ONTARIOPOWER GENERATION

Report

OPG Proprietary

Document Number:	Usage Classification:
NA44-REP-03611-00036	**N/A**
Sheet Number:	Revision:
N/A	**R003**

Title:
Pickering Nuclear Generating Station A Probabilistic Safety Assessment Summary Report

Pickering Nuclear Generating Station A Probabilistic Safety Assessment Summary Report

NA44-REP-03611-00036-R003

2024-01-30

Order Number: N/A
Other Reference Number: N/A

OPG Proprietary

Prepared by: Jingwen Zhu 2024-01-30
Jingwen Zhu
Assistant Technical Officer
Nuclear Safety and Technology Department

Concurred by: Lawrence Yu 2024-02-06
Lawrence Yu
Manager
Nuclear Safety and Technology Department

Reviewed by: Wargha Peiman 2024-02-02
Wargha Peiman
Senior Technical Engineer
Nuclear Safety and Technology Department

Approved by: Divya Ommen 2024-02-08
Divya Kakuzhyil
Senior Manager
Nuclear Safety and Technology Department

Table of Contents

Page

List of Tables and Figures

Page

Revision Summary

Revision Number	Date	Comments
R000	April 2014	Initial issue.
R001	September 2018	Revised to reflect the 2018 Pickering ‘A’ PSA update results.
R002	November 2023	Revised to reflect the 2023 Pickering ‘A’ PSA update results.
R003	January 2024	Revised to correct the typographical error in Table 20 in Revision R002 for the Large Release Frequency result of the 2023 Pickering 'A' Level 2 Outage PSA update.

Executive Summary

The objective of Probabilistic Safety Assessment (PSA) at Ontario Power Generation (OPG) Nuclear is to provide an integrated review of the adequacy of the safety of the current station design and operation for each nuclear power station. The Pickering Nuclear Generating Station ‘A’ (PNGS-A) PSAs are required to comply with the Canadian Nuclear Safety Commission (CNSC) Regulatory Document REGDOC 2.4.2 [R-1].

A PSA for a nuclear power plant identifies the various sequences that lead to radioactive material releases, assigns them to different categories of consequences, and calculates their frequencies of occurrence. Additionally, the PSA is used to identify the sources of risk and assess the magnitude of radiological risks to the public from potential accidents due to operation of nuclear reactors while at power as well as during outages. Furthermore, the PSA is used to assess the magnitude of radiological risks to the public from potential accidents due to the operation of the non-reactor facilities that contain sources of radioactivity. The PSA is a comprehensive model of the plant that incorporates knowledge about plant design, operation, maintenance, testing and response to abnormal events. To the extent possible, the PSA is intended to be a realistic model of the plant.

The PNGS-A PSA followed a quality assurance plan consistent with Canadian Standards Association standard CSA N286-12 [R-2] and CSA N299.1 [R-3]. The PSA was prepared using computer programs consistent with Canadian Standards Association standard CSA N286.7-16, Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants [R-4]. The PNGS-A PSA is in line with CSA standard N290.17-17 [R-5].

The PNGS-A PSA was prepared following methodologies consistent with best industry practice. All methodologies used in the preparation of the PNGS-A PSA were accepted by the CNSC under compliance with REGDOC 2.4.2 [R-1].

The baseline PNGS-A PSAs are documented in several reports:

- A hazard screening assessment identifies the hazards that require assessment in a PSA model.
- The Level-1 and Level-2 Internal Events At-Power PSAs assess the risk of severe core damage and radioactive releases from internal events occurring while the reactor is at power; i.e., it considers the challenges to reactor core cooling from accident sequences covering Design Basis Accidents (DBAs) and Beyond Design Basis Accidents (BDBAs) including Severe Accidents while the reactor is at full power.
- The Internal Events Outage PSA assesses the risk of severe core damage and large releases of radioactive material from internal events occurring while the reactor is in the Guaranteed Shutdown State (GSS); i.e., it considers the challenges to reactor core cooling from accident sequences during unit outages, including loss of shutdown heat sinks.
- The PSA-based Seismic Margin Assessment estimates the risk of severe core damage and large release from seismic events occurring while the reactor is at full power and provides an estimate of the containment failure frequency as a result of seismic events.

