equipment later to the seismic PSA in a subsequent update subject to benefit cost considerations.

6.4 Seismic PSA, Continued

The seismic PSA for Point Lepreau Nuclear Generating Station provides a measure of seismic risk by estimating the severe core damage frequency and large release frequency resulting from seismic initiators. These seismic-induced risk metrics are obtained from the seismic PSA by integrating the seismic hazard curve (see **Figure 11**), seismic capacities of structure, system, and components, and the plant response. The seismic PSA work reflects seismic PSA international guidelines, best industry practices and the most recent hazard information (See *Section 4.2.6)* for the Point Lepreau site.

The major steps of the seismic PSA are:

- Development of seismic hazard curves at the foundation levels of safety-related structures based on the seismic hazard assessment described in *Section 4.2*
- Collect and review seismic design guide, design criteria, seismic analysis reports, flow sheets, arrangement drawing and other design documents and drawing
- Review the internal events PSA for applicability to seismic PSA
- Develop the safe shutdown equipment list to identify structures, systems and components for fragility analysis
- Perform seismic capability walkdown and screen out seismically rugged structures, systems and components in accordance with the Electric Power Research Institute methodology shown in NP-6041-SL [23]
- Develop floor response spectra and structural response
- Perform fragility analysis for selected structures, systems and components which were not screened out from the seismic walkdown
- Perform failure mode and effects analysis for those structures, systems and components that have a seismic capacity less than the screening capacity
- Establish seismic initiating events
- Perform relay chatter analysis
- Develop the plant seismic PSA model
- Perform seismic accident sequence quantification

6.4.1 Seismic Hazard Curves

The foundation input response spectra utilized as an input to fragility analysis, and the seismic hazard corves used for convolution to produce frequency-based risk estimates, are discussed in *Section 4.2.6* and provided in **Figure 11**.

As part of this step, the potential for soil-structure interaction, soil liquefaction, slope stability, and damage to buried pipelines and structures have been assessed early in the process of developing the seismic PSA.

Typically, nuclear power plants have been sited such that there was a remote possibility of soil liquefaction. Liquefaction is expected to occur under the following conditions:

- During high energy ground motion, pore water pressures may build up in saturated cohesion less deposits
- If the amplitude and duration of shaking are sufficiently large, the pore water pressure can equal to the confining pressure resulting in the loss of the shear strength of the soil
- In this condition, water flows to the surface forming springs, sand boils, and ground cracks
- Buildings may sink with large differential settlement, and massive landslides may be initiated.

The phenomenon of soil liquefaction is not applicable to Point Lepreau Nuclear Generating Station. The envelope of the Point Lepreau Nuclear Generating Station is founded on competent rock.

6.4.2 Plant Design Information

PSAs are broad, integrated studies that require a considerable amount of information related to the plant design, analysis and operation. This applies to internal events PSA or external events analyses. The seismic PSA requires additional work that involves the seismic capacity analysis of structures and components. To assess the seismic capacity of the plant, the seismic design philosophy needs to be understood. This information is available in safety and engineering design guides, and in seismic Canadian Standards documents.

A significant amount of information is required from almost every discipline that is responsible for the design and the operation of the plants, which has been factored into the seismic PSA modeling and assessment.

6.4.3 Review of Internal Events PSA for Applicability to Seismic PSA

As part of this intermediate step, the internal events PSA was reviewed to identify any potential seismic-induced initiating events and to modify the internal events PSA event trees and fault trees as necessary. The preliminary safe shut down equipment list was also developed but not limited to the mitigating systems and components credited in the internal events PSA.

6.4.4 Safe Shutdown Equipment List

The preliminary set of safe shut down equipment includes but is not limited to the mitigating systems equipment in which failure may lead to severe core damage for the Level 1 internal events PSA and a large radiological release for Level 2 internal events PSA.

The internal events PSA fault trees do not provide a complete list of equipment for the seismic PSA and structural items must be added to the safety shutdown equipment list, e.g., electrical panels and cabinets, instrument racks, masonry walls, and buildings etc. Structures containing equipment relevant to PSA must be identified. For each safety function, the safety system(s) must be identified and then the equipment necessary is listed. These additional structural items are added to ensure that the safe shutdown equipment list is comprehensive and fully supports detailed analysis in the seismic PSA.

6.4.5 Seismic Walkdown

To determine the seismic susceptibility of the components on the safety shutdown equipment list, a seismic walkdown is performed. Walkdowns have been performed at the Point Lepreau site as part of the original PSA-based seismic margin assessment work done in support of plant refurbishment, with more recent walkdowns post refurbishment, as part of the updated PSA submission. The results and insights/findings from the last walkdown were used to update the safe shutdown equipment list in support of the seismic PSA work. The seismic walkdown also included consideration of concerns related to seismic-induced internal fires and seismic-induced internal floods.

6.4.5 Seismic Walkdown, Continued

The purpose of the seismic walkdown is to perform the following:

- Screen seismically rugged components from the safe shutdown equipment list, i.e., based on the latest seismic demand (see *Section 4.2.6*). As per the foundation input response spectra (**Figure 9**) the screening criteria has remained unchanged at 0.3g high confidence low probability of failure (HCLPF) for non-seismically qualified structures, systems and components, and at 0.5g HCLPF for seismically qualified structures, systems and components. However, in accordance with EPRI NP-6041-SL [27], to better describe the potential damage using a ground-motion parameter, the response spectrum limits (i.e., < 0.8g, 0.8-1.2 g and > 1.2g) were also utilized for screening, which are consistent with the PGA limits in NUREG/CR-4334 [30]. The screening criteria are presented in **Table 8**;
- Identify equipment or structures that are not included in the safe shutdown equipment list but its structural failure may impact the nearby safety shutdown equipment list items (i.e., seismic interaction concerns);
- Define failure modes (e.g., functionality, structural integrity, or anchorage failure) of the safe shutdown equipment list items that are not screened and the type of further evaluation required; and,
- Address issues of seismic induced fire, seismic induced flooding, and actuation of fire suppression systems. The safe shutdown equipment list includes equipment items for seismic/fire interaction and seismic/flooding interaction.

The items that could not be screened out during the walkdown were recommended for detailed fragility analysis (i.e. seismic capacity estimation).

6.4.6 Seismic Response Characterization

As discussed in *Section 4.2*, the seismic vibration from an earthquake—at some depth below the plant in the hard rock—are predicted by the seismic hazard assessment and is represented as uniform hazard response spectra (see **Figure 5**). To better understand the impact the earthquake may have on buildings at Point Lepreau Nuclear Generating Station, the seismic vibrations are propagated upwards (see *Section 4.2.6)* through the rock as soil layers into the foundations, which is represented as foundation input response spectra (see **Figure 8**). However, in reality those seismic vibrations will move upwards through the various floors of the building and the higher the elevation, the higher the magnitude of the seismic vibrations. The response of the buildings at each floor level is represented by additional curves referred to as floor response spectra (see **Figure 12** for an example), which can then be used as an input to the seismic strength, or fragility analysis.

6.4.7 Fragility Analysis

The fragility of a structure, system or component is defined as the conditional probability of failure for a given seismic input motion or response parameter, e.g., spectral acceleration at natural frequency. The structure, system or component response to the seismic force exerted upon it is normally represented as a curve showing the dependency of the failure probability function on the spectral acceleration. This curve is defined as a fragility curve. **Figure 33** shows a typical fragility curve.

The objective of the fragility evaluation is to estimate the spectral acceleration capacity of a given piece of equipment or structure.

There are two aspects to the calculation of fragilities:

- The definition of the failure of the SSC
- The determination of the seismic capacity. Components may have more than one failure mode, and each mode should be considered in the analysis. Therefore, there may be more than one fragility curve for a particular component, wherever different failure modes are possible. However, for the purposes of this methodology when components have more than one failure modes only the bounding failure mode will be analyzed.

For equipment, failure denotes the inability of the equipment to perform its safety function.

Fragility analysis has been performed following the latest international guidance and practice.

6.4.8 Seismic Induced Initiating Event Assessment

An assessment was performed to review the impacts of the seismic induced failures of the structures and components on plant safety and determines whether the seismic-induced failures should be considered as initiating events or reflected in the seismic fault trees. The results of the assessment are used as inputs for the development of seismic event trees and seismic fault trees. In seismic fault tree, these new seismic basic events are positioned in the fault tree such that their failure would be similar to that of the random failure basic events of affected components.

6.4.9 Relay Chatter Analysis

One of the concerns in the seismic assessment is that the equipment of concern can be unavailable or spuriously actuated due to the relay chatter, affecting the availability of the safety systems that are required to respond to the seismic induced events. The undesired equipment operations caused by seismically induced relay chatter are:

(a) Inadvertent actuation: undesired valve opening/closing, pump starting/stopping, breaker opening/closing or other actuation caused by relay contact chatter.
(b) Failure to actuate – failure of breaker to open/close, valve to open/close, or other device to actuate upon demand. Undesired relay seal in and lockout functions are included in this mode.

Each of these failure modes is required to be considered when evaluating the potential effects of contact chatter.

The relay chatter analysis is 1) to identify essential relays related to the PSA credited component, 2) to screen out relays in terms of generic seismic capacity of the relays and/or function of the relays, 3) to estimate seismic capacity of relays, and 4) to provide inputs about the effects of relay chatters with potential recovery actions to the seismic plant modelling.

6.4.10 Seismic Event Progression

Seismic event trees are used to perform accident sequence quantification. The methodology for developing seismic event trees is somewhat different from that of the internal events PSA. The internal events PSA considers many initiating events. Each initiating event leads to one of a number of possible consequences represented in the event tree. Top events in the event tree correspond to short-term availability and long term reliability of mitigating systems and operator actions.

In contrast, the seismic PSA considers only one seismic initiating event - the earthquake. Initially, a primary seismic event tree is developed, which postulates different seismic event amplitudes and attributes a consequential internal initiating event to each one. Then secondary seismic event trees, which contain random failures of systems, seismic-induced failures or combinations of both, are developed to detail the mitigation scenario with the available systems following the postulated seismic event.

6.4.10.1 Primary Seismic Event Tree

The first event tree is the primary seismic event tree containing seismically induced failures of structures, systems and components which can lead directly to severe core damage or to some seismically-induced initiating events. The essential purpose of this primary event tree is to determine seismic-induced initiating events. A seismically induced initiating event refers to the plant failures caused by the seismic motion. The event order in the seismic initiating event trees depends on the results of the seismic capability of the systems. The most critical failures are put at the front of the seismic event tree. The top events of the primary seismic event tree consist of potential seismically induced failures.

6.4.10.2 Secondary Seismic Event Trees

The secondary seismic event trees are to delineate the plant behaviour after the seismic initiators. The secondary event trees are developed by modifying the PSA internal event trees to reflect the seismic-induced conditions. The headings in the secondary event trees represent a failure of a system due to the seismic induced failures, random failures or combinations of both.

6.4.10.3 Seismic Fault Trees

For the mitigating systems identified from the secondary seismic event trees, seismic fault trees have been developed by modifying the internal event master fault tree. The functional or structural seismic-induced failures of components are added into the master fault tree nearby the random failure of the components.

6.4.11 Seismic Accident Sequence Quantification

Quantification of a seismic PSA involves the convolution of the seismic hazard curve from **Figure 11** with the fragility curves in the seismic PSA model to estimate the contribution to the frequency of severe core damage or large radiological release as a result of those events. Therefore, the seismic PSA outcomes provide an estimate of severe core damage frequency (Level 1) and large release frequency (Level 2), which can then be compared to acceptance criteria or safety goals.

6.4.11 Seismic Accident Sequence Quantification, Continued

To mathematically convolve the seismic hazard curve, it is divided into discrete intervals referred to as bins (see **Figure 34** for a representation of the concept). The frequency of each bin is the difference of the mean annual frequency of exceedance for each end of the peak ground accelerations represented by the bin. In total seven intervals were used to represent the different seismic hazards as shown in **Table 9**. These intervals are the initiating events for the seismic PSA. Fragilities for structures, systems and components are calculated specifically for each interval and then the corresponding probability is used in the seismic PSA model. A different set of seismic events (i.e. fragility events) and associated accident sequence logic are developed and quantified for each interval, and then the sequence frequencies for each interval are combined.

6.5 All-Hazard Model Integration

At Point Lepreau Nuclear Generating Station, each hazard PSA is integrated into a single model for the purpose of importance analysis, uncertainty analysis and sensitivity analysis. In this manner, all hazards are considered when deriving additional insights from this work.

6.5.1 Importance Analysis

Importance analysis is performed to identify systems and component that are important to overall plant severe core damage frequency and large release frequency. Importance analysis is performed to identify the dominant contributors to those risk metrics. In accordance with the guidance in regulatory document REGDOC-2.4.2 [24], for security reasons dominant contributors, specific vulnerabilities and associated event sequences are not included in this report.

6.5.2 Uncertainty Analysis

Since the PSA model attempts to simulate reality, it is inevitable that there will be simplifying assumptions and idealizations of rather complex processes and phenomena. These simplifications and idealizations will generate uncertainties. There are three major categories of sources of uncertainties in these models:

1. Completeness
2. Modeling adequacy
3. Input parameter uncertainties

Uncertainties can vary widely depending on the hazard being assessed. Typically, the uncertainty associated with internal events is quite low whereas the uncertainty associated with external hazards is quite high particularly for very rare events where there is little historical evidence or data supporting the extrapolation of data to very low frequency of occurrence. The high degree of uncertainty in external hazard assessments is the primary reason that great care needs to be taken in interpreting their results and what insights they provide.

At Point Lepreau Nuclear Generating Station, the uncertainty associated with various hazards PSA is expressed as an “error factor”, which in general terms is defined as the ratio between the 95% confidence value and the 50% confidence or mean value, depending on the source of data, for a particular potential failure event. For seismic events, the error factor is determined from the natural logarithm of the modeling uncertainty at one standard deviation.

6.5.3 Sensitivity Analysis

Sensitivity analysis is used to evaluate the impact on the results of a number of assumptions made in the event tree analysis and fault tree analysis, as well as assumptions impacting the quantification of initiating events, undeveloped events, and human error events. By applying reasonable variations in key parameters and assumptions for both the PSA risk metrics and severe accident analyses, an improved understanding can be gained of the level of conservatism in certain assumptions that may be driving plant risk estimates. Given that sensitivity analysis can identify vulnerable plant configurations or scenarios, the results of sensitivity analysis are not included in this report for security reasons.

7.0 Summary of PSA Results

The Point Lepreau Nuclear Generating Station uses two measures from the Level 1 and Level 2 PSA that can then be compared to safety goals and targets for decision-making purposes such as potential safety improvements (see *Section 6.1* for a full discussion regarding safety goals and their application at Point Lepreau Nuclear Generating Station), namely:

- Frequency of severe core damage
- Frequency of large release

As shown in **Table 6**, the plant damage states (PDS) that lead to severe core damage include PDS0, PDS1 and PDS2, which are summed to provide an overall estimate of the severe core damage frequency.

As shown in **Table 7**, the external plant release categories (EPRC) that have the potential to exceed the large release threshold of $1x10^{14}$ Becquerel (i.e. 100 TBq) of Cs-137 include EPRC0 to EPRC6, which are summed to provide an overall estimate of the large release frequency.

The outcomes of each hazard PSA (internal events at power, internal fires at power, internal floods at power, seismic events at power, internal events while shutdown), each assume that the reactor is in the state analyzed for 100% of the time. As such, it is not appropriate to simply sum the raw at-power PSA results with raw shutdown PSA results because the plant cannot simultaneously be in both plant states at the same time.

There appears to be an international consensus [33] that aggregating risks for the purpose of comparison with site safety goals should include the risks from all hazards, sources of radioactivity and all modes of plant operation. However, there is an equal consensus of concern that has been expressed that:

(a) The simple addition of contributions for disparate risk contributors ignores the widely-varying uncertainty distributions in the results (low uncertainty for internal events versus high uncertainty distributions for external events)
(b) The aggregation of results across different hazards and evaluated with different methodologies of varying maturity and data quality will produce an inappropriate conservative bias such that comparison with safety goals would be dominated by the mathematical treatment of uncertainty rather than the underlying risk levels

7.0 Summary of PSA Results, Continued

As discussed in *Section 6.1.1*, while safety goals are typically applied on a per-reactor/per-hazard basis in support of plant licensing, the Canadian industry is investigating risk aggregation methods in an attempt to address the above concerns. Until an international consensus has been reached on whole-site PSA and all-hazard risk aggregation methods are developed and accepted, simple addition of the hazards is provided where appropriate in the following tables.

Table 11: Aggregated PSA results with the reactor at power.
Table 12: PSA results with the reactor shut down.

In all cases and regardless of how the results are presented, safety goals related to PSA are met for Point Lepreau Nuclear Generating Station.

8.0 Emergency Planning

Although NB Power does not expect a radiation emergency to develop at Point Lepreau Nuclear Generating Station (PLNGS), NB Power and the NB Emergency Measures Organization has prepared comprehensive plans and procedures to deal with the unthinkable and to protect its workers and the public.

The emergency program at PLNGS is governed by:

(a) On-site detailed emergency procedures to be followed by plant staff involving an emergency confined to the facility, and not posing a danger to the general public

(b) The Off-Site Plan – this is a Government of New Brunswick document, held by the New Brunswick Emergency Measures Organization. This plan details procedures to be followed for an emergency incident at Point Lepreau Nuclear Generating Station which could pose danger to the general public, and thus would require a coordinated multi-agency response. This plan would require response activities from a number of Government of New Brunswick departments, as well as external supporting agencies

8.0 Emergency Planning, Continued

While the risk to life or the environment from an accidental major release of radionuclides or other industrial accident is remote, it is in the interest of the public to be prepared to respond, by having in place effective emergency plans to deal with such events. For example, in terms of earthquakes a seismic monitoring system is installed at the plant to detect an earthquake that might affect the plant. If the earthquake is of sufficient magnitude alarms are generated in the main control room. In response to those alarms, the shift supervisor follows the on-site detailed emergency procedure and takes specific action depending on the magnitude of the earthquake, which includes shutting the plant down if the design basis earthquake is exceeded. Restart of reactor would not occur until extensive structural and equipment inspections demonstrate that the plant is safe to return to service. In the very unlikely event that the earthquake results in damage to the reactor core or a threat of radiation release, the New Brunswick Emergency Measures Organization are notified and the off-site plan is activated.

The off-site plan identifies criteria for initiating protective actions to prevent deterministic effects and to minimize stochastic effects as a result of radiological release from Point Lepreau and include:

- Sheltering
- Ingestion of potassium iodide pills (distributed to each resident within 20 kms of the plant)
- Evacuation.

8.1 Emergency Planning Zones

For the purposes of emergency planning, three zones are defined. The precautionary action zone is the area surrounding the plant out to 4 km that should be evacuated promptly in the event of an imminent release. The urgent protective action zone is the area surrounding the plant out to 12 km; protective actions in this area should be based on radiation survey results and plant conditions. The longer-term protective action zone is the remaining area outside the plant to 20 km; protective actions in this area should be based on radiation survey results and plant conditions.

In the outline evacuation plan, it is stated that in the worst scenario, a complete evacuation of the 20 km zone could involve up to 3000 people, 1400 vehicles, 20 large animals and 50 fishing boats. However, a more specific demographic survey was performed in 2011 for the various zones around the plan that are separated by a warden system (see **Table 14**). Twelve of fifteen identified warden zones have been established within the 20 km radius (see **Figure 35**). These zones are based on total road distance and population density parameters that permit coverage within 45 minutes, driving at low speed. There are within the 20 km radius three additional zones, called Zones #13, #14 and #15, consisting mainly of camps and other temporary residences. The Department of Natural Resources is responsible for alerting these three zones.