- The Internal Fire PSA assesses the risk of severe core damage from internal fires occurring while the reactor is at full power, and an estimate of the risk of large release as a result of internal fire events.

- The Internal Flooding PSA assesses the risk of severe core damage from internal floods occurring while the reactor is at full power, and a bounding estimate of the risk of large release as a result of internal floods.

- The High Wind PSA assesses the risk of severe core damage from high winds occurring while the reactor is at full power, and an estimate of the risk of large release as a result of high wind events.

- The Non-Reactor Sources PSA assesses the risk of radioactive releases from sources other than the reactor core.

The completion of the PNGS-A PSA has demonstrated that for each hazard the safety goals are met for Severe Core Damage Frequency (SCDF) and Large Release Frequency (LRF).

1.0 INTRODUCTION

The objective of Probabilistic Safety Assessment (PSA) at Ontario Power Generation (OPG) Nuclear is to provide an integrated review of the adequacy of the safety of the current station design and operation for each nuclear power station. The station PSAs are required to comply with the Canadian Nuclear Safety Commission (CNSC) Regulatory Document REGDOC-2.4.2 [R-1].

A nuclear PSA identifies the various sequences that lead to radioactive releases, assigns them to different categories of consequences, and calculates their frequencies of occurrence. Additionally, the PSA is used to identify the sources of risk and assess the magnitude of radiological risks to the public from potential accidents due to operation of nuclear reactors while at power as well as during outages. Furthermore, the PSA is used to assess the magnitude of radiological risks to the public from potential accidents due to the operation of the non-reactor facilities that contain sources of radioactivity. The PSA is a comprehensive model of the plant that incorporates knowledge about plant design, operation, maintenance, testing and response to abnormal events. To the extent possible, the PSA is intended to be a realistic model of the plant.

The PSA for the identified hazards for Pickering Nuclear Generating Station ‘A’ (PNGS-A), commonly referred to as PARA, provides an estimate of the station risk in its current configuration and is required for compliance with CNSC REGDOC-2.4.2 [R-1]. The PSA reflects the current station design and operation, is consistent with the OPG PSA methodology, and is consistent with best industry practice. The OPG PSA Methodologies have been accepted by the CNSC under REGDOC-2.4.2 [R-1]. A separate hazard screening assessment for internal and external events has been completed to confirm that no other identified hazards require assessment in a PSA.

The PNGS-A PSA was prepared following a quality assurance plan consistent with CSA standard CSA N286-12 [R-2] and CSA N299.1 [R-3]. The PSA was prepared using computer programs that were consistent with CSA N286.7-16 [R-4]. The PNGS-A PSA is in line with CSA standard N290.17-17 [R-5].

OPG has safety goals for Severe Core Damage Frequency[1] (SCDF) and Large Release Frequency[2] (LRF), as shown in Table 1. The intent of these goals is to ensure the radiological risks, arising from nuclear accidents associated with the operation of OPG’s nuclear power reactors, are low in comparison to risks to which the public is normally exposed. The baseline PARA studies show that the overall risk from the operation of PNGS-A is below the safety goals.

The first PARA studies for S-294 [R-6] compliance were completed in 2013 and the previous update was completed in 2018. All PARA studies have been updated in 2023 as part of the regular update cycle under REGDOC-2.4.2 compliance. The updates included:

- Station design, operation and analysis information up to the study freeze date of December 31, 2021;

---

[1] Severe Core Damage is the loss of core structural integrity.

[2] Large Release is a release greater than 1E14 Bq of Cs-137.

- Several model and documentation enhancements;
- Event and Fault tree modelling updates to reflect recent safety analysis, as well as PNGS-A design and operation; and
- The credit of Severe Accident Management Guidelines (SAMG) in the Level 2 PSA including Phase II Emergency Mitigating Equipment (EME).

This report summarizes the probabilistic safety assessments of PNGS-A and compares the results with OPG's Safety Goals, as shown in Table 1.