8.2 Emergency Response Strategy

When an accident occurs, it is very difficult for off-site emergency response organizations to predict if there will be an airborne or liquid release, or how large the release will be. Hence, the initial protective action strategy must rely on very little information and should err on the safe side.

The following initial protective action strategy is recommended in the off-site emergency plan for an airborne release:

- When an accident that could lead to core melt is detected, immediately evacuate or shelter the full precautionary action zone around the station. The action is implemented over the full 360 degrees as a precaution against possible wind shifts
- Immediately dispatch survey teams downwind to monitor ambient radiation levels and air contamination to detect a release
- Once a release is imminent or has been detected, shelter people within the urgent protective action zone downwind from the station. If the wind direction changes, adjust the sectors in which the protective action is implemented
- Conduct environmental radiation surveys within the urgent protective action zone to determine if further protective actions are required
- If readings are high compared with intervention criteria, expand the area surveyed and adjust protective actions where required

Sheltering in place is recommended when the radiation release is predicted to be of a short duration (e.g., less than 6 hours). Sheltering in place for as much as 24 hours may be recommended to allow time to organize an evacuation. Potassium iodide pills should be administered in conjunction with the shelter in place order or if evacuation is to be carried out through a radioactive plume.

9.0 Public Health Risk Estimation

During plant refurbishment, NB Power exceeded the requirements of the Canadian Nuclear Safety Commission for PSA by going a step further and assessing the potential off-site consequences of a highly improbable severe accident. The assessment was later updated considering five representative accident scenarios based on the Level 2 PSA:

- Two postulated cases involving early containment failure due to failure of containment isolation or containment bypass
- One postulated case involving late containment failure (24-72 hours) due to progression of the severe accident
- Two postulated cases selected for plant habitability

9.0 Public Health Risk Estimation, Continued

Four additional cases were assessed to evaluate the effectiveness of using the spent fuel bay as an alternative path for containment venting, in support of severe accident management program.

The consequences of loss of spent fuel storage/reception bay inventory or cooling was considered bounded by the selected cases that lead to severe core damage and large releases.

In essence, the off-site consequence analysis can be viewed as a "limited" Level 3 PSA in the context that potential economic consequences are not considered, and only one dominant sequence from the Level 2 PSA was propagated into the analysis for each of the five representative accident scenarios. Nonetheless, the results can provide useful insights into emergency planning.

The off-site consequence analysis estimates health risks to average individual members of the hypothetical public critical group most at risk due to operations of Point Lepreau Nuclear Generating Station. The critical group is defined as a fairly homogenous group of people whose age, habits and diet cause them to receive radiation doses higher than the average received by the rest of the population living in the same environment.

In carrying out the consequence analysis, very conservative assumptions (i.e. results will show a higher result than reality) were used as follows:

- For the postulated failures above, the entire severe accident source term was released to the environment; the hypothetical critical group that was postulated to be exposed to a radiological release was assumed to reside and work at the same location on the site boundary, 1 km from the center of the reactor
- Contrary to the off-site emergency plan the critical group was not evacuated or sheltered (i.e. shielded) for the first 48 hours after the start of the release
- Plume rise due to buoyancy was ignored
- Air concentrations and dose calculations were performed along the plume centerline
- Infant mortality factors were applied regardless of age of the individual to receive the highest calculated dose
- The calculations for delayed effects were carried out over an assumed 70-year lifespan

9.0 Public Health Risk Estimation, Continued

The off-site public health risks were expressed in terms of individual early fatality risk and individual delayed fatality risk based on expected doses calculated from each representative source term factoring in the atmospheric transport of a release and the resultant inhalation, cloudshine, groundshine and ingestion from ground concentrations. The individual early fatality risk represents the risk of fatality as a result of the exposure to the critical group during the first 48 hours, and the individual delayed fatality risk represents the risk of developing a fatal cancer over the stated 70-year lifetime.

The results of the analysis also include potential for containment leakage at 2.5 times greater than the current leak rate criterion of 1% volume per day (i.e. leakage was assumed at 2.5 % volume per day). The results of the off-site consequence analyses are shown in Table 13**Table 13**.

Note that the delayed fatality calculated risk assumes that the critical group returns after 66 days and, therefore, reflects the risk associated with developing a fatal cancer of the remaining 70-year period.

Typical safety goals that have been used in Canada in the past for multi-unit stations have been one in 1,000,000 years for individual early fatality risk and one in 100,000 years for individual delayed fatality risk. The results for Point Lepreau Nuclear Generating Station meet the safety goals.

10.0 References

[1] International Atomic Energy Agency (IAEA) Safety Fundamentals No. SF-1, “Fundamental Safety Principles”, Vienna (2006).

[2] International Nuclear Safety Advisory Group report, INSAG-10, “Defence in Depth in Nuclear Safety”, International Atomic Energy Agency, Vienna (1996).

[3] Canadian Nuclear Safety Commission (CNSC), INFO-0824, “CNSC Fukushima Task Force Report”, October 2011.

[4] Canadian Nuclear Safety Commission (CNSC) Integrated Action Plan, “On the Lessons Learned from the Fukushima Daiichi Nuclear Accident”, August 2013.

[5] Electric Power Research Institute (EPRI), U.S. Department of Energy (U.S. DOE), and U.S. Nuclear Regulatory Commission (U.S. NRC), 2012, Technical Report: Central and Eastern United States Seismic Source Characterization for Nuclear Facilities.

[6] Leblanc, G., and Burke, K.B.S., 1985, Re-evaluation of the 1817, 1855, 1869, and 1904 Maine–New Brunswick area earthquakes: Earthquake Notes, v. 56, pp. 107-123.

[7] American Society of Mechanical Engineers, ASME/ANS RA-Sa-2009, “Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications”, Addendum A to RA S-2008.

[8] Regulatory Guide 1.200, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities”, US Nuclear Regulatory Commission, March 2009, Revision 2

[9] Twisdale, L.A., et al. (1981). “Tornado Missile Simulation and Design Methodology,” EPRI NP-2005, Volumes 1 and 2, Electric Power Research Institute, Palo Alto, CA.

[10] American Society of Civil Engineers, ASCE 7-10, “Minimum Design Loads for Buildings and Other Structures”, Reston, VA, 2010

[11] US Nuclear Regulatory Commission (USNRC), NUREG/CR-7005, “Technical Basis for Regulatory Guidance on Design-Basis Hurricane Wind Speeds for Nuclear Power Plants”, Draft – November 2011

[12] Atomic Energy Control Board (AECB), Regulatory Guide C-6 (Revision 1), “Safety analysis of CANDU nuclear power plants”, Issued for Public Comments, September 1999

[13] Canadian Nuclear Safety Commission (CNSC) Regulatory Document REGDOC 2.4.1, “Deterministic Safety Analysis”, May 2014

10.0 References, Continued

[14] U.S. Nuclear Regulatory Commission (USNRC), NUREG/CR 2300, "A Guide to the performance of probabilistic risk assessments for nuclear power plants", January 1983

[15] International Atomic Energy Agency (IAEA), TECDOC 1341, "Extreme external events in the design and assessment of nuclear power plants", March 2003

[16] International Atomic Energy Agency (IAEA), TECDOC 1487, "Advanced nuclear plant design options to cope with external events", February 2006.

[17] American Society of Mechanical Engineers (ASME), ASME/ANS RA Sb 2013, "Addenda to ASME/ANS RA S 2008 Standard for level 1 large early release frequency probabilistic risk assessment for nuclear power plants applications", 2013.

[18] International Atomic Energy Agency (IAEA), Safety Standards Series, Specific Safety Guide, SSG-3, "Development and application of level 1 probabilistic safety assessment for nuclear power plants", Vienna 2010.

[19] Kuzmina, Irina, Overview of IAEA's Projects on Safety Goals and Integrated Risk Informed Decision Making", Presentation, 1st Consultants' Meeting on the INPRO Collaborative Project: Review of Innovative Reactor Concepts for Prevention of Severe Accident and Mitigation of their Consequences (RISC), 31 March – 2 April 2014, IAEA, Vienna, Austria.

[20] International Atomic Energy Agency (IAEA), IAEA Safety Standard Series No. GSR Part 4, "Safety Assessment for Facilities and Activities", Vienna, 2009.

[21] OECD Nuclear Energy Agency, "The Structure and Application of High Level Safety Goals, Multinational Design Evaluation Program", Safety Goals Sub- Committee, January 2011.

[22] U.S. Nuclear Regulatory Commission (USNRC), NUREG-2150, "A Proposed Risk Management Regulatory Framework", April 2012.

[23] International Nuclear Safety Advisory Group report, INSAG-12, "Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1", International Atomic Energy Agency, Vienna (1999).

[24] Canadian Nuclear Safety Commission (CNSC) Regulatory Document REGDOC 2.4.2, "Probabilistic Safety Assessment (PSA) for Nuclear Power Plants", May 2014

[25] Canadian Nuclear Safety Commission (CNSC) Regulatory Document REGDOC 2.5.2, "Design of Reactor Facilities: Nuclear Power Plants", May 2014

[26] US Nuclear Regulatory Commission (USNRC), NUREG/CR-6850, "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities", EPRI 1011989, September 2005

10.0 References, Continued

[27] Electric Power Research Institute (EPRI), EPRI NP-6041-SL, Revision 1, "A Methodology for Assessment of Nuclear Power Plant Seismic Margin", Final Report, August 1991.

[28] U.S. Nuclear Regulatory Commission (USNRC), Policy, "Technical and Licensing Issues Pertaining to Revolutionary and Advanced Light Water Reactors (ALWR) Designs", SECY-93-087, April 1993.

[29] U.S. Nuclear Regulatory Commission (USNRC), Final Report, "Procedural and Submittal Guidance for Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities", NUREG-1407, June 1991.

[30] U.S. Nuclear Regulatory Commission (USNRC), NUREG/CR-4334, "An Approach to the Quantification of Seismic Margins in Nuclear Power Plants", UCID-20444, August 1985.

[31] U.S. Nuclear Regulatory Commission (USNRC), NUREG/CR-0098, "Development of Criteria for Seismic Review of Selected Nuclear Power Plants", May 1978.

[32] Leonard, L.J., Rogers, G.C., and Mazzotti, S., 2012, "A preliminary tsunami hazard assessment of the Canadian coastline: Geological Survey of Canada", Open File 7201

[33] J. Vecchiarelli et. al, February 2014, "Development of a Whole-Site PSA Methodology", COG-13-9034 R0

[34] GeoPentech, 2015, Southwestern United States Ground Motion Characterization SSHAC Level 3 – Technical Report Rev. 2, March 2015, 673 pp.

[35] U.S. Nuclear Regulatory Commission (2008). "NRC Regulatory Issue Summary 2008-14: Use of TORMIS Computer Code for Assessment of Tornado Missile Protection," Office of Nuclear Reactor Regulation, Washington, D.C., June 16.

[36] U.S. Nuclear Regulatory Commission (1983). Safety Evaluation Report, "EPRI Topical Reports Concerning Tornado Missile Probabilistic Risk Assessment Methodology," Transmittal Memo dated October 16, 1983, from L.S. Rubenstein, Assistant Director for Core Plant Systems, Division of Systems Integration, to F.J. Miraglia, Assistant Director for Safety Assessment, Division of Systems Integration.

[37] Canadian Standards Association, CSA N289.1-08 (Reaffirmed 2013), "General requirements for seismic design and qualification of CANDU nuclear power plants", September 2014.

Appendix A: Figures

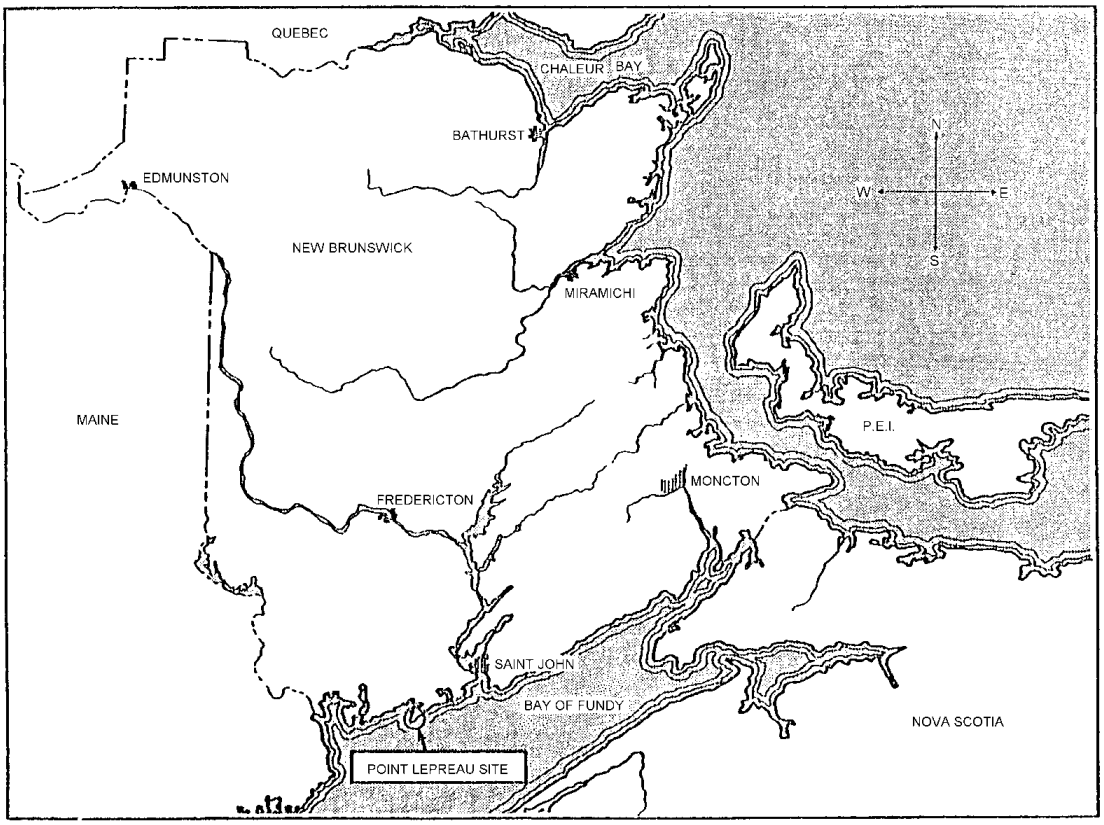


Figure 1: General Location of Site

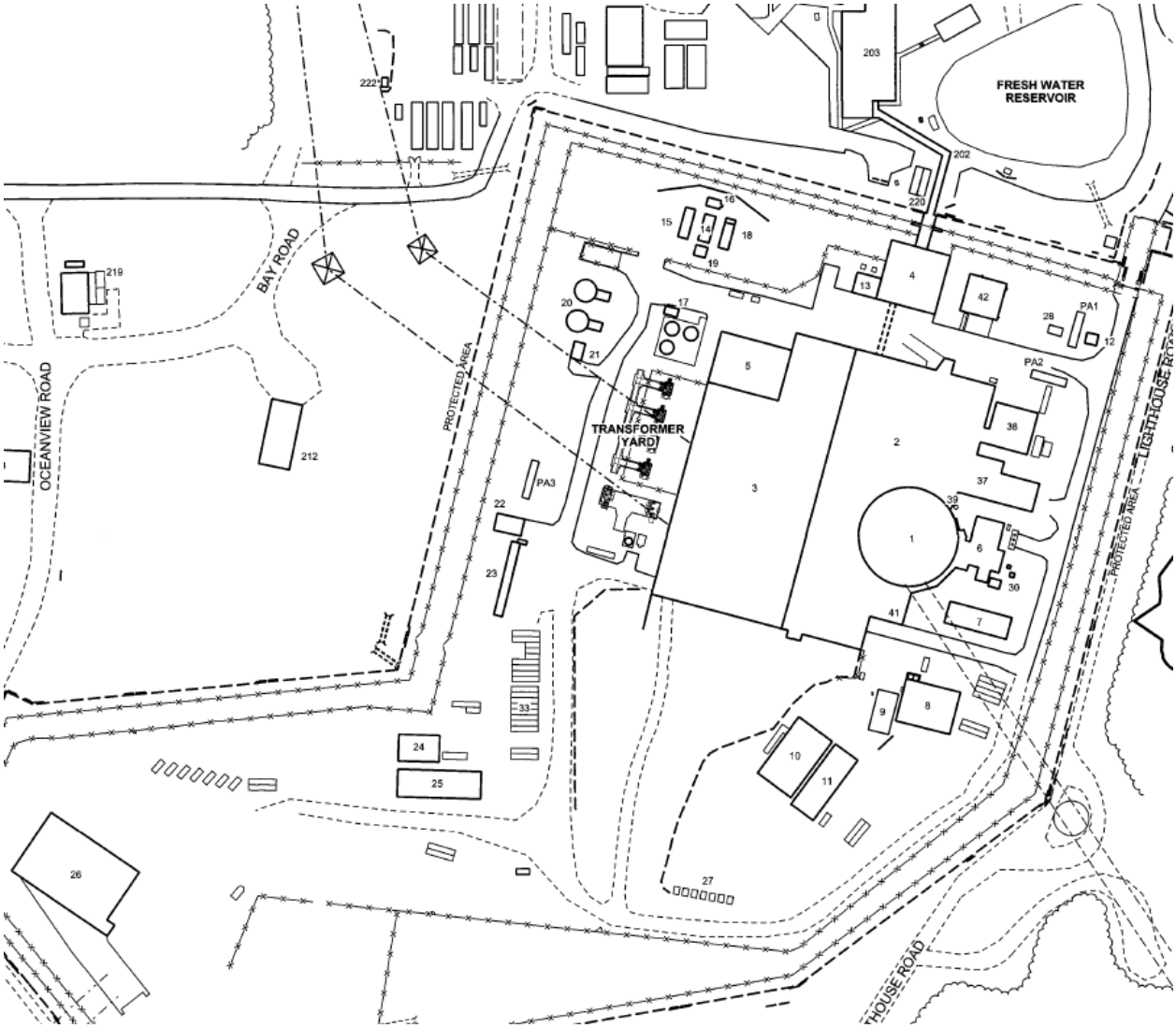


Figure 2: Site Layout

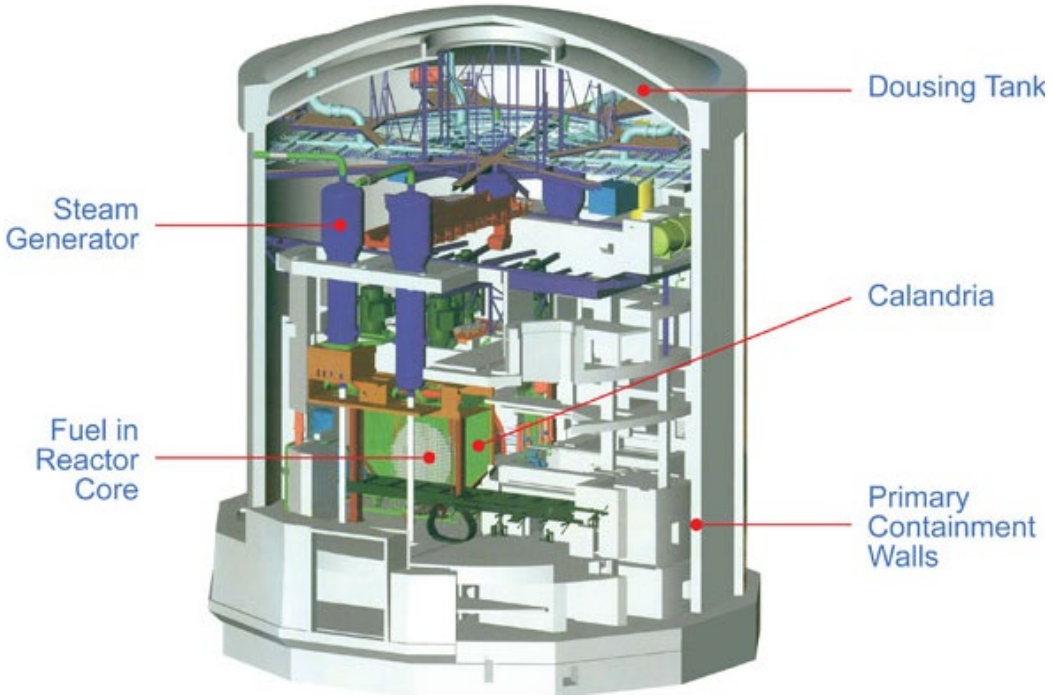


Figure 3: Typical CANDU-6 Reactor Building

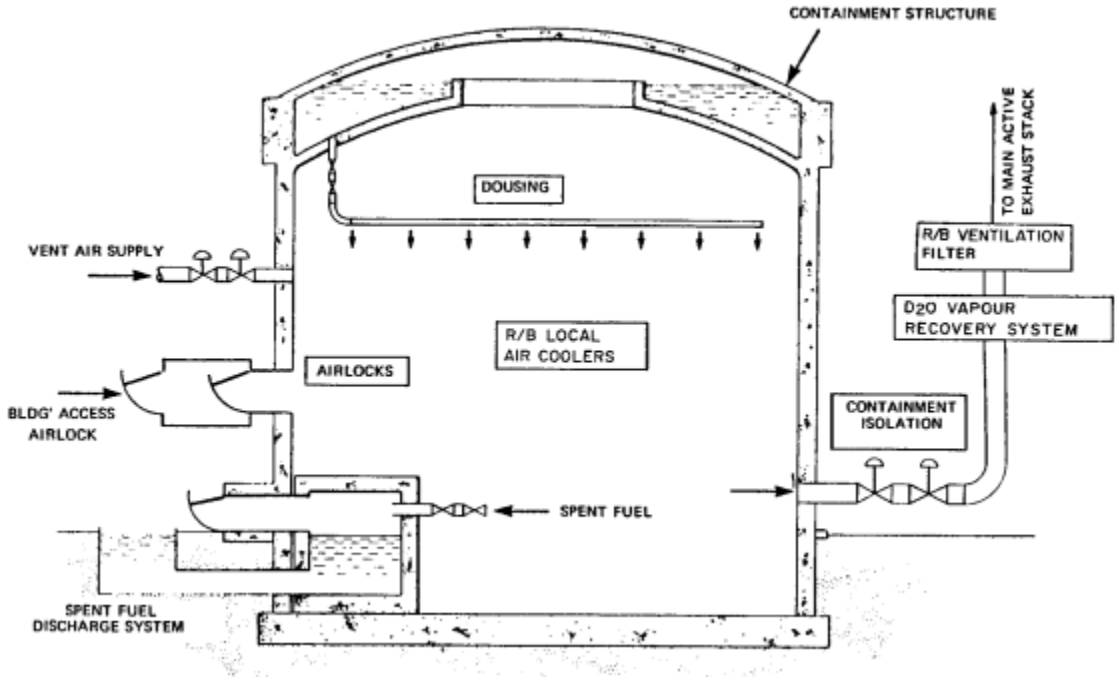


Figure 4: Simplified Diagram of Containment Envelope

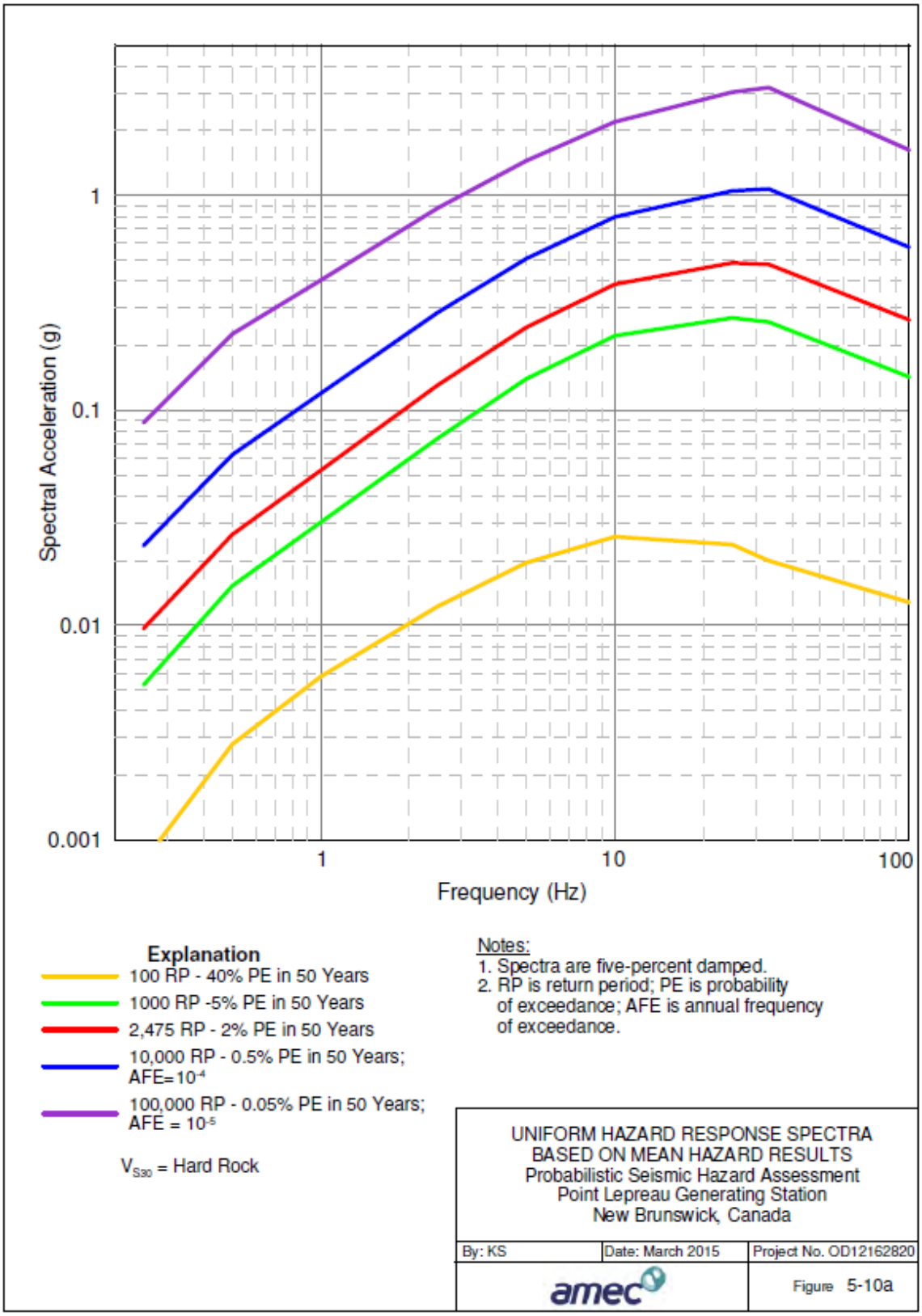


Figure 5: Uniform Hazard Response Spectra in Hard Rock below the Plant

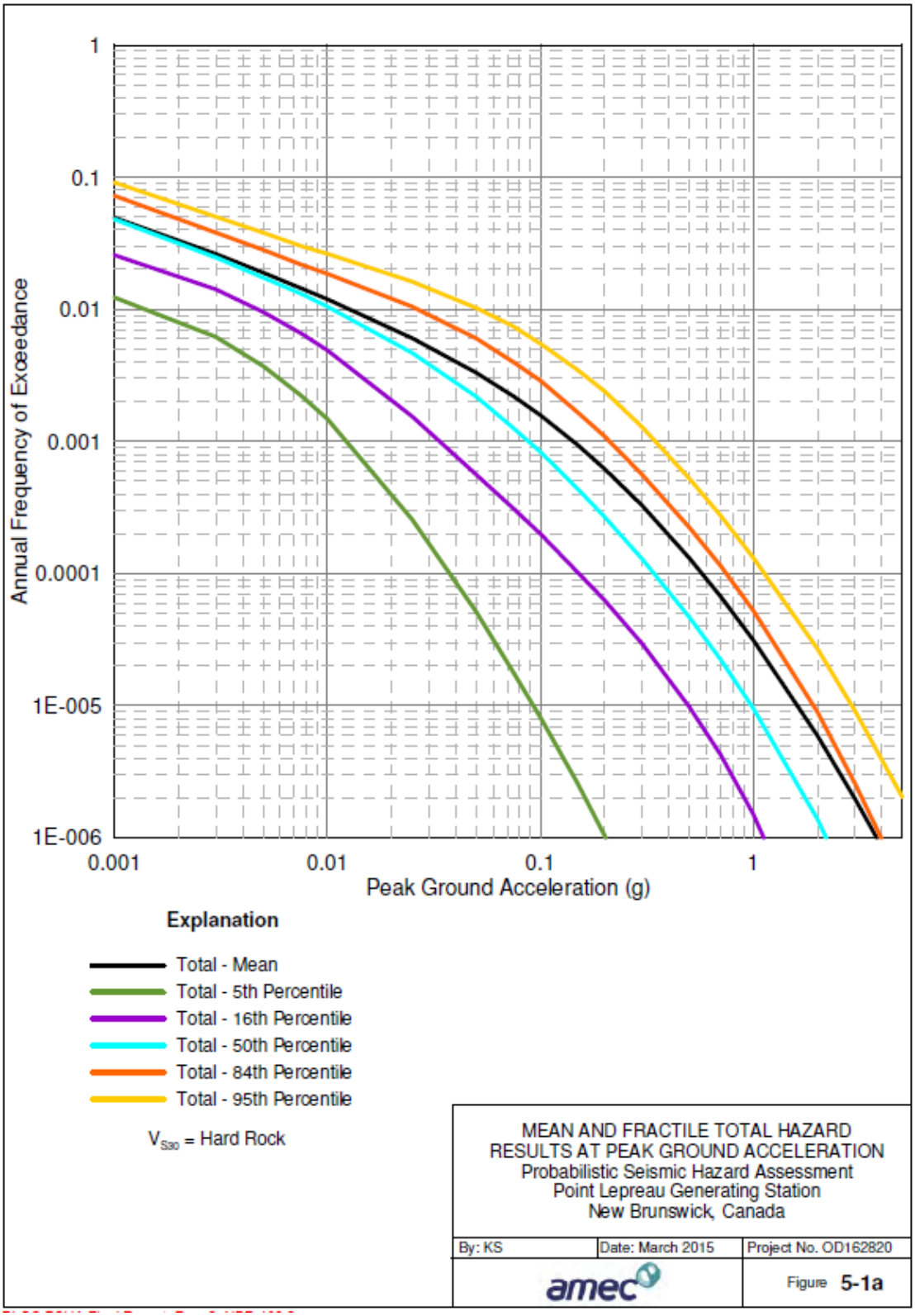


Figure 6: Mean and Fractile Total Hazard Curves in Hard Rock below Point Lepreau Site

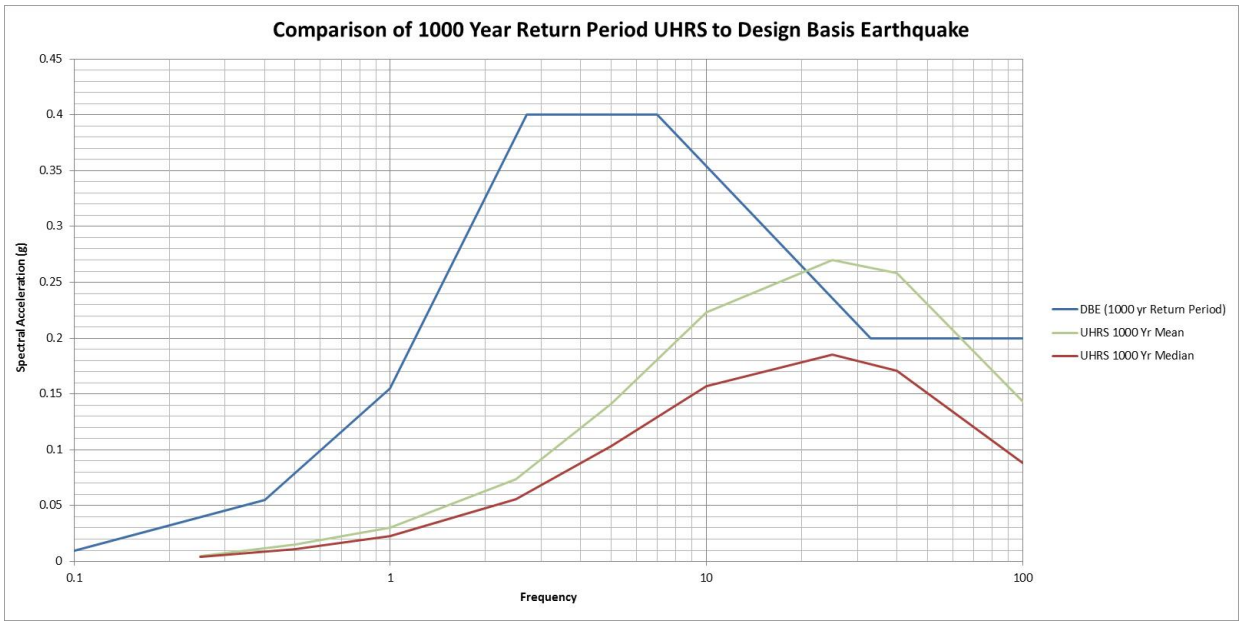


Figure 7: Comparison of 1000-year Return Period Uniform Hazard Response Spectra to PLNGS Design Basis Earthquake

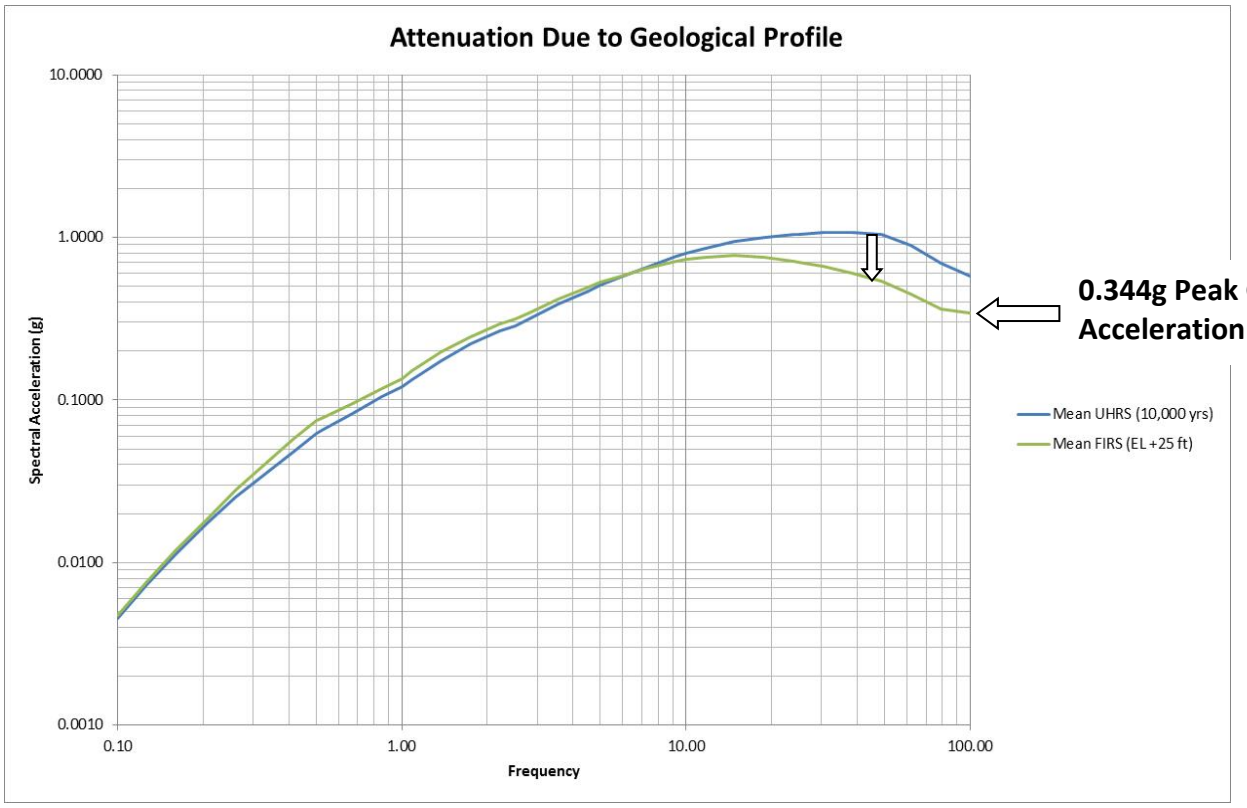


Figure 8: Attenuation of Site Seismic Response Analysis on Uniform Hazard Response Spectra at Building Foundations

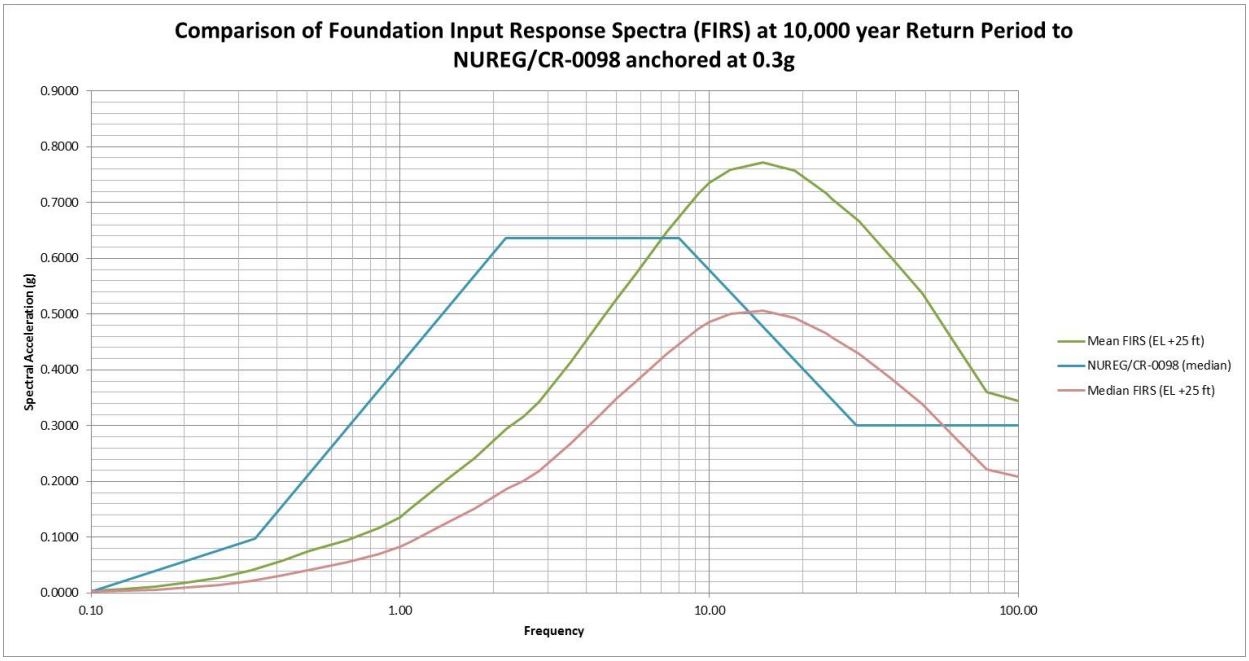


Figure 9: Comparison of Foundation Input Response Spectra (FIRS) at 10,000 year return period versus prior curves used in analysis from NUREG/CR-0098