1.1 Objectives

The principal objectives of the PNGS-A PSA were:

1. To provide an integrated review of the adequacy of the safety of the current station design and operation;
2. To prepare a risk model in a form that can be used, in conjunction with ancillary application tools, to assist in safety-related decision making process, and
3. To assess risk results and ensure that they are acceptably low.

1.2 Scope

The baseline PNGS-A PSAs are addressed in ten separate assessments, as follows:

1. A PNGS-A Hazard Screening Assessment for internal and external hazards, which identifies the hazards that require further detailed analysis in a PSA.
2. A PNGS-A Level-1 Internal Events At-Power PSA (PARA-L1P). This PSA studies the risk of severe core damage from events occurring within the station (e.g., Loss Of Coolant Accidents (LOCA), steam line breaks) while the reactor is at full power; it considers the challenges to reactor core cooling from accident sequences covering Anticipated Occupational Occurrences, Design Basis Accidents, and Beyond Design Basis Accidents including Severe Accidents while the reactor is at full power.
3. A PNGS-A Level-2 Internal Events At-Power PSA (PARA-L2P). This PSA studies the frequency and composition of radioactive material releases to the environment resulting from events occurring within the station (e.g., LOCA, steam line breaks) while the reactor is at full power. This PSA is the extension of the Level-1 PSA (i.e., PARA-L1P) described in item 2.
4. A PNGS-A Level-1 Internal Events Outage PSA (PARA-L1O). This PSA studies the risk of severe core damage from internal events occurring at the station while the reactor is in the GSS. The outage PSA studies severe core damage due to failure to remove decay heat produced during unit outages, including loss of shutdown heat sinks.

5. A PNGS-A Level-2 Internal Events Outage PSA (PARA-L2O), which is a reduced scope Level 2 outage analysis based on modelling of accident progression and source term estimation and provides an estimation of the LRF.

6. A PNGS-A PSA-Based Seismic Margin Assessment (PSA-based SMA[3]), which studies the risk of severe core damage and large release from seismic events occurring while the reactor is at full power and provides an estimate of the containment failure frequency as a result of seismic events.

7. A PNGS-A Internal Fires PSA (PARA-IFPSA), which studies the risk of severe core damage and provides an estimate of LRF from internal fire events (e.g., fires caused by failures in station electrical equipment) occurring while the reactor is at full power.

8. A PNGS-A Internal Flooding PSA (PARA-Flood), which studies the risk of severe core damage and provides a bounding estimate of LRF from floods originating inside the station (i.e., pipe breaks of plant systems) occurring while the reactor is at full power.

9. A PNGS-A High Wind PSA (PBRA-Wind), which studies the risk of severe core damage and provides an estimate of LRF from high wind events (e.g., severe thunderstorms, tornadoes) occurring while the reactor is at full power.

10. A Pickering Nuclear Generating Station (NGS) Non-Reactor Sources PSA, which assesses the risk of releases to the environment from non-reactor sources of radioactivity.

The PARA reports, mentioned in bullet 2 to 10 above, do not cover the following potential sources of risk:

- Hazards from chemical materials used and stored at the plant;

- Other external Initiating Events (IEs) such as external floods, airplane crashes, train derailment, etc.; and

- Other internal IEs such as turbine missiles.

These types of hazards were addressed separately through screening studies or deterministic hazard studies (see Section 4.0). Consistent with industry practice, wilful acts (e.g., sabotage) are not modelled in the OPG PSAs.

The response of both PNGS-A units to various IEs is essentially identical. Therefore, it was generally only necessary to model a single unit, with this unit considered representative of the other unit. Unit 4 was selected as the reference unit. Design differences between units were not analyzed in detail as they were not expected to be significant in terms of risk.

---

[3] Pickering NGS A PSA-based SMA is also referred to as PARA-SEISMIC and would be used interchangeably in this report.

1.3 Organization of Summary Report

In addition to the general information presented in this introductory section, this Summary Report provides:

(a) A short description of the PNGS-A station and units (Section 2.0);

(b) An overview of PSA methods (Section 3.0);

(c) An overview of the hazard screening methods and the internal/external hazard screening assessment (Section 4.0);

(d) An overview of the methods used for Level 1 PSA (Section 5.0) and Level 2 PSA (Section 6.0); and

(e) A discussion of the main results of the PARA studies (Section 7.0).