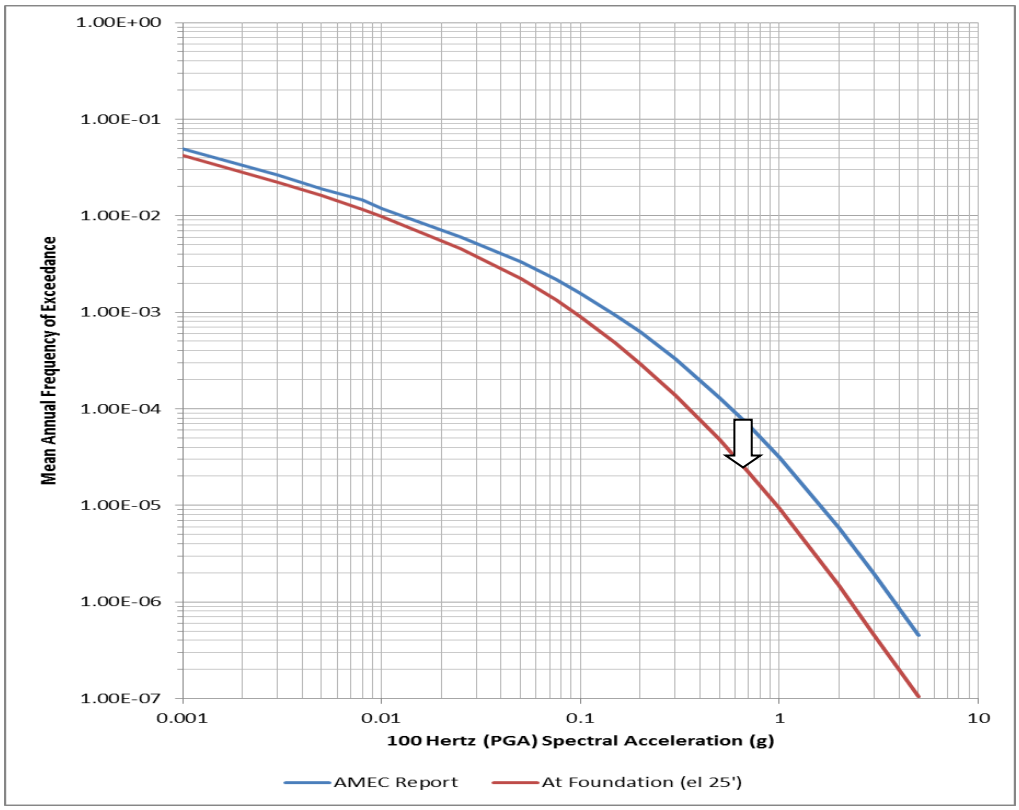


Figure 10: Effect of Site Seismic Response Analysis on Mean Seismic Hazard Curve

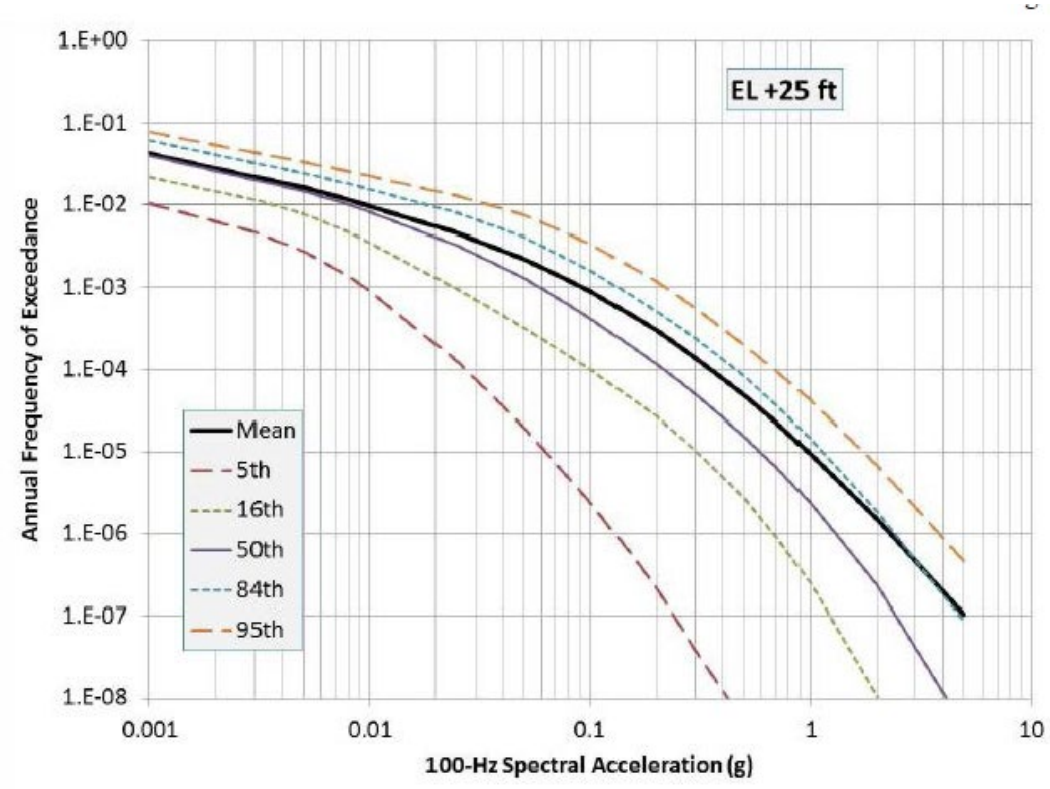


Figure 11: Mean and Fractile Total Hazard Curves at Building Foundations

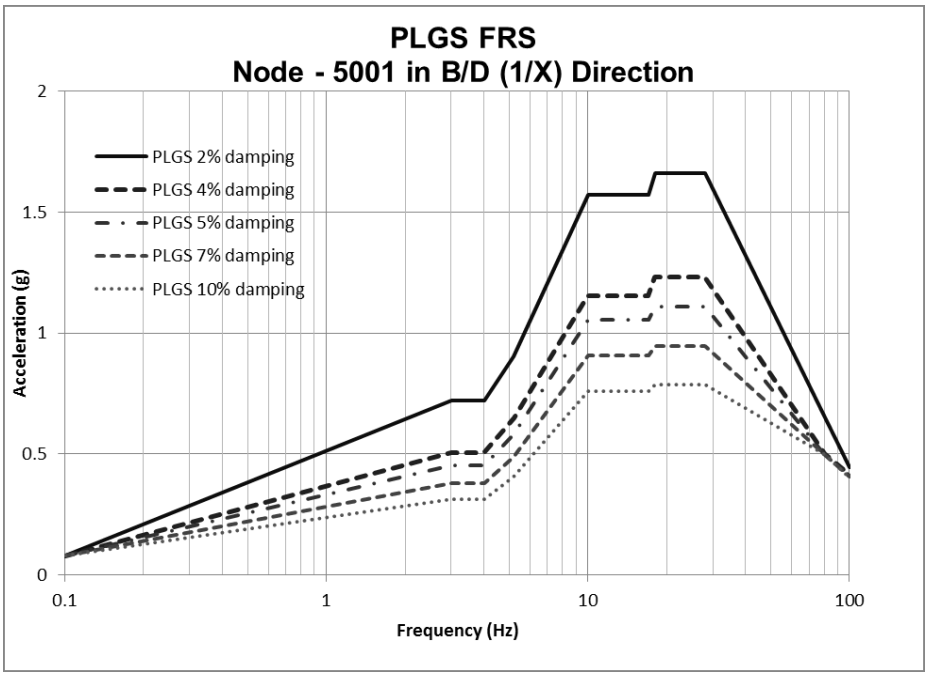


Figure 12: Example of Floor Response Spectra

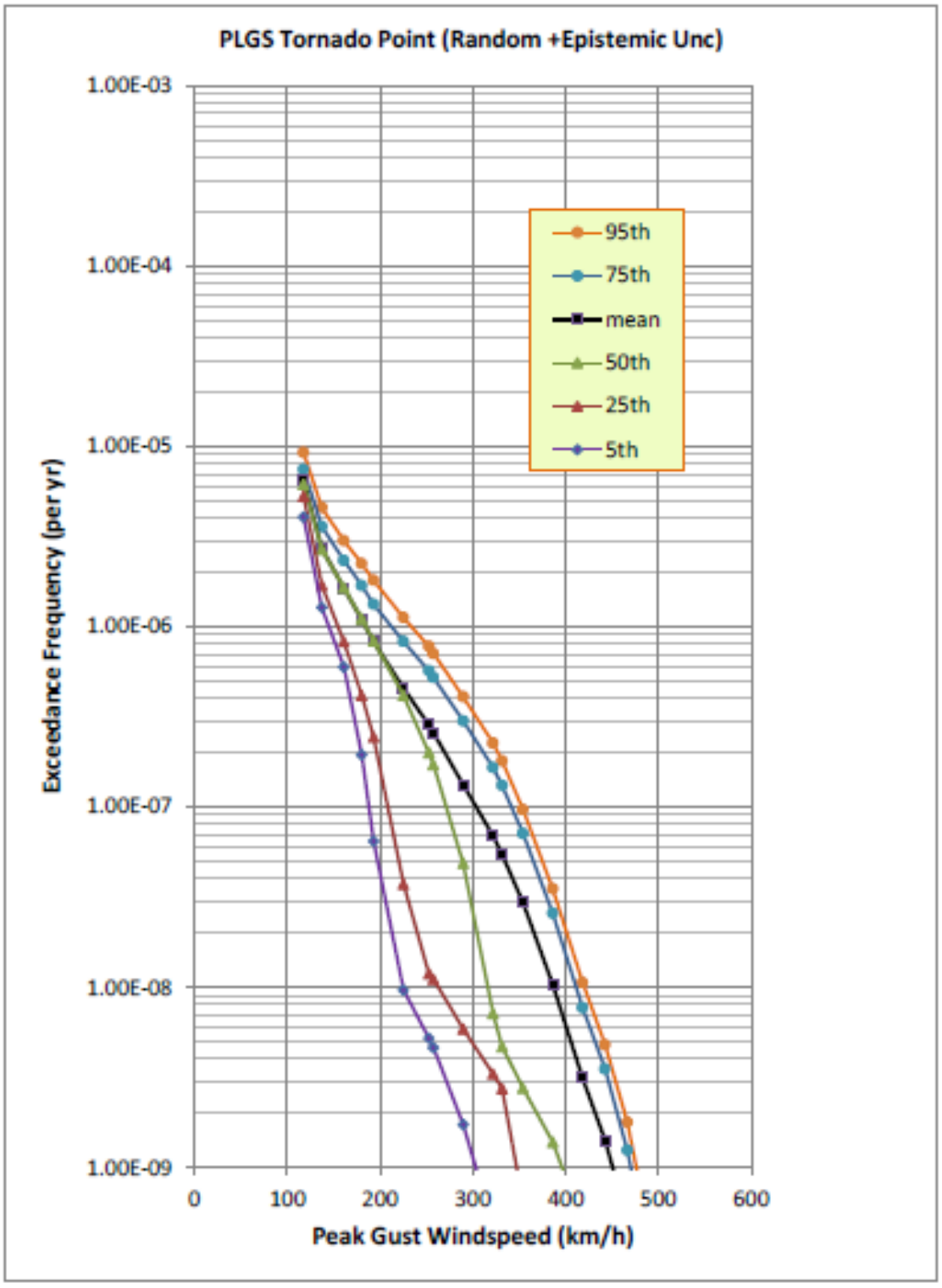


Figure 13: Tornado Point Hazard Curve for Point Lepreau Site

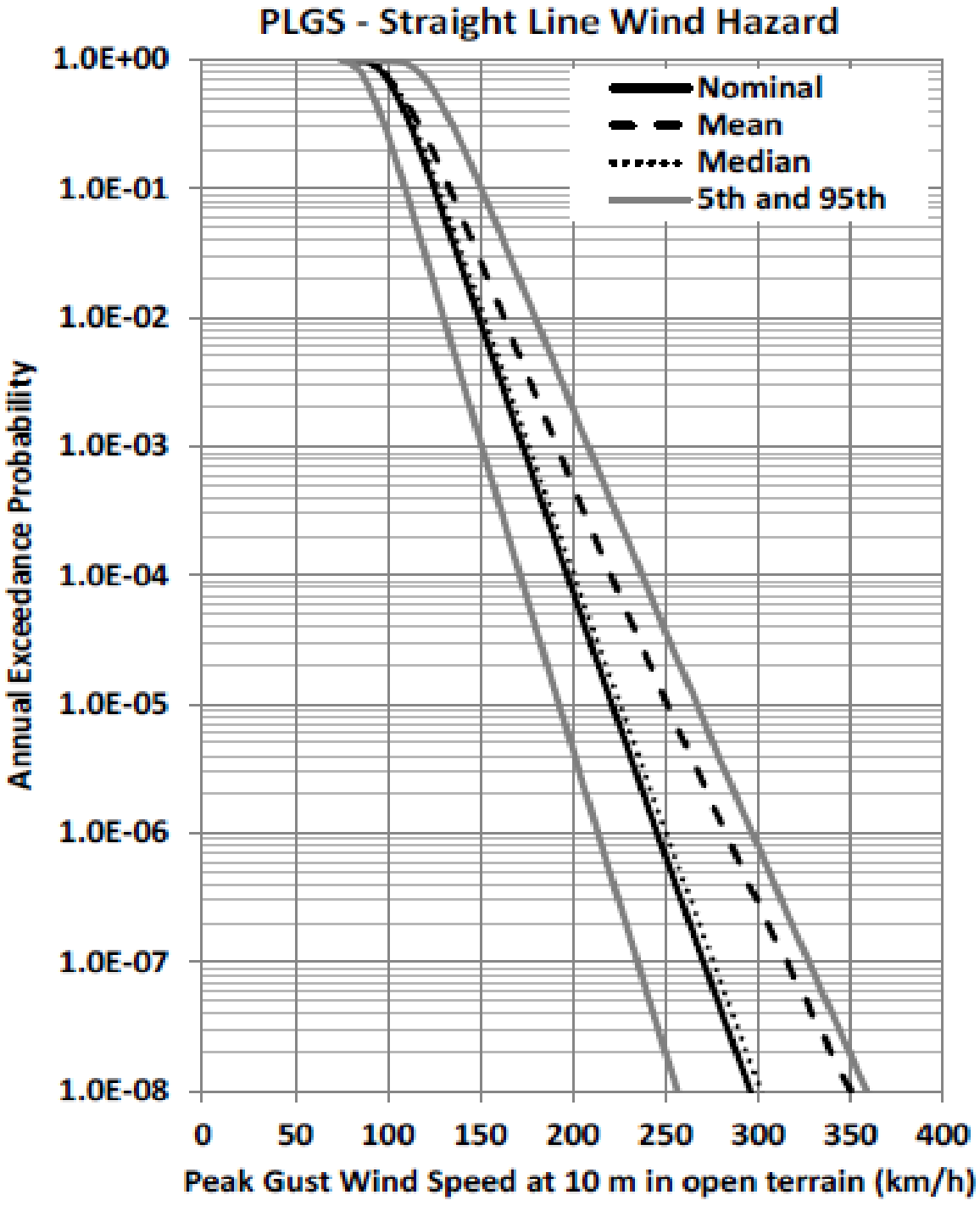


Figure 14: Straight-Line Wind Hazard for Point Lepreau Site

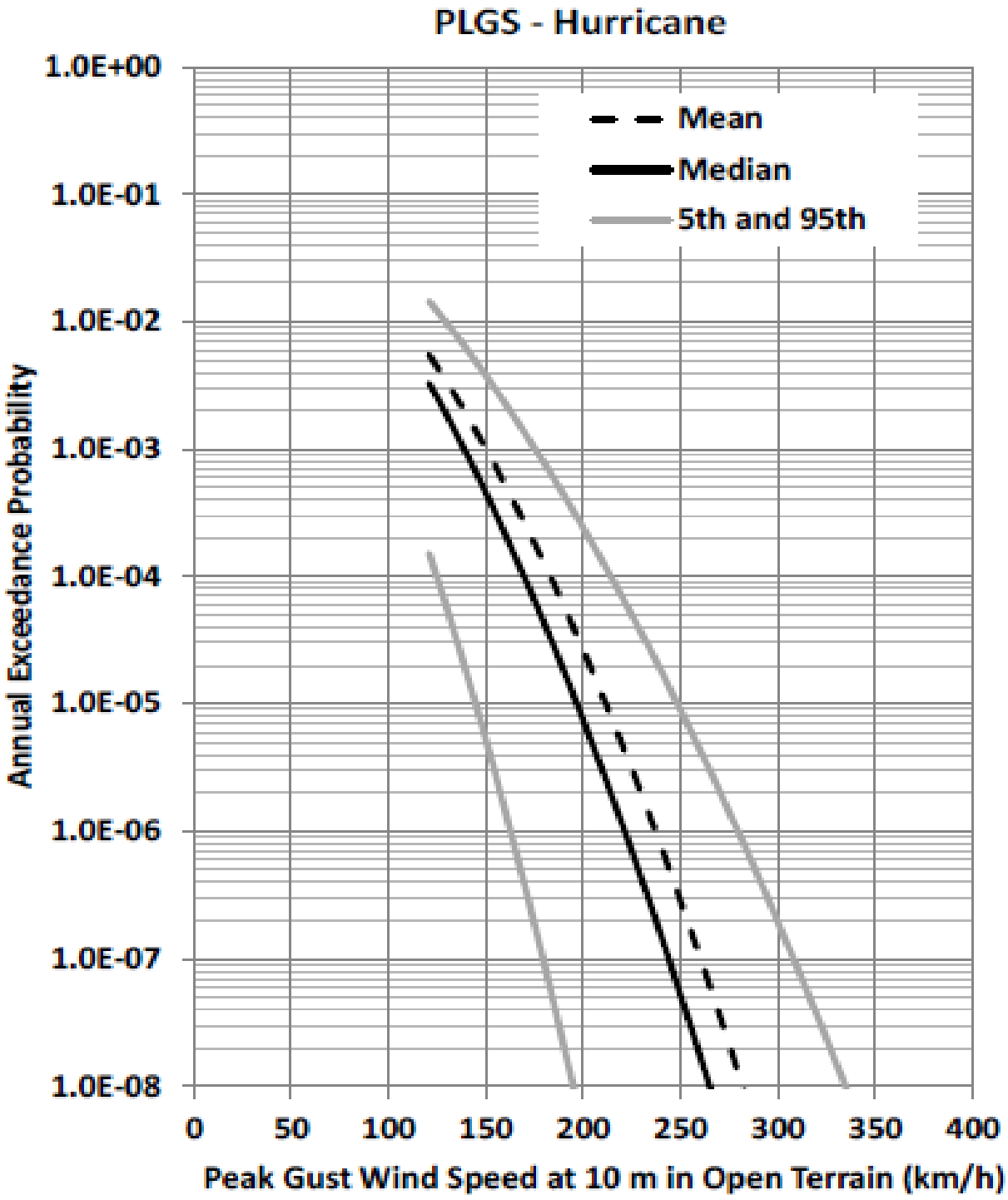


Figure 15: Hurricane Wind Hazard for Point Lepreau Site

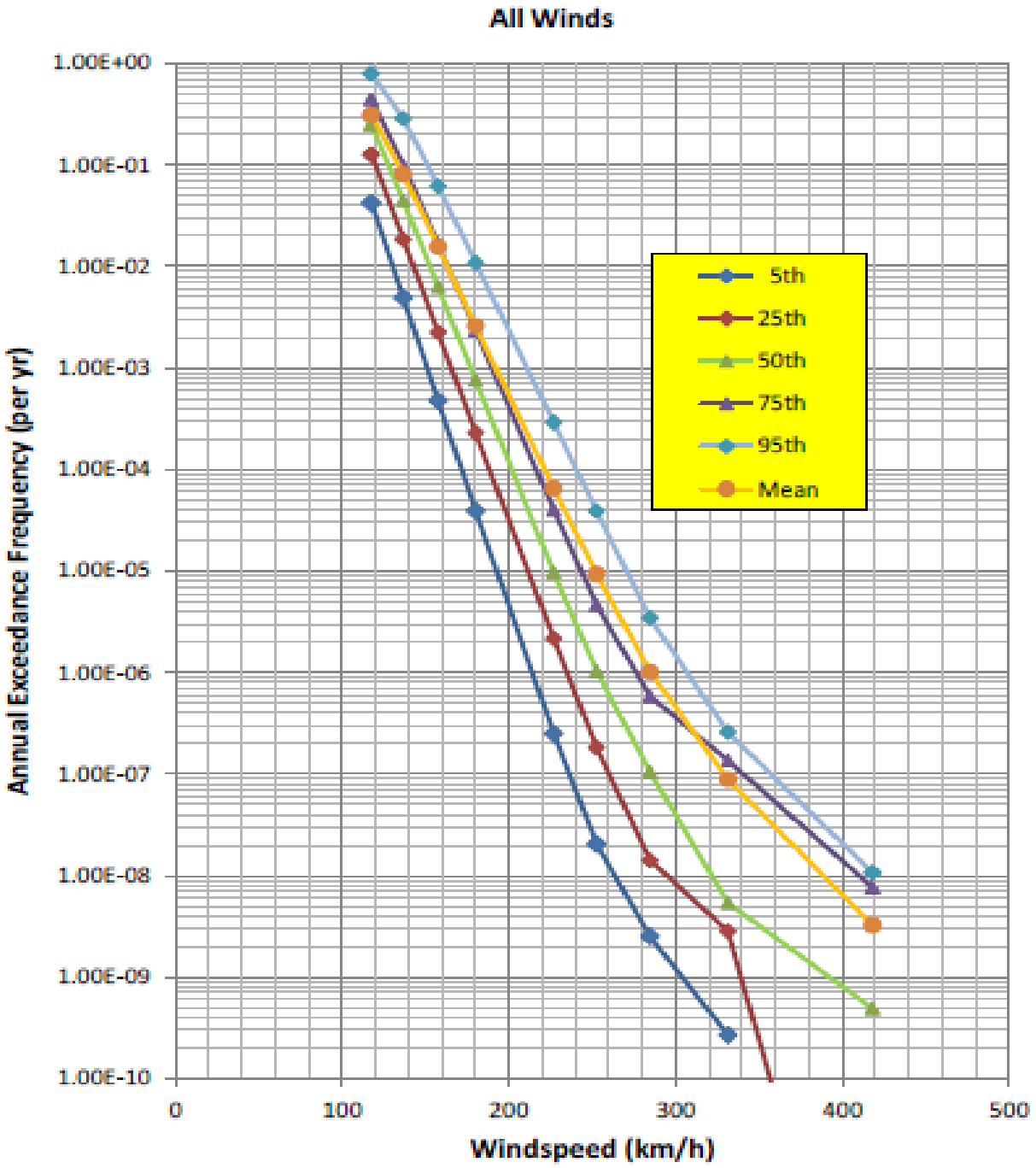


Figure 16: All Winds Family of Hazard Curves for Point Lepreau Site

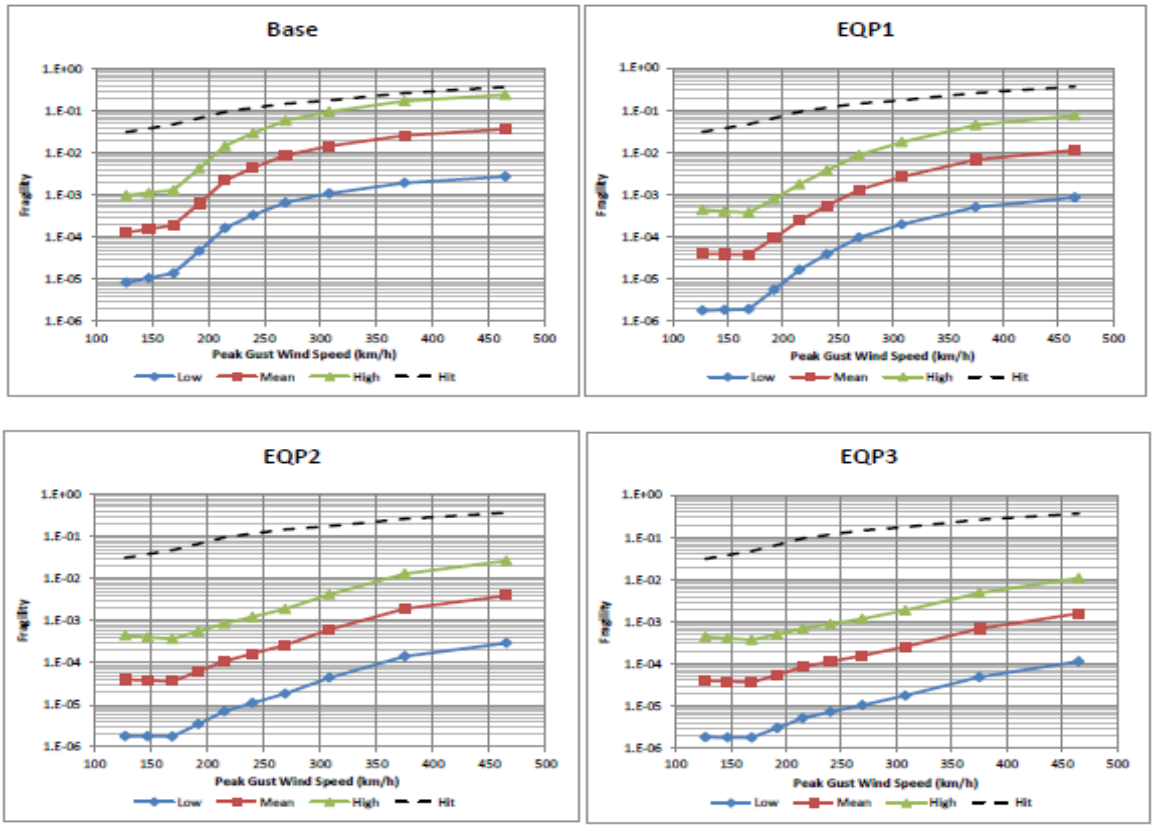


Figure 17: Sample Missile Fragility Output