Appendix A contains a list of the abbreviations and acronyms used in this report.

2.0 PLANT DESCRIPTION

The following sections provide a short description of the Pickering site and plant.

2.1 Site Arrangement

PNGS-A comprises four CANDU pressurized heavy water nuclear reactors, four Turbine Generators (TGs) and their associated equipment, services and facilities. Currently Units 1 and 4 are operating and Units 2 and 3 are in safe storage. The arrangement of the eight-unit Pickering site (PNGS-A and PNGS-B) is shown in Figure 1. PNGS-B comprises the other four units (Units 5 to 8) at the site.

The design net electrical output of each unit is 515 MWe at a 90 percent power factor, yielding a total station net output of 1030 MWe. Power is produced at 24 kV and delivered at 230 kV and 60 Hz to the Southern Ontario grid. The station is designed for base-load operation.

Each unit comprises a power source capable of operating independently of the other units with reliance on certain common services. The power generating equipment of each unit is a conventional steam-driven turbine generator. The associated heat source is a heavy water moderated, pressurized heavy water cooled, natural uranium dioxide fuelled, horizontal pressure tube reactor. This type of nuclear steam supply is used in all nuclear power stations built in the province of Ontario.

2.2 Buildings and Structures

The principal structures at the Pickering A site are as follows:

(a) Four reactor buildings;

(b) A reactor auxiliary bay;

(c) A powerhouse, including the turbine hall and turbine auxiliary bay;

(d) A Vacuum Building, together with its associated Pressure Relief Duct (PRD);

(e) A service wing;

(f) An administration building;

(g) An Irradiated Fuel Bay (IFB) and an Auxiliary Irradiated Fuel Bay (AIFB);

(h) A heavy water (D_2O) upgrading building;

(i) A screenhouse;

(j) A water treatment building;

(k) A High Pressure Emergency Coolant Injection (HPECI) pumphouse;

(l) An HPECI water storage tank;

(m) Two buildings housing unitized instrument rooms for the Shutdown System Enhancement (SDSE) program; and

(n) EME buildings and outdoor portable generator area.

The administration and service buildings, the heavy water upgrading building, the vacuum building, the HPECI structures, the EME buildings and the Auxiliary Power Supply (APS) building serve the entire eight-unit station.

The containment boundary is formed by the reactor buildings, the PRD, the vacuum ducts and the vacuum building. Each reactor building is a reinforced concrete structure with cylindrical walls and an elliptical dome. The vacuum building is also a reinforced-concrete structure with a cylindrical wall and a flat roof. A tank in the top of the vacuum building contains water for the dousing system. A reinforced concrete ring around the vacuum building, outside the perimeter wall near the base, provides additional pressure retaining capability. The PRD, also a reinforced concrete structure, is rectangular in section and is linked to the vacuum building by steel vacuum ducts 1.8 m in diameter.

Unit emergency control centers (UECCs), one for each unit, are located under the PRD.

The reactor auxiliary bay runs the full length of the station, joining at its eastern end, the ‘B’ station reactor auxiliary bay. It is a conventional four-story steel frame building fitted around the northern halves of the four reactor buildings. It houses some reactor auxiliary systems, the Main Control Room (MCR) and the IFB, located at the mid point of the "A" station, between Units 2 and 3.

The service wing extension is located at the eastern end of the Pickering ‘A’ station, (i.e., in the center of the eight units), and provides additional space for waste management, laboratories, stores, locker and change facilities, maintenance shops, fuelling machine dismantling facilities and offices. The service wing basement contains the waste management facilities. The station administration building is connected by a bridge to the upper floor of the service wing. This bridge is the main entry and exit route for station personnel to all work areas and contains the final monitoring station.

In support of the Large Scale Fuel Channel Replacement Program for Units 1 to 4, an extension to the west end of the Pickering NGS ‘A’ reactor auxiliary bay and to the east end of the Pickering NGS ‘B’ reactor auxiliary bay have been constructed. These extensions are conventional two-story steel frame structures.