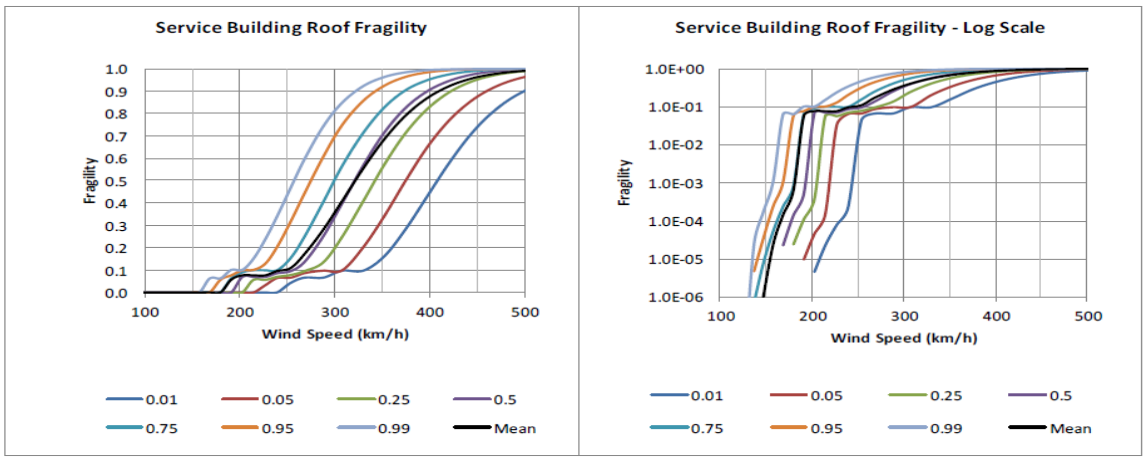


Figure 18: Sample Wind Fragility Curves

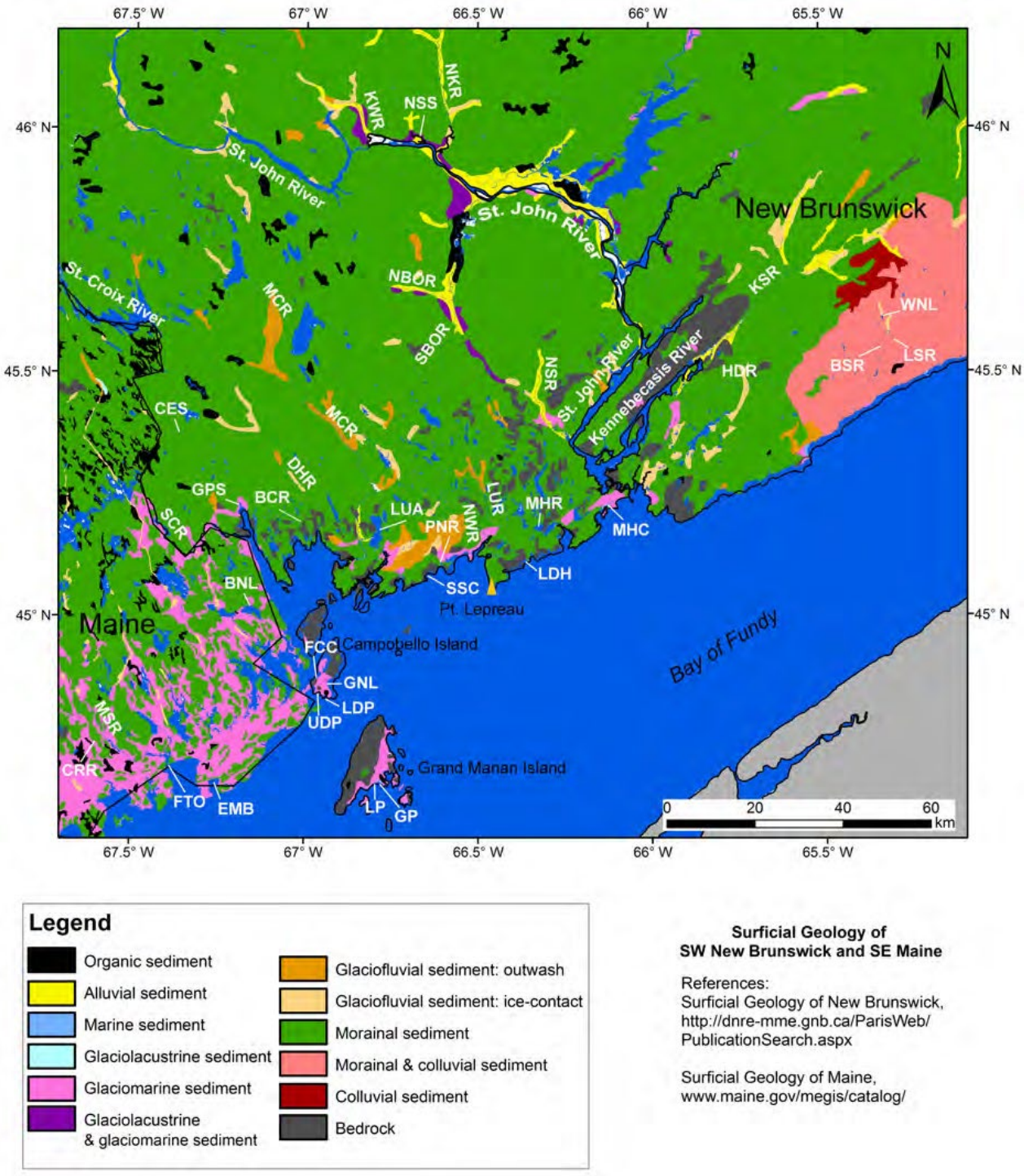


Figure 19: Area of Study for Field Work to determine if Tsunamis have Inundated Southern New Brunswick in the Past

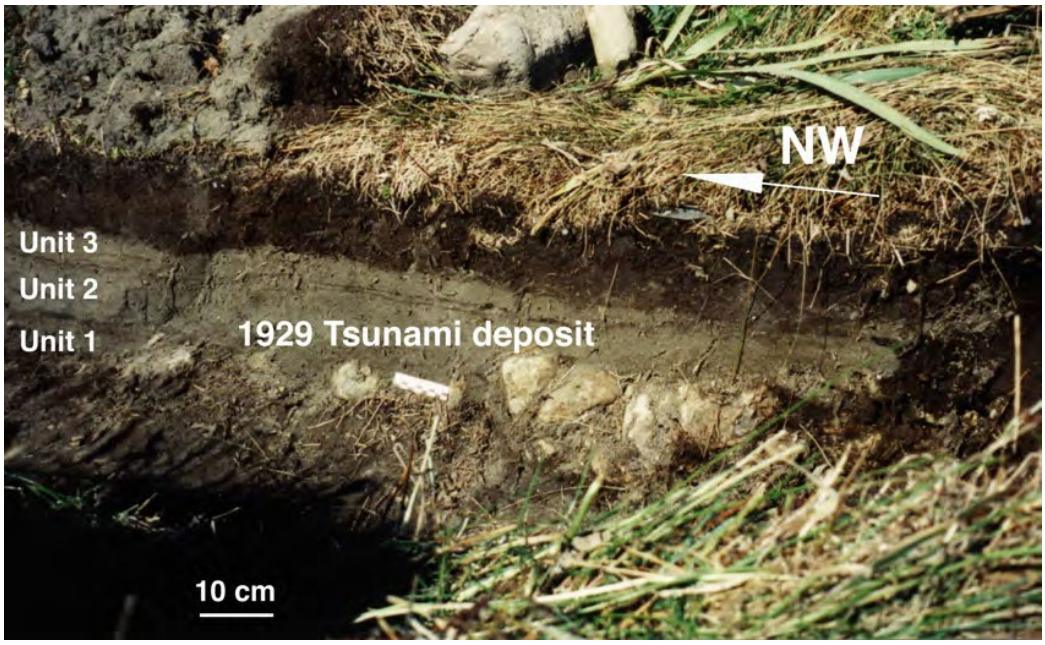


Figure 20: Example of what is looked for during field excavations. Photograph of 1929 tsunami deposit at Taylor's Bay on southern coast of Newfoundland. Sandy tsunami deposit is composed of three units deposited by consecutive waves.

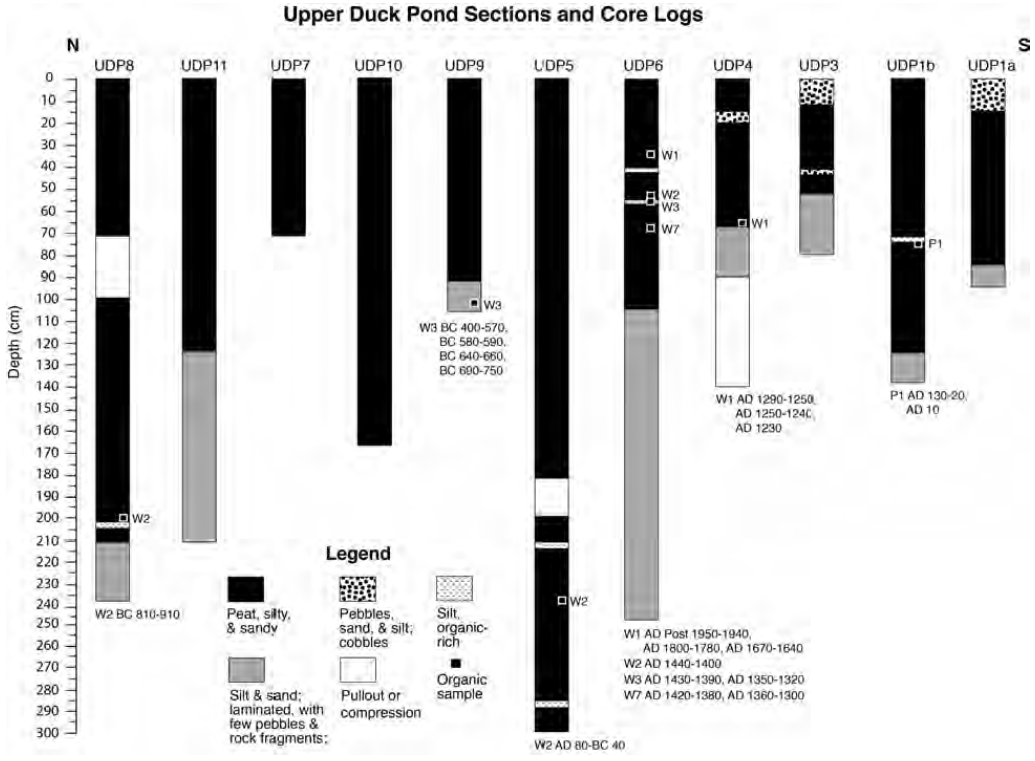


Figure 21: Partial Upper Duck Pond Sections and Core Logs

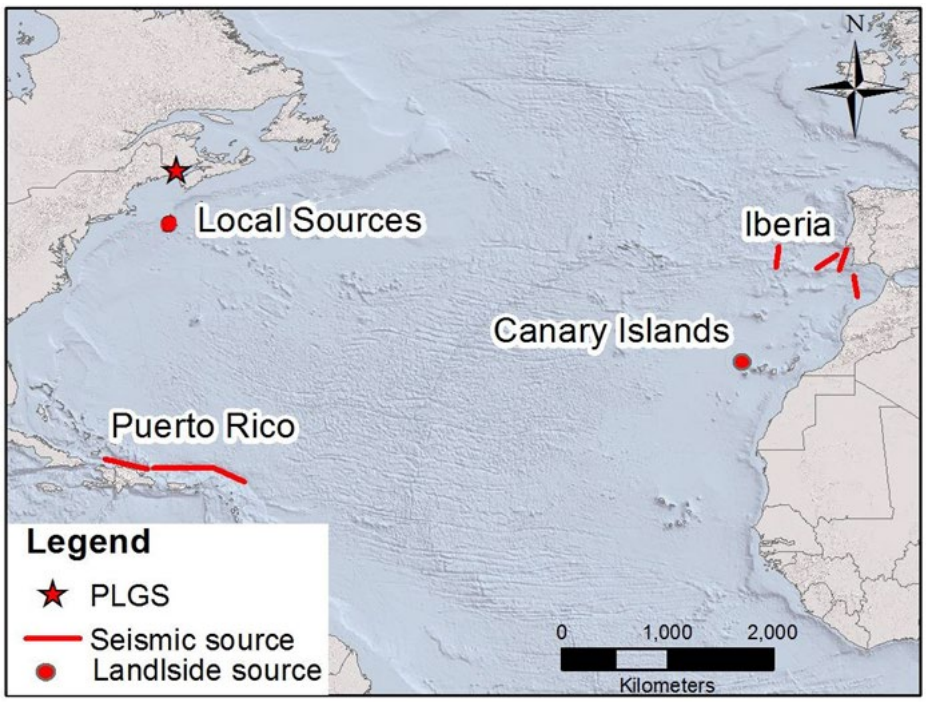


Figure 22: Transatlantic Source Zones Considered in the Tsunami Study

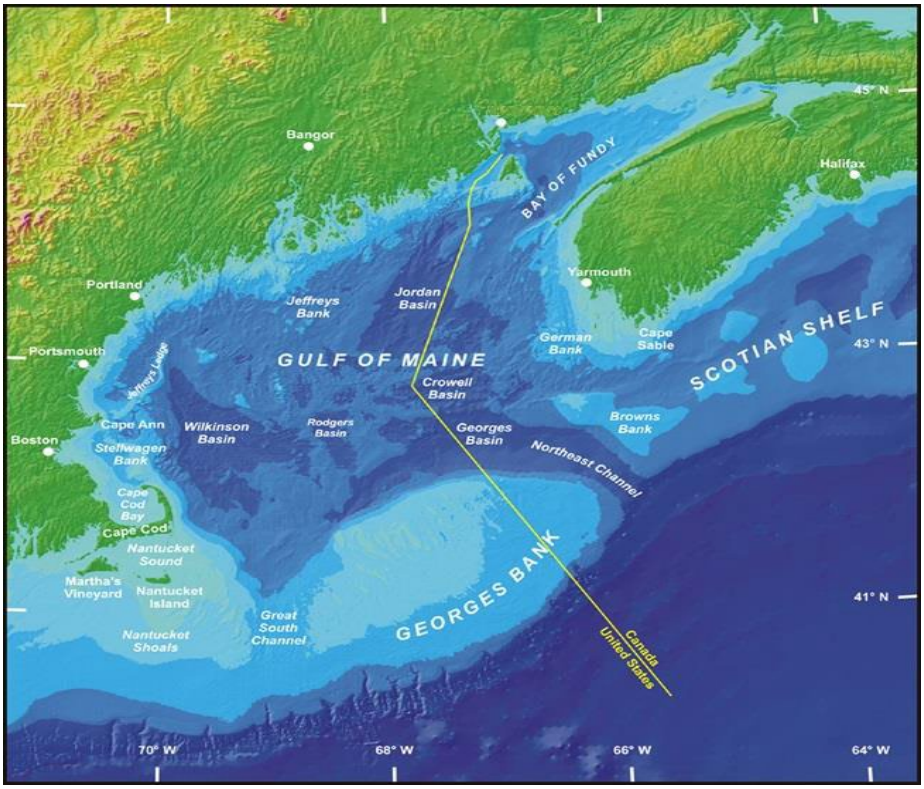


Figure 23: Bathymetric features of the continental shelf / Gulf of Maine (credit: NOAA)

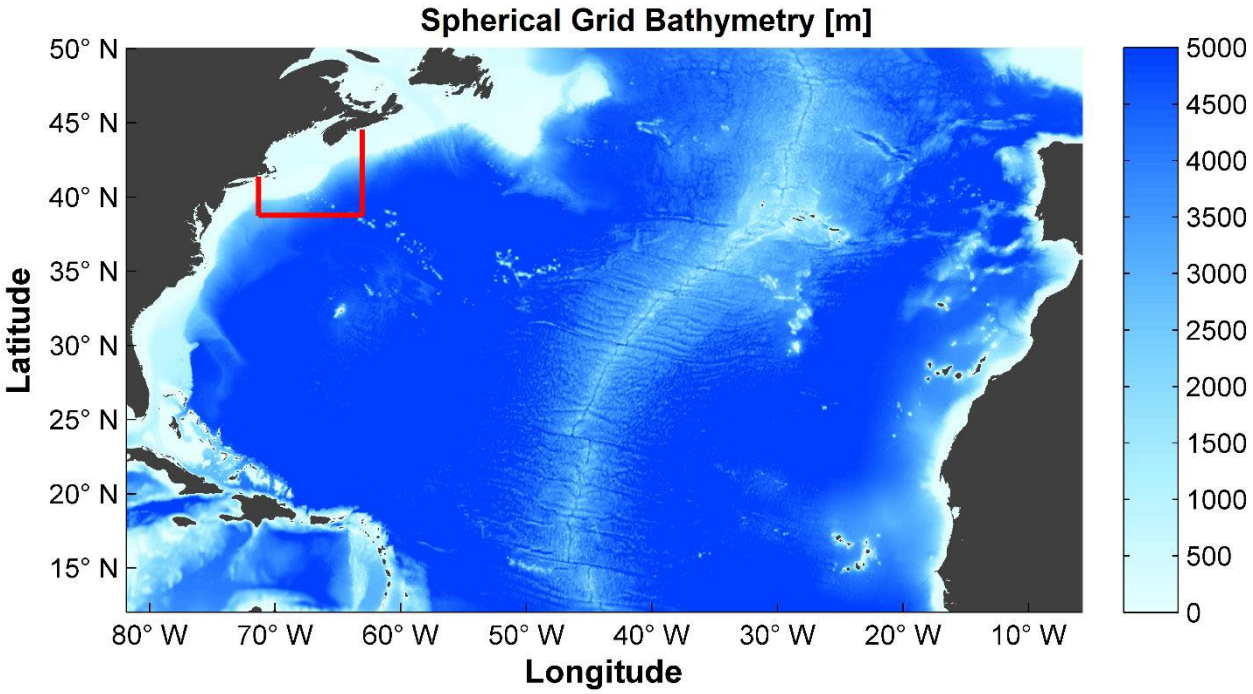


Figure 24: Bathymetry of the Atlantic Ocean Modeling grid. The Boundary of the Nested Regional Continental Shelf Grid Is Marked in Red

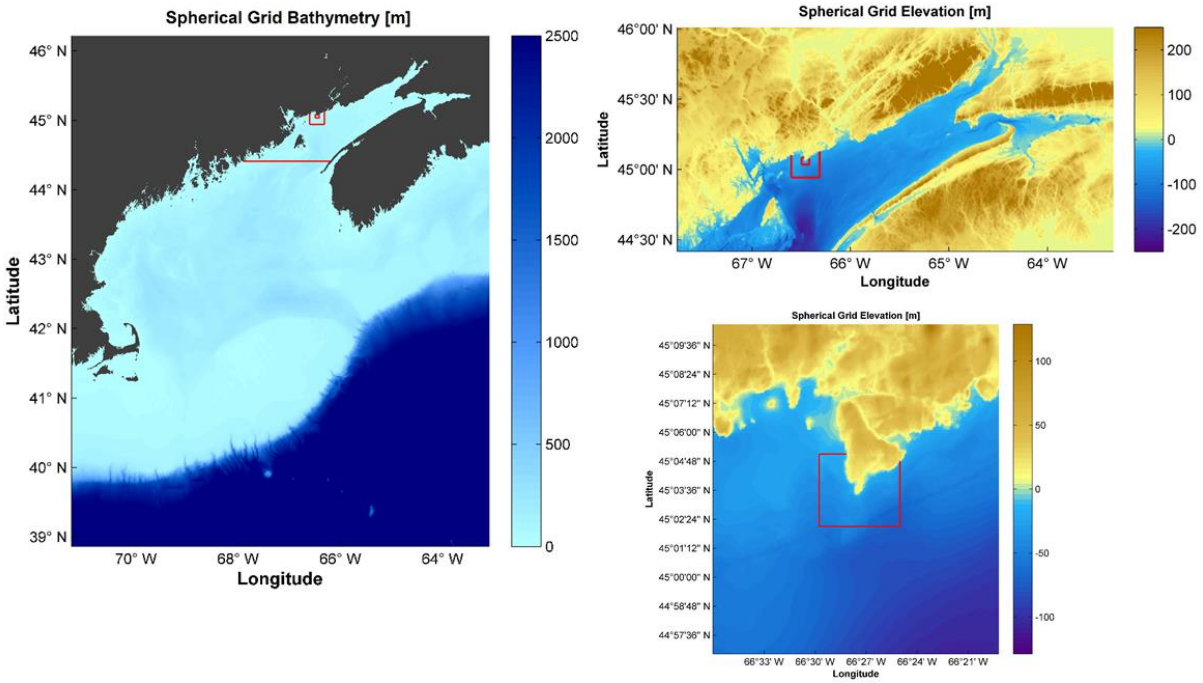


Figure 25: Spherical Grid Resolution Increases

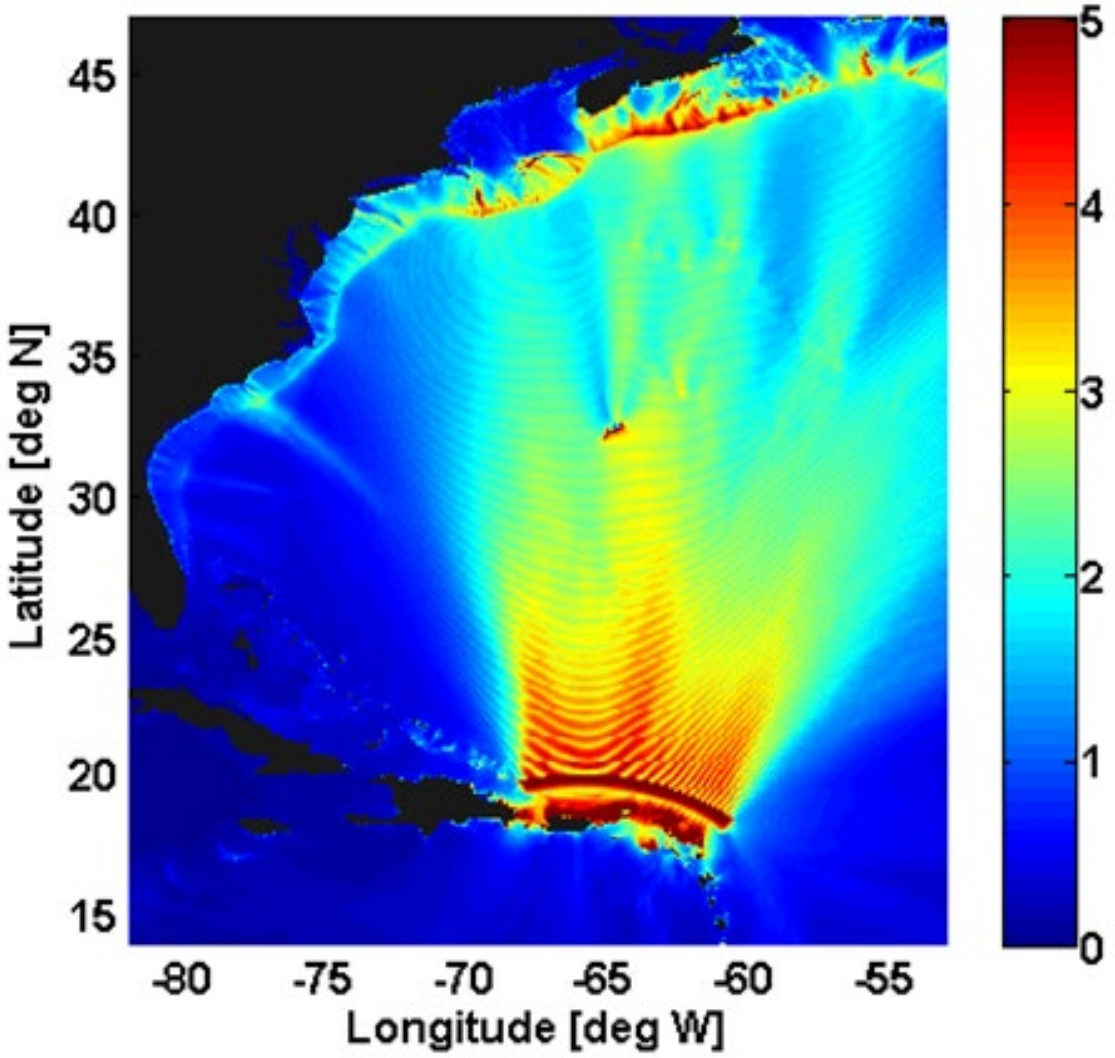


Figure 26: Maximum Water Levels Throughout Simulation From Puerto Rico Trench (Assumed M 9.1 Earthquake, 20 m average slip, 95 km fault width, 550 km fault length)

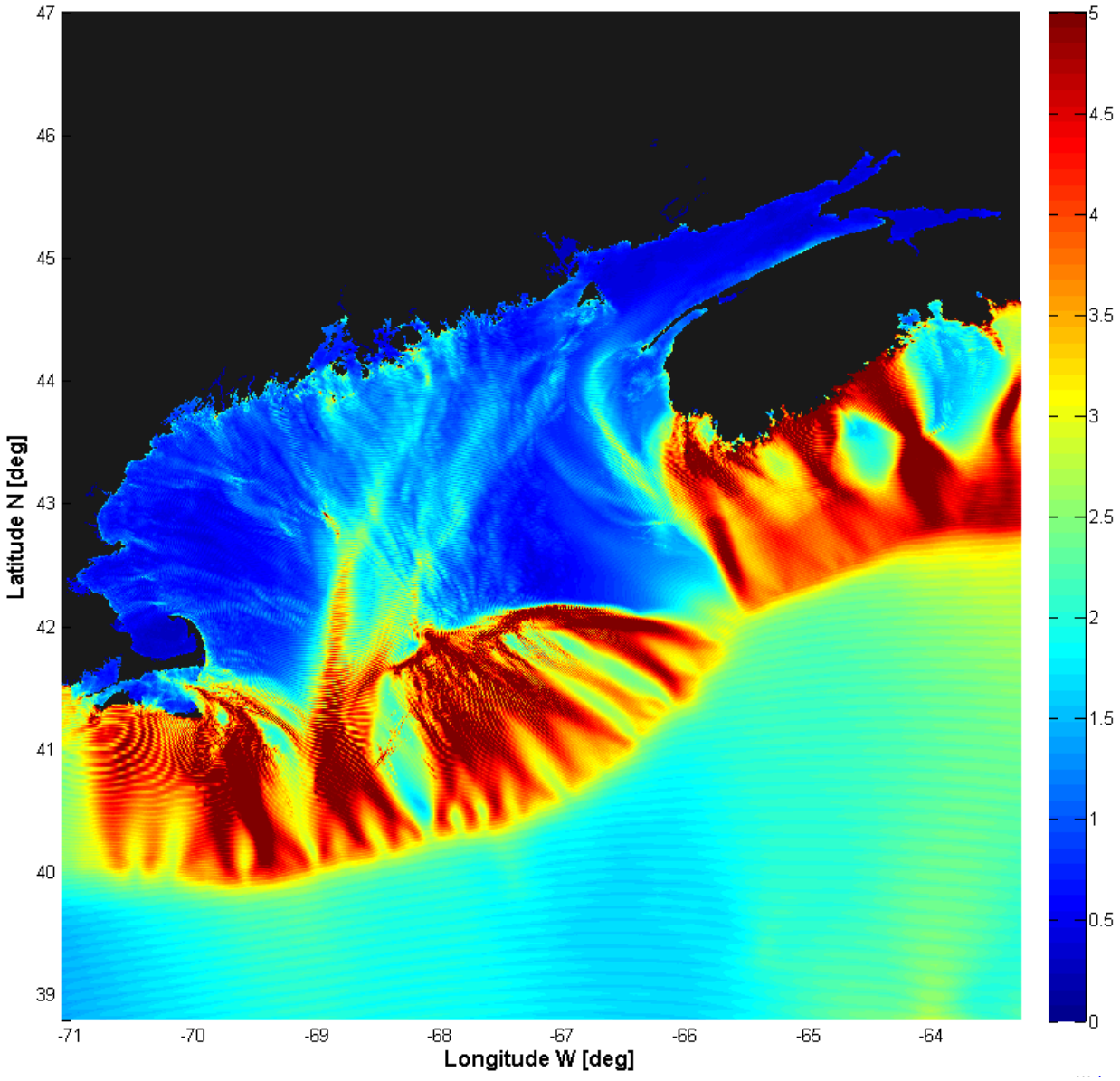


Figure 27: Bathymetric Effects as Potential Tsunami Moves Towards Shore (Maximum Water Levels Throughout Simulation)

(Assumed M 9.1 earthquake from Puerto Rico Trench per Figure 26)