The EME buildings and outdoor portable generator storage area are located north of the Brock Road Security building. The EME building houses portable fuel totes, portable pumps and portable generators.

2.3 Reactor

The reactor consists of a horizontal cylindrical structure (the calandria) filled with heavy water and penetrated by 390 horizontal tubes, 390 fuel channel assemblies and reactivity monitoring and control units. Below this is a large cylindrical tank (the dump tank) connected to the reactor by four goose-neck pipes, to provide rapid draining of the moderator water from the calandria. The calandria and dump tank are housed in an air-filled heavy-concrete vault. The ends of the calandria assembly (the end shields) are located in openings in the calandria vault wall and form part of the vault enclosure. The end shields (in conjunction with shield plugs in the fuel channels) provide sufficient shielding against radiation from the reactor and its fuel to permit personnel access to the fuelling machine vaults when the reactor is shutdown. An arrangement of embedded pipes carrying natural water provides cooling for the vault concrete.

A typical PNGS-A reactor assembly is illustrated in Figure 2.

2.4 Fuel and Fuel Handling

The fuel is in the form of compressed and sintered natural uranium dioxide pellets, which are sheathed and sealed in Zircaloy-4 tubes. Twenty-eight tubes are assembled between two end plates to form one fuel bundle. The tubes have a thin layer of graphite on the inner surface which reduces susceptibility to stress corrosion cracking on reactor power ramps. Each fuel bundle has an outside diameter of 100 mm and weighs 22.5 kg. Each of the reactor's 390 fuel channels contains 12 fuel bundles to provide a total of 4680 bundles per reactor.

The reactors are fuelled on-power. Each reactor is serviced by two remotely controlled fuelling machines, one at each reactor face, which operate at opposite sides of the same fuel channel, match primary heat transport (PHT) system pressure, open the channel and insert fresh fuel or remove irradiated fuel, without interrupting reactor operation.

Irradiated fuel is transferred by an elevator and conveyor to the primary IFB where it remains for a minimum of four years before transfer to the AIFB. The two bays' combined storage capacity is 22 station years irradiated fuel accumulation. After a minimum 10 years cooling in the AIFB, irradiated fuel is loaded into the dry storage containers, which are transferred for processing and storage to the Pickering Waste Management Facility (PWMF). The PWMF provides sufficient capacity to store the used fuel generated from the Pickering reactors until the end of the station's service life.

2.5 Reactivity Control Mechanisms and Systems

In-core neutron flux detectors are used to measure neutron flux in specific areas of the core. These are supplemented by ion chambers and fission chambers located on the south side of the calandria shell. Signals from these detectors are supplied to the Reactor Regulating System (RRS) and/or the Shutdown System (SDS).

Fast shutdown of the reactor following a plant upset is accomplished by the SDS. The SDS releases 23 stainless steel clad cadmium shutoff rods into the reactor core. To augment shutdown, the heavy water moderator in the calandria can be dumped into the dump tank.

A liquid zone control system is used for reactivity control and consists of vertical tubes containing natural water. Varying the level of the water in each tube changes the local neutron absorption in each zone of the reactor, thereby controlling the local neutron flux level and hence the reactor neutron flux shape. Varying the water level in all of the tubes provides control of overall reactor power. The removal of vertical stainless steel adjuster rods from the core provides excess reactivity for shim operation; however, the adjuster rods have been immobilized in core in their fully inserted position.

2.6 Heat Transport System

The Heat Transport System (HTS) consists of two identical loops, linked by two interconnect valves, one of which is open during full power operation. Each loop consists of fuel channels filled with natural uranium fuel bundles surrounded by pressurized heavy water, boilers, circulation pumps, valves and associated piping. The coolant in the fuel channels removes the heat generated by the fuel. During normal operation the heat from the fuel is generated by nuclear fission, following shutdown the heat from the fuel is generated by fission product decay. During normal operation, the HTS main circulating pumps transport the heat to the boilers.

The HTS interfaces with a number of systems, e.g.:

- The Shutdown Cooling System (SDCS), which removes decay heat when the reactor is shutdown;
- The feed and bleed system, which provides pressure and inventory control for the coolant;
- The D_2O recovery system, which recovers lost heavy water from leaks; and
- The Emergency Coolant Injection System (ECIS), which adds light water to the HTS following a LOCA beyond the capacity of the D_2O recovery system.

2.7 Moderator System

During normal plant operation the moderator system is used to slow the neutrons produced by the reactor in order to maintain a critical fission reaction. Heat is generated in the moderator by the neutrons as they slowdown, and energy is transferred to the moderator from the calandria tubes, shell, tube sheets and, reactivity mechanisms. During normal operation a small fraction of the heat produced by the fuel is transferred to the moderator. The moderator system includes pumps and heat exchangers (HXs) to remove this heat. After an accident, the moderator can be used as an additional heat sink to remove decay heat from the reactor. This additional heat sink is an important, unique feature of the CANDU reactor design.

2.8 Feedwater and Condensate System

The main role of the HTS is to transport the heat generated in the fuel channels to the boilers. The role of the boilers is to transfer this heat and boil the light water on the secondary side of the boilers. The steam generated in the boilers is then used to spin the TG to convert the thermal energy to electrical power. During this process, the boiling water condenses. The condensate is returned to the feedwater system and eventually returned to the boilers to continue the process.

2.9 Main Steam System

Steam is produced in 12 boilers and fed into four separate steam mains which pass through the reactor building wall to the turbine building where they connect to the turbine steam chest. Over-pressure protection is provided by the steam relief system.

2.10 Steam Relief System

The steam relief system protects the steam generators from overpressure and is also used for rapid cooling of the HTS when needed. Eight steam reject valves, six large valves and two small valves, are provided to permit a poison prevent capability. The large steam reject valves also provide the capability to rapidly depressurize the boilers and the HTS in an emergency.

2.11 Boiler Emergency Cooling System

The Boiler Emergency Cooling System (BECS) is designed to provide a short term supply of cooling water to the boilers in the event of a total loss of feedwater. This system is designed to be used until an alternative heat sink can be placed in service.

2.12 Emergency Boiler Water Supply System

The Emergency Boiler Water Supply System (EBWS) supplies emergency make-up to the PNGS-A boilers from the Pickering Nuclear Generating Station ‘B’ (PNGS-B) High Pressure Service Water System (HPSW). The piping system runs from the Pickering ‘B’ HPSW through the basement of the turbine auxiliary bay to the Pickering ‘A’ units. The piping contains manual valves and motorized valves. The motorized valves are supplied from the Class III power system, with a backup from the Site Electrical System via the interunit transfer busses. The motorized valves may also be opened manually.

The PARA includes models for the PNGS-B systems that are required to support the PNGS-B HPSW.

2.13 Powerhouse Emergency Venting System

The Powerhouse Emergency Venting System (PEVS) is used to mitigate harsh environments caused by high temperature or high humidity in the powerhouse, due to steam line or feedline breaks.

2.14 Special Safety Systems

Three special safety systems are incorporated into the plant design to limit radioactive releases to the public following an abnormal event:

(a) SDS;

(b) ECIS; and

(c) Negative Pressure Containment System (NPCS).

2.14.1 Shutdown System

The function of the SDS is to shut down the reactor when any one of the trip parameters in either Shutdown System A (SDSA) or Shutdown System Enhancement (SDSE) exceeds its setpoint. SDSA and SDSE each have its associated instrumentation to monitor their trip parameters and channelized logic to activate the shutdown mechanisms. SDSA monitors 10 parameters and SDSE monitors 4 parameters.

The shutdown mechanisms are:

- The shutoff rod system.

  There are a total of 23 vertical stainless steel cladded cadmium shut off rods for Units 1 and 4. Each rod is suspended by a drive mechanism which is essentially a sheave and cable, driven by a three-phase electric motor through an electromagnetic clutch. When a trip signal is received, the electromagnetic clutch on each shutoff rod is de-energized and the shutoff rod falls into the core.

- Moderator dump.