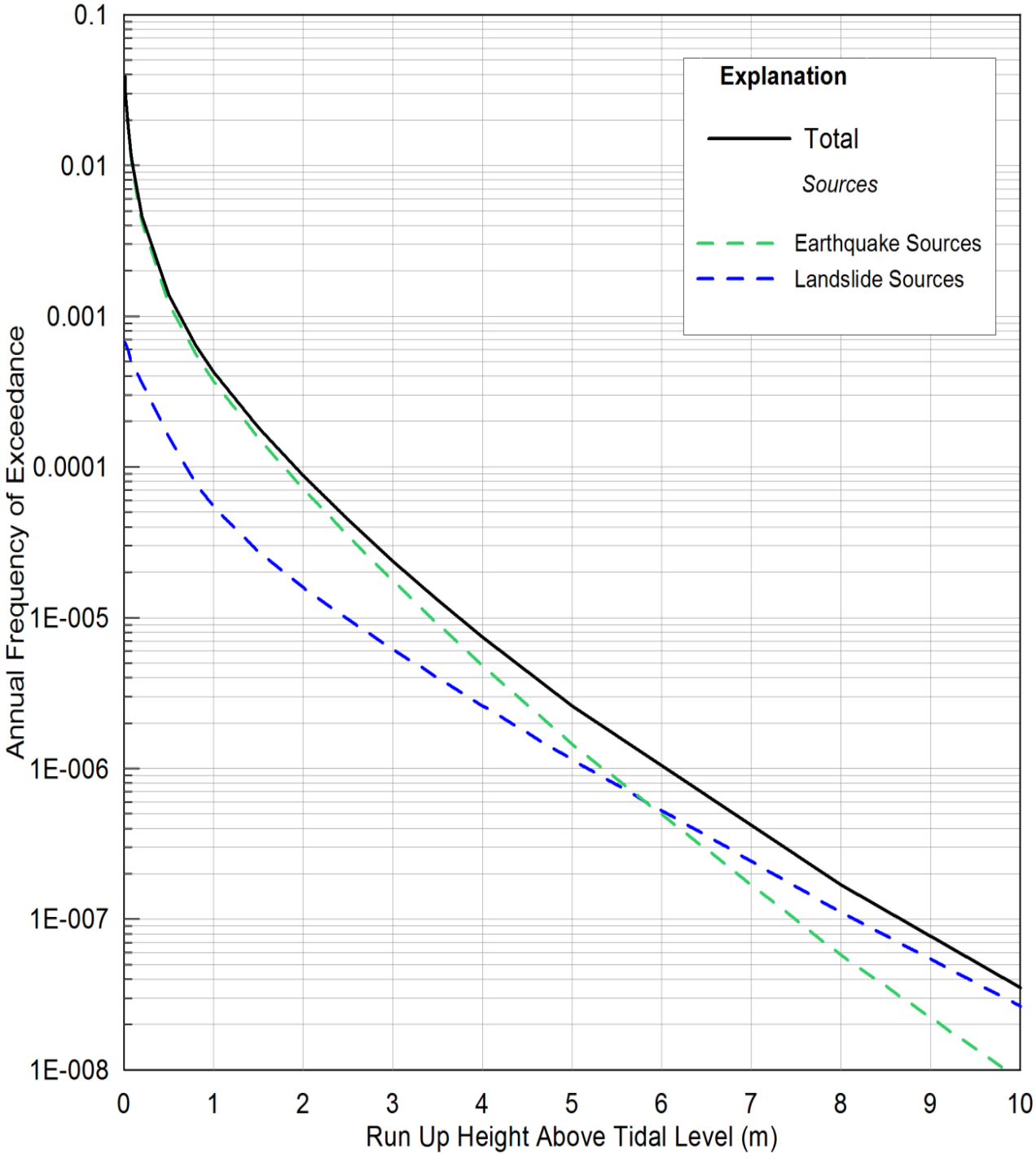


Figure 28: Probabilistic Tsunami Runup Hazard at High Astronomical Tide

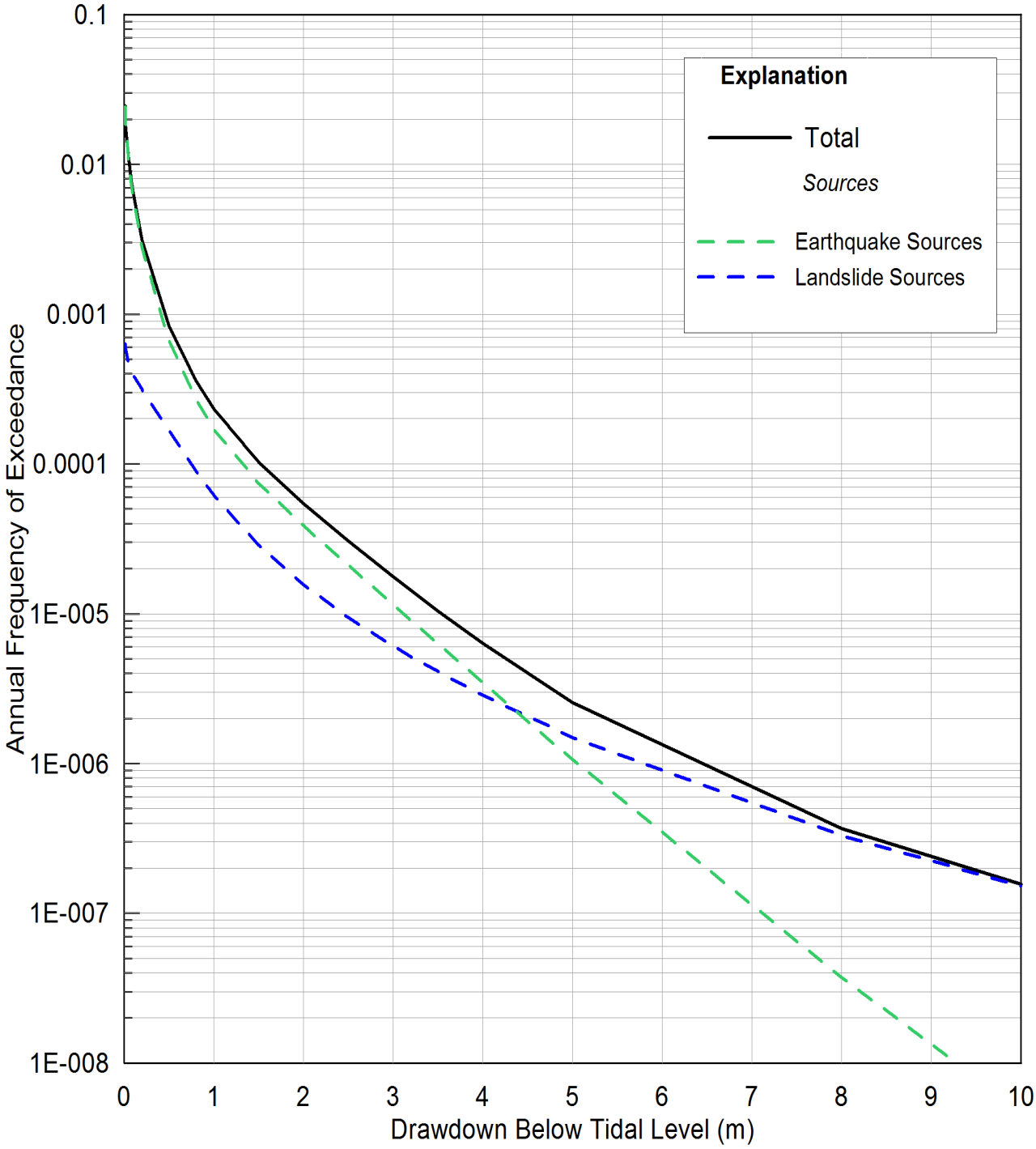


Figure 29: Probabilistic Tsunami Drawdown Hazard at Mean Sea Level

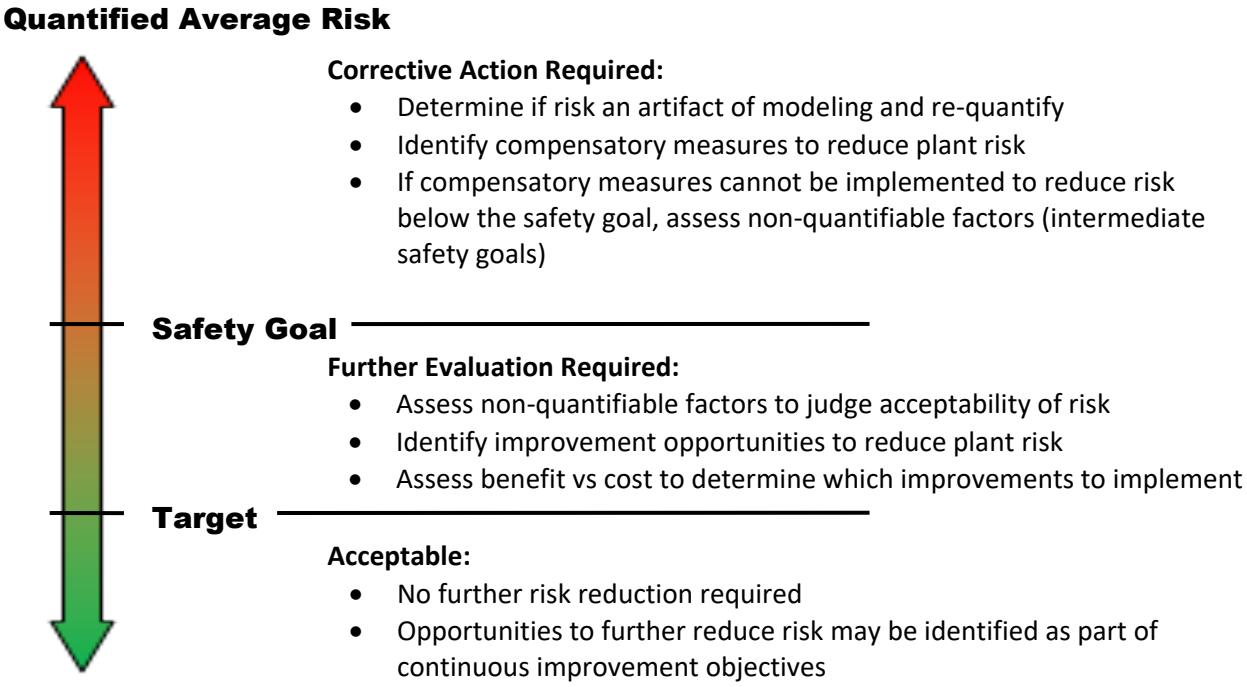


Figure 30: Application of Safety Goals

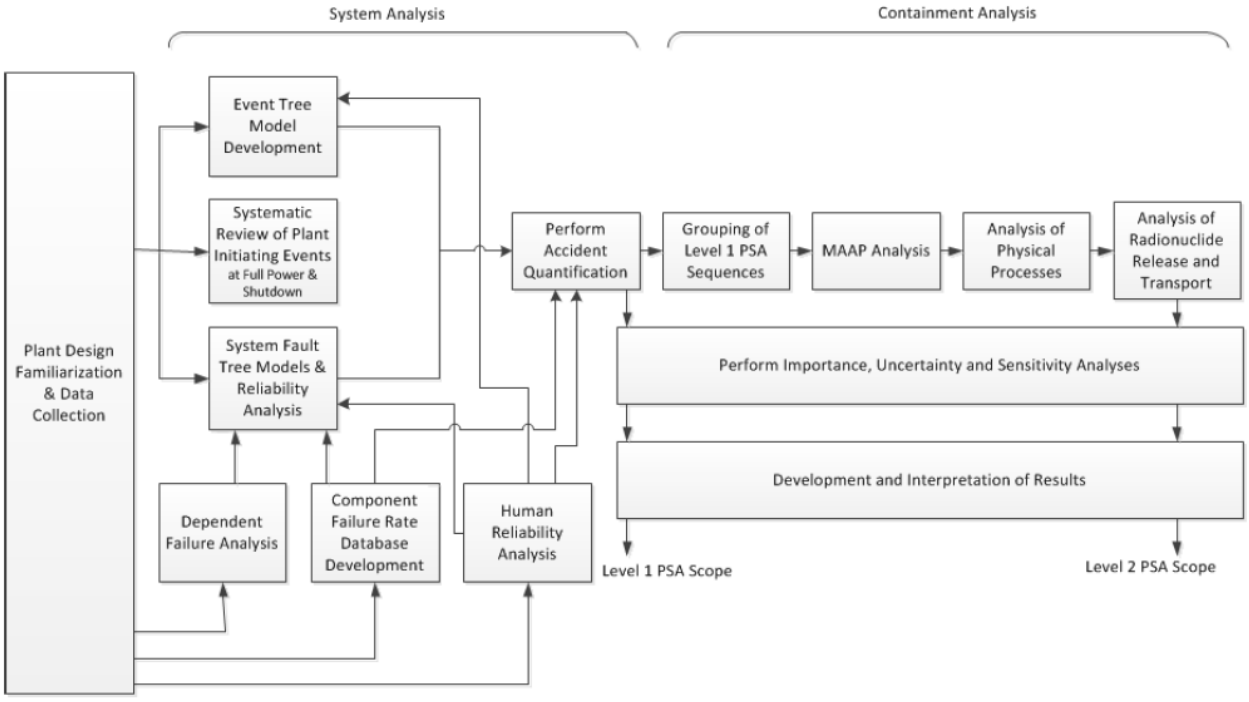
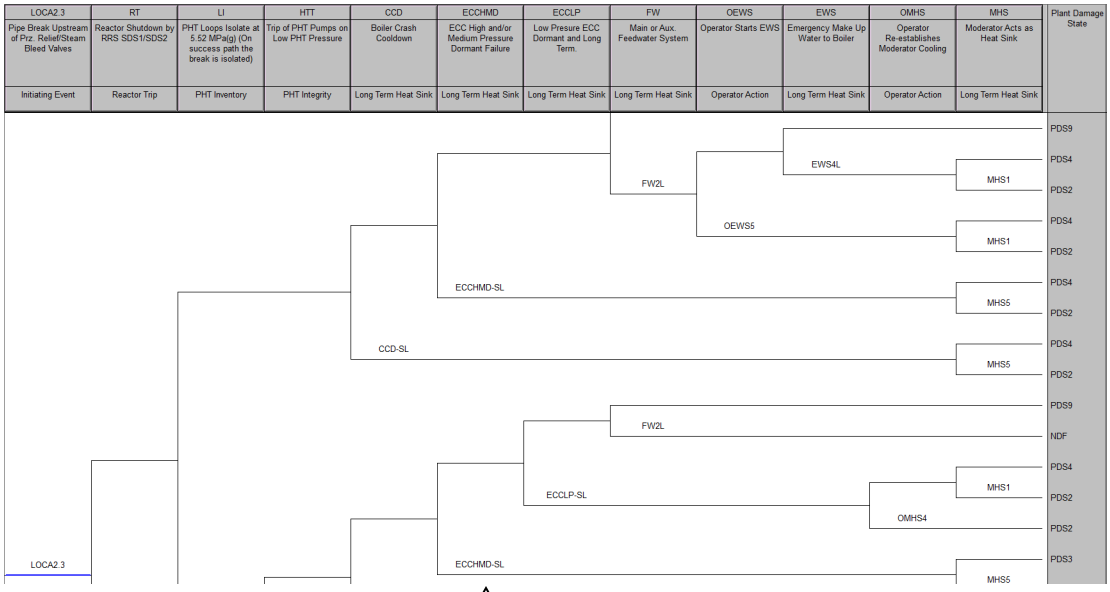
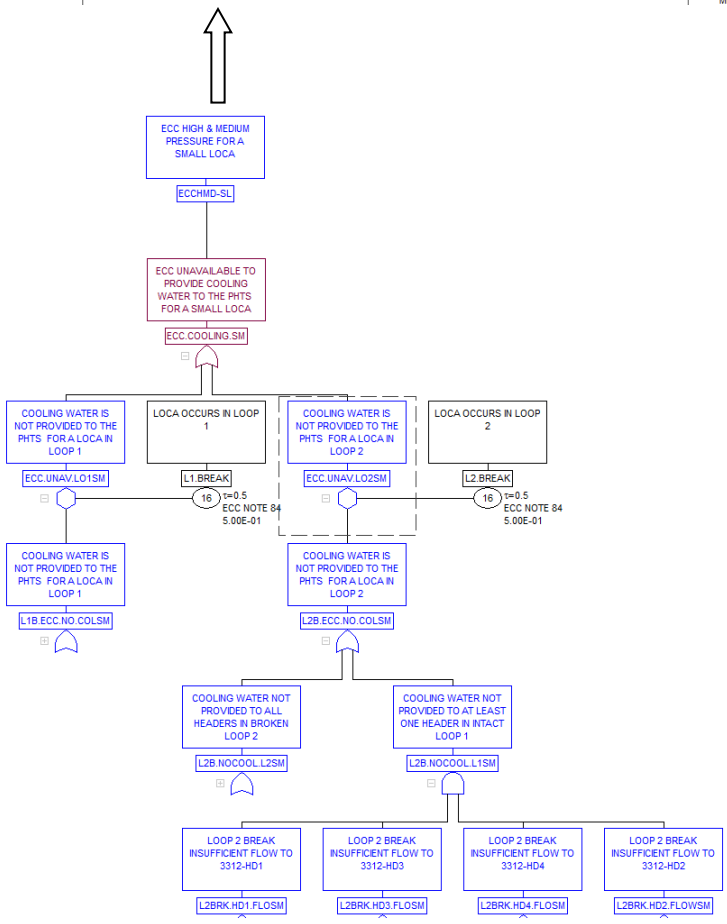


Figure 31: Simplified Overview of PSA Process



Sample of Event Tree



Sample of Fault Tree

Figure 32: Sample of Event Tree and Fault Tree Integration

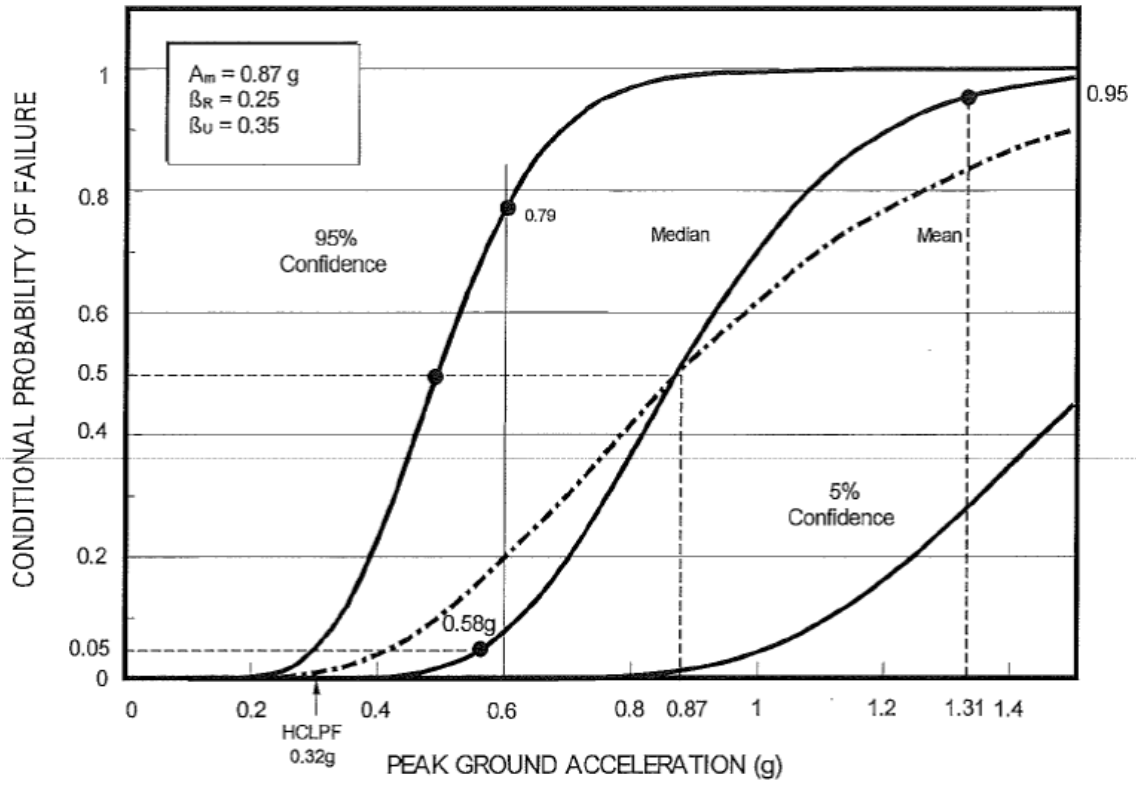


Figure 33: Example of a Fragility Curve

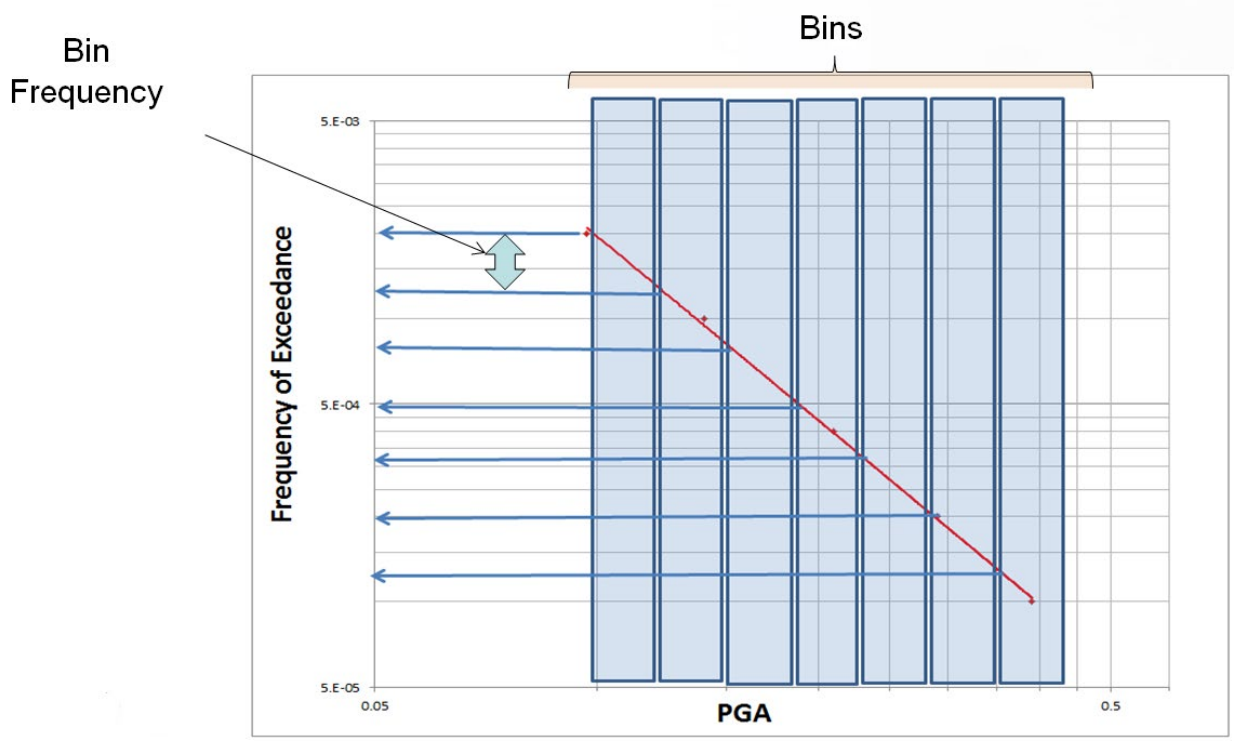


Figure 34: Example of Segregating Hazard Curve into Intervals (Bins)