  A moderator dump system is provided to augment the shutoff rods. A dump signal causes large valves between the calandria and the dump tank to open, equalizing the pressure between the two tanks, allowing the heavy water moderator in the calandria to rapidly drain to the dump tank. Automatic operation of the dump system occurs when reactor power has been measured as not decreasing fast enough, or not reaching a sufficiently low level, following operation of the SDS.

2.14.2 Emergency Coolant Injection System

The ECIS provides make-up cooling water to the HTS following a postulated LOCA. The PNGS-A ECIS includes an initial high pressure injection from the HPECI system, shared with PNGS-B, and a low pressure recovery injection.

2.14.3 Negative Pressure Containment System

The NPCS provides a physical barrier designed to limit the release of radioactive material to the environment, which might result from a process or system failure. The containment system is a reinforced concrete envelope around the nuclear components of the reactor cooling system, with provisions for controlling and maintaining a negative pressure within the envelope before and after accidents.

The NPCS includes a number of sub-systems required for providing normal and post-accident functions such as reactor building cooling, pressure suppression, control of hydrogen, and air discharge filtration.

2.15 Support Systems

Support systems are considered in the risk assessment as they provide common services to the systems described above. Failure of the support systems can result in failure of the mitigating systems credited to remove heat after an initiating event. The following systems are modelled as support systems in the PSA.

2.15.1 Electrical Power Systems

The electrical systems at Pickering ‘A’ are organized into four classes:

1. Class IV power is the main site electrical power supplied from a combination of the provincial electrical grid and the station generating unit transformers;
2. Class III power is the back-up supply to Class IV and provides alternating current supplies for safety related equipment and auxiliaries. Class III power includes three standby generators for each paired unit (1/4 or 2/3);
3. Class II power is primarily used to supply continuous alternating current to control and monitoring systems, instrumentation, and protection systems; and
4. Class I power is a continuous direct current supply primarily used to supply motive power to electrical breakers.

Class II and Class I both have battery backup supplies.

Standby power supplies to the unit loads are provided by three distinct systems:

1. The Site Electrical System (SES): This standby power source is comprised of two permanently energized busses to which all eight units at the Pickering site have access;
2. The Standby Generators (SGs): This power source is comprised of six independent oil turbine driven generators. The standby power is available to only the portion of the service loads required to support safe shutdown of a unit; and
3. The Auxiliary Power System: This system is comprised of two 100% redundant Combustion Turbine Unit (CTU) driven generators that can supply Class IV power to selected Group 1 Class IV loads through the SES following a total loss of Class IV power across the Pickering ‘A’ and ‘B’ stations following a Loss of Bulk Electrical Supply (LOBES). The APS supply is independent of the Bulk Electrical System and the normal station Class IV power supply.

2.15.2 Service Water Systems

The service water systems provide cooling water for various loads. The service water systems for PNGS-A consist of:

(a) Service Water System:

Service water is drawn from Lake Ontario through an open canal bounded by two rock filled groynes extending into the lake. The water is drawn from the canal to an open forebay, then through a common screen house into an enclosed concrete duct or intake channel. The service water system is divided into two sub-systems referred to as low pressure service water and HPSW. The LPSW pumps, powered from the Class IV electrical system, draw water from the intake channel. The HPSW pumps, also powered from the Class IV electrical system, draw water from the discharge of the LPSW pumps, and provide a pressure boost to deliver service water to higher elevations in the plant. Service water is used once and returned to the lake.

In the event of a failure of the Class IV electrical power system, service water is provided to key safety related loads by the emergency low pressure service water system and the emergency high pressure service water system. These systems are powered from the Class III electrical system and draw water directly from the intake channel.

(b) Recirculated Cooling Water System:

The Recirculated Cooling Water (RCW) system provides clean, demineralized cooling water to equipment that might become contaminated or plugged if supplied by raw lake water. The RCW system recirculates water via a set of pumps and cools the water via a set of HXs. The LPSW system is used on the secondary side of the RCW system HXs for cooling purposes.