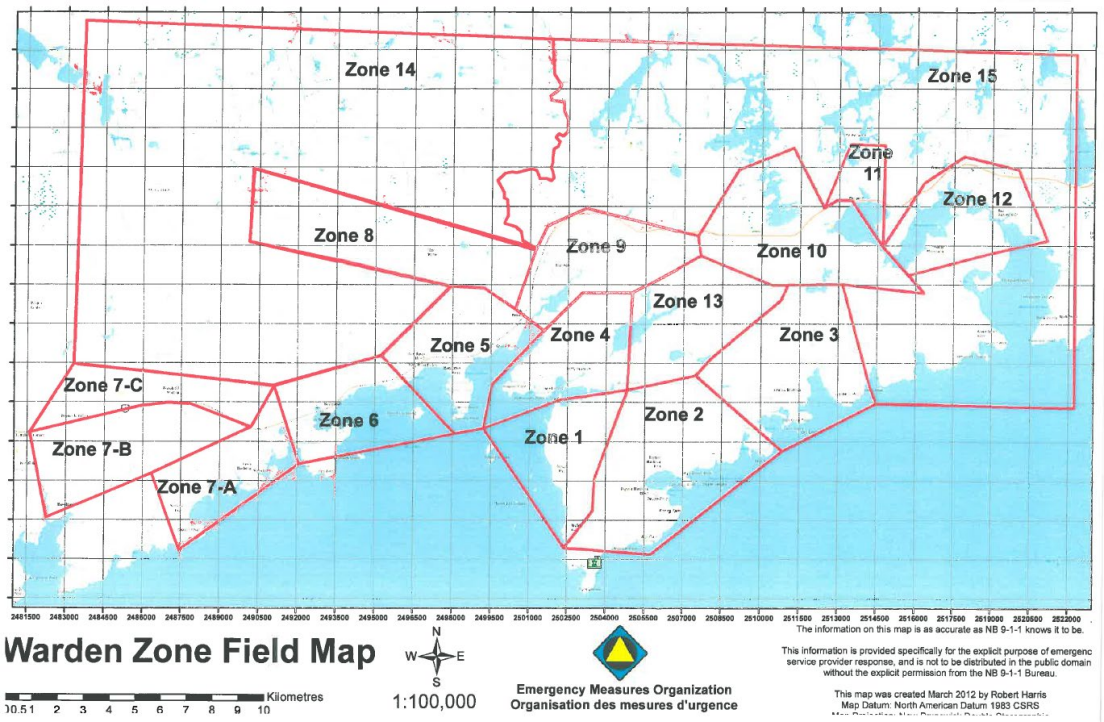


Figure 35: Map of Warden Zones for Emergency Off-Site Response

Appendix B: Tables

Table 1: Point Lepreau Nuclear Generating Station Safety System Groupings

SAFETY FUNCTION	GROUP 1 SYSTEMS	GROUP 2 SYSTEMS
Shutdown	Shutdown System 1	Shutdown System 2
Fuel Cooling	Emergency Core Cooling	Emergency Water Supply
Monitoring and Control	Main Control Room	Secondary Control Area

Table 2: Horizontal Uniform Hazard Response Spectra for Point Lepreau

Spectral Frequency (Hz)	Spectral Acceleration (g) at 5% Damping for Return Period (yr)				
	475	1,000	2,475	10,000	100,000
Mean hazard					
100	0.078	0.143	0.264	0.575	1.628
40	0.140	0.258	0.479	1.073	3.175
25	0.151	0.270	0.486	1.048	3.024
10	0.129	0.233	0.387	0.796	2.205
5	0.083	0.141	0.244	0.508	1.452
2.5	0.044	0.074	0.131	0.286	0.876
1	0.019	0.030	0.053	0.120	0.403
0.5	0.010	0.015	0.027	0.062	0.227
0.25	0.003	0.005	0.010	0.024	0.088
50th Percentile hazard					
100	0.052	0.088	0.157	0.343	0.982
40	0.098	0.171	0.310	0.675	1.946
25	0.107	0.185	0.322	0.677	1.862
10	0.094	0.157	0.263	0.527	1.366
5	0.064	0.103	0.171	0.336	0.861
2.5	0.035	0.056	0.092	0.182	0.474
1	0.015	0.023	0.038	0.073	0.191
0.5	0.007	0.011	0.018	0.035	0.089
0.25	0.002	0.004	0.007	0.013	0.037
84th Percentile hazard					
100	0.127	0.212	0.362	0.747	1.921
40	0.229	0.387	0.685	1.438	3.727
25	0.241	0.400	0.677	1.388	3.520
10	0.199	0.321	0.527	1.032	2.543
5	0.126	0.203	0.332	0.652	1.671
2.5	0.067	0.107	0.182	0.373	1.009
1	0.027	0.042	0.072	0.154	0.446
0.5	0.014	0.022	0.037	0.079	0.232
0.25	0.005	0.008	0.014	0.031	0.092

Table 3: Comparison of Updated Seismic Hazard to Previous Studies

Probability of Exceedance [Equivalent Return Period]	Structural Frequency, f (Hz)	Spectral Acceleration, S_a (g)[1]				
		This Study [Mean]	This Study [Median]	2010 NBCC [Median][2]	2010 NBCC Adjusted to Hard Rock[2,3] [Median]	AECL and Maritime Nuclear (1984)[4] [Median]
PE = 10% in 50 Years [475 years]	PGA	0.078	0.052	0.074	0.053	0.09-0.12
	5	0.083	0.064	0.162	0.084	---
	2.5	0.044	0.035	0.089 (T=0.5 sec)	0.037 (T=0.5 sec)	---
	1	0.019	0.015	0.043	0.017	---
	0.5	0.010	0.007	0.015	0.005	---
PE = 2% in 50 Years [2.475 years]	PGA	0.264	0.157	0.199	0.143	0.17-0.25
	5	0.244	0.171	0.387	0.200	---
	2.5	0.131	0.092	0.209 (T=0.5 sec)	0.088 (T=0.5 sec)	---
	1	0.053	0.038	0.101	0.039	---
	0.5	0.027	0.018	0.032	0.011	---
AFE = 10^{-4} [10,000 years]	PGA	0.575	0.343	0.460	0.331	0.25-0.43
	5	0.508	0.336	0.800	0.412	---
	2.5	0.288	0.182	0.44 (T=0.5 sec)	0.185 (T=0.5 sec)	---
	1	0.120	0.073	0.210	0.081	---
	0.5	0.062	0.035	0.060	0.021	---

NOTES:

1. All spectral ordinates are given as spectral acceleration (S_a) relative to gravity acceleration (g).
2. Values for AFE = 10^{-4} have been estimated by extrapolation of a straight line projection connecting the 10% in 50 and 2% in 50 years exceedance probability values reporting by the Geology Survey of Cada, as suggested by the 2010 National Building Code of Canada (NBCC) National Seismic Hazaard Maps.
3. Median 2010 NBCC values have been adjusted from Site Class C (soil) to “rock or stiff soil” using Reference Ground Condition factors.
4. Values cited are based on the full range of results reported for probabilistic seismic hazard analysis of three assumed seismic source models and parametric variations on the source model parameters; no combined single hazard curve was presented.

Table 4: Comprehensive List of Other External Hazards Screened for Consideration in Point Lepreau Nuclear Generating Station PSA

Aircraft impacts	High summer temperature	Seiche
Avalanche	Heavy load drop	Sinkholes
Biological events (detritus and zebra mussels)	Hurricane	Snow
Coastal erosions	Ice cover	Soil shrink/swell
Dam failures	Industrial or military facility accident	Storm surge
Drought	Landslide	Solar flares
Electromagnetic interference	Lightning	Transportation accidents
Events in other reactors on the site	Low lake or river level	Tsunami
External Flooding	Low winter temperature	Toxic gas
Extreme winds and tornados	Meteorite/satellite strikes	Turbine-generated missile
Fog	Non-safety building fire	Volcanic activity
Forest Fire	Pipeline accident	Waves
Frost	Intense precipitation	Subsurface freezing
Grass fire	Release of chemicals from onsite storage	Collision of floating debris
Hail	River diversion	Snow melt
High tide	Sandstorm	Explosions

Table 5: Initiating Events for Level 1 Internal Events PSA

INITIATING EVENT CODE	EVENT GROUP
LORA1.1	Loss of regulation: core power excursion
LORA1.2	Loss of regulation: regional power excursion
LOCA 1.1	Large LOCA: containment bypass into medium pressure emergency core cooling
LOCA 1.2	Large LOCA: no containment bypass
LOCA 2.1	Small LOCA: multiple steam generator tube rupture
LOCA 2.2	Small LOCA: loss of gland seal cooling to all PHT pumps
LOCA 2.3	Small LOCA: pipe break upstream of pressurizer relief/steam bleed valves
LOCA 2.4	Small LOCA: multiple tube ruptures in any recirculating cooling water HX (containment bypass)
LOCA 2.5	Small LOCA equivalent to 2.5% RIH break
LOCA 2.6	Pressure tube and calandria tube rupture
LOCA 2.7	Feeder stagnation break
LOCA 3.1	Fuelling machine induced LOCA with no fuel ejection
LOCA 3.2	Fuelling machine induced LOCA with fuel ejection
LOCA 3.3	Fuelling machine induced end fitting failure
LOCA 3.4	Fuelling machine induced LOCA, FM on reactor
LOCA 4.1	HTS leak: within operating D2O feed pump capacity (no containment bypass)
LOCA 4.2	HTS leak: heat exchanger single tube rupture into recirculating cooling water (containment bypass)
LOCA 4.3	HTS leak: steam generator tube rupture
LOCA 4.4	HTS leak: leak into annulus gas system
LOFA 1.1	Total loss of heat transport system pumped flow
LOFA 1.2	Partial loss of heat transport system pumped flow
LOFA 2.1	Single Channel Flow Blockage
LOHS 1.1	Loss of feedwater flow
LOHS 1.2	Asymmetric feedwater line break inside RB upstream of SG check valve
LOHS 1.3	Asymmetric feedwater line break inside RB downstream of SG check valve
LOHS 1.4	Symmetric feedwater line break outside RB

Table 5: Initiating Events for Level 1 Internal Events PSA (Continued)

INITIATING EVENT CODE	EVENT GROUP
LOHS 1.5	Feedwater break over main control room
LOHS 1.6	Asymmetric feedwater line break outside RB
LOHS 2.1	Asymmetric SG blowdown line break inside RB
LOHS 2.2	Symmetric SG blowdown line break inside RB
LOHS 2.3	Symmetric SG blowdown line break outside RB
LOHS 3.1	Loss of condensate flow to deaerator
LOHS 3.2	Loss of condenser vacuum
LOHS 3.3	Small Condenser Cooling Water Line Break Considered under Flooding Only.
LOHS 3.4	Large Condenser Cooling Water Line Break Considered under Flooding Only.
LOHS 4.1	Main steam line leak inside Turbine Building
LOHS 4.2	Main steam line break inside Reactor Building
LOHS 4.3	Main Steam line leak over main control room
LOHS 5.1	Small main steam line failures causing low deaerator level
LOPC 1.1	HTS pressure control failure low
LOPC 1.2	HTS pressure control failure high
LOPC 2.1	Pressurizer relief/steam bleed valves fail open
LOPC 3.1	Heat transport LRVs fail open
SDLORA 1.1	Shutdown loss of regulation: core power excursion
SDLOCA 1.1	Shutdown LOCA: HTS pipe leaks HTS full and depressurized
SDLOFA 1.1	Loss of SDC pumped flow HTS drained to header level
SDLOFA 1.2	Loss of SDC pumped flow HTS full and depressurized
SDLOHS 1.1	Loss of SDC heat removal HTS drained to header level
SDLOHS 1.2	Loss of SDC heat removal HTS full and depressurized
MOD 1.1	Total loss of moderator cooling
MOD 1.2	Partial loss of moderator cooling
MOD 2.1	Calandria inlet/outlet pipe break outside calandria vault
MOD 3.1	Moderator pipe break inside calandria vault
MOD 3.2	Calandria Tube Leaks Into Annulus Gas
MOD 4.1	Moderator heat exchanger single tube rupture
MOD 4.2	Moderator heat exchanger multiple tube rupture
MGAS 1.1	Loss of moderator cover gas deuterium control
END 1.1	Loss of end shield heat sink

Table 5: Initiating Events for Level 1 Internal Events PSA (Continued)

INITIATING EVENT CODE	EVENT GROUP
END 1.2	Loss of end shield coolant flow
END 1.3	End shield cooling pipe break
FM 1.1	Fuelling machine D2O system failures
FM 2.1	Fuelling machine failures causing mechanical damage to fuel on reactor
FM 3.1	Loss of cooling to fuel in fuelling machine F/M off reactor. Considered for Level 2 only.
DIR 2.1	Chemical damage to fuel
STOR 1.1	Spent fuel transfer system failures. Considered for Level 2 only.
STOR 1.2	Mechanical damage to fuel during storage.
STOR 1.3	Mechanical damage to fuel during transfer to spent fuel bay. Considered for Level 2 only.
STOR 1.4	Loss of spent fuel bay heat sink
STOR 1.5	Partial Loss Of Storage Bay Inventory
XEL 1.1	Partial loss of class I power
XEL 2.1	Partial loss of class II power. Not considered. Deemed to be represented by IE-DCC
XEL 4.1	Total loss of class IV power reactor operating
XEL 4.2	Total loss of class IV power – reactor shutdown, HTS cold depressurized and full
XEL 4.3	Total loss of class IV power – reactor shutdown, HTS cold depressurized and drained to the header level
XIA 1.1	Total loss of instrument air reactor operating at full power
XIA 1.2	Total loss of instrument air reactor shutdown, HTS cold full and depressurized
XIA 1.3	Total loss of instrument air reactor shutdown, HTS drained to header level
XSW 1.1	Total loss of service water reactor operating at full power
XSW 1.2	Loss of service water reactor shutdown HTS cold full and depressurized
XSW 1.3	Loss of service water reactor shutdown HTS drained to header level
DCC	Dual computer control failure
GENT	General transient

Table 6: Plant Damage States for Level 1 PSA

PLANT DAMAGE STATE	DEFINITION	TYPE OF ACCIDENT
0	Early (Rapid) Loss of Core Structural Integrity	Severe Core Damage
1	Late Loss of Core Structural Integrity with High PHT Pressure	Severe Core Damage
2	Late Loss of Core Structural Integrity with Low PHT Pressure	Severe Core Damage
3	loss of coolant accident + loss of emergency core cooling with Moderator Required within Fifteen (15) Minutes	Core Deformation
4	Loss of coolant accident + loss of emergency core cooling with Moderator Required after Fifteen (15) Minutes	Core Deformation
5	Large LOCA with Early Flow Stagnation	Widespread Fuel Damage
6	Single Channel LOCA with Containment Overpressure	Limited Fuel Damage
7	Single Channel LOCA with No Containment Overpressure (In-Core LOCA)	Limited Fuel Damage
8	Loss of Cooling to Fuelling Machine	Limited Fuel Damage
9	LOCA with No Significant Fuel Failures	Radioactive and Tritium Release
10	Deuterium Deflagration (D_2 > 4%) in Cover Gas and/or Release of Moderator into Containment (Fuel Cooling is Maintained)	Radioactive and Tritium Release

Table 7: External Plant Release Categories

EXTERNAL PLANT RELEASE CATEGORY	DEFINITION	TYPE OF ACCIDENT
EPRC0	Early external releases as a result of containment isolation failure	Large Release
EPRC1	External releases as a result of severe core damage, between 0 and 6 hours	Large Release
EPRC2	External releases as a result of severe core damage, between 6 and 24 hours	Large Release
EPRC3	Late releases as a result of severe core damage, between 24 and 72 hours	Large Release
EPRC4	Initial containment by-pass + EPRC1	Large Release
EPRC5	Initial containment by-pass + EPRC2	Large Release
EPRC6	Initial containment by-pass + EPRC3	Large Release
EPRC7	Initial containment by-pass + mitigated successfully	Small Release
EPRC8	PDS3 and PDS4 and containment isolation failure	Very Small Release
EPRC9	PDS3 and PDS4 and failure of containment heat sinks	Very Small Release
EPRC10	PDS5 to PDS10 and containment isolation failure	Very Small Release
EPRC11	PDS5 to PDS10 and failure of containment heat sinks	Very Small Release
EPRC12	PDS8 with failure of spent fuel bay isolation	Very Small Release
EPRC13	Initial containment by-pass, MSSV reclosed in 30 minutes + mitigated successfully	Small Release
EPRC14	Successful Emergency Filtered Containment Venting and Calandria Vault Make-up	Very Small Release

Table 8: Seismic Screening Criteria (Capacity versus Demand)

Screening Levels	Structures, Systems and Components Located at Base Slab	Structures, Systems and Components Located above Base Slab
Screened at 0.3g Peak Ground Acceleration	5% damped peak Floor Response Spectra ≤ 0.8g	5% damped peak Floor Response Spectra ≤ 1.2g
Screened at 0.5g Peak Ground Acceleration	5% damped peak Floor Response Spectra ≤ 1.2g	5% damped peak Floor Response Spectra ≤ 1.8g

Table 9: Seismic Hazard Bins

No.	Seismic-induced Initiating Event	Seismic Level/ HCLPF[4] (g PGA)[5]	PGA Seismic Range (g)	Bin Frequency (1 occurrence in *X* years)
1	Loss of Class IV Power	0.10	0.10 to 0.20	1,628.7
2	Loss of Group 1 Systems	0.20	0.20 to 029	7,092.2
3	Very Small Loss of Coolant Accident (<27 kg/s)	0.29	0.29 to 0.30	63,694.3
4	Main Steam Line Break in the Turbine Building	0.30	0.30 to 0.42	18,552.9
5	Small Loss of Coolant Accident	0.42	0.42 to 0.48	37,174.7
6	Large Loss of Coolant Accident Leading to Severe Core Damage	0.48	0.48 to 0.53	77,519.4
7	Failures Leading Directly to Severe Core Damage	0.53	0.53 to 0.60	109,890.1

Table 10: Safety Goals and Targets

Metric	Safety Goal	Target
Severe Core Damage (1 occurrence in *X* reactor-years)	10,000	100,000
Large Release (1 occurrence in *X* reactor-years)	100,000	1,000,000

[4] HCLPF = High Confidence, Low Probability of Failure, or there is 95% confidence that the failure probability of the item is 5% or less at the stated peak ground acceleration (PGA).
[5] g PGA = Peak ground acceleration expressed in *g* (the acceleration due to Earth's gravity)

Table 11: Aggregated PSA Results with Reactor At-Power

Model	Severe Core Damage Frequency (1 occurrence in *X* reactor-years)	Large Release Frequency (1 occurrence in *X* reactor-years)
Internal Events	141,043.7	7,407,407.4
Internal Floods	9,259,259.3	9,259,259.3
Internal Fires	138,504.2	2,487,562.2
Seismic	100,704.9	400,000.0
SIMPLE AGGREGATE	**41,071.1**	**317,965.0**
Safety Goal Met (per Table 10**)?**	**YES**	**YES**

Table 12: PSA Results with Reactor Shut Down

Model	Severe Core Damage Frequency (1 occurrence in *X* reactor-years)	Large Release Frequency (1 occurrence in *X* reactor-years)
Internal Events	252,525.3	56,818,181.8
Safety Goal Met (per Table 10**)?**	**YES**	**YES**

Table 13: Public Health Risk Estimates

Health Effect	Calculated Risk (1 occurrence in *X* years)	Typical Target (1 occurrence in *X* years)
Early Fatality (per individual)	2,551,020.4	1,000,000
Delayed Fatality (per individual)	255,102.0	100,000

Table 14: Population by Warden Zones (per September 2011 Demographic Survey)

Warden Zone	Adults	Children	TOTAL
Zone 1	317	51	368
Zone 2	134	14	148
Zone 3	259	20	279
Zone 4	116	7	123
Zone 5	283	25	308
Zone 6	183	13	196
Zone 7A	159	17	176
Zone 7B	226	40	266
Zone 7C	253	24	277
Zone 8	117	8	125
Zone 9	195	27	222
Zone 10	250	21	271
Zone 11	217	29	246
Zone 12	104	7	111
Zone 13	0	0	0
Zone 14	0	0	0
Zone 15	0	0	0
TOTAL	2813	303	3116
GRAND TOTAL	**3116**		
PLGS	800	0	800
TOTAL	800	0	800
GRAND TOTAL	**3916**		3916