(c) Emergency Storage System:

The Emergency Water Storage (EWS) system is a redundant water supply, designed to provide cooling water in the event that other sources of water fail. The water storage tank in the top of the vacuum building serves as an emergency supply of service water to all reactor units in the event of failure of both Class IV and Class III power. A common header connects the HPSW supply of each unit to the EWS tank.

2.15.3 Instrument Air Systems

The instrument air supply is a support system providing compressed air. This compressed air is used for various plant activities including operating valves, starting motors, and inflating airlock seals. The instrument air systems are comprised of the High Pressure Instrument Air (HPIA) system, the low pressure instrument air system and the backup instrument air system.

The backup instrument air system is designed to provide instrument air to key safety related loads following failure of the high and low pressure systems. Its source is a central bottle station, consisting of compressed air cylinders, and piping to critical equipment in the reactor auxiliary bay and the pressure relief duct.

2.15.4 Cooling and Ventilation Systems

The cooling and ventilation system provides heating and cooling to the station buildings. Failure of the cooling and ventilation in these rooms may result in equipment failures in the support or mitigating systems.

2.16 Emergency Mitigating Equipment

As a result of Fukushima, OPG has implemented EME for Pickering NGS ‘A’. The EME was designed to cope with a total loss of heat sink caused by a complete loss of all AC power. OPG has adopted a two-phase approach for the implementation of EME.

Phase I focuses on prevention of severe accidents by addressing immediate actions required to maintain cooling of reactor fuel and short-term actions to maintain cooling of fuel in IFBs. The PNGS ‘A’ phase I EME consists of:

- Four (two for each unit) 120 V Portable Uninterruptable Power Supplies (PUPS) that are used to provide power to instrumentation until the power is restored by the diesel generators.
- Two portable 15 kW diesel generators (one for each unit) available to provide emergency power to critical safety monitoring instrumentation at PNGS ‘A’.
- One HL260M pump that is shared between PNGS-A and PNGS-B, which supplies make-up water to ECI storage tank for both PNGS-A and B.
- Three HL5M pumps which are deployed to the Reactor Auxiliary Bay (RAB) in units 1, 2 and 4. The unit 1 pump provides cooling to the unit 1 moderator via ECI. The unit 2 pump provides cooling to the unit 1 and 4 boilers via EBWS and cooling water to the AIFB. The unit 4 pump provides cooling to the unit 4 moderator via ECI and cooling water to the IFB-A.

Phase II EME supports long term actions intended to sustain fuel cooling and ensure containment integrity in the unlikely case that Phase I EME fails to prevent progression to a severe accident. Phase II consists primarily of large electrical generators (1.4 MW) which are deployed to power available support systems such as service water, essential instrumentation, Containment Air Cooling Units (ACUs) and moderator pumps. The objective of Phase 2 EME is to continue recovery of affected units to a stable state, and also includes actions needed if initial actions are not successful and use of Severe Accident Management Guidelines (SAMGs) become necessary. Phase 2 EME consists of:

- Five 1.4 MW generators capable of supplying a steady-state load to the Class III distribution system (shared between all units at PNGS and DNGS) that are used along with portable switchgear, which can then be used to supply power to:

  (1) Class II emergency power supply.

  (2) Emergency Water Supply System main pump, recovery pump, strainers and travelling screens.

  (3) Boiler room and FM Vault ACU fans.

  (4) Filtered Air Discharge System (FADS).

  (5) ECI Recovery pumps and sump pumps.

3.0 OVERVIEW OF PSA METHODS

The purpose of a PSA is to establish whether the design and operation of the plant poses an acceptable level of risk to the public and to identify the major sources of risk. Risk is defined as the frequency of occurrence of an event multiplied by the consequence of the event, and is expressed in units of consequence per unit of time. For example, consider a residential sump pump that fails on average once every four years. If the consequence of the pump failing is $1000 in property damage, then the average risk from failure of the pump is $250 per year.

Risk 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 PSA 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.

For a Nuclear Generating Station, the events studied are those leading to damage to fuel both in the core and out of core or releases of radioisotopes into the environment. Consistent with the requirements of the CNSC REGDOC-2.4.2 [R-1], OPG has completed hazard screening, Level 1 and Level 2 PSAs to assess the risk from PNGS-A:

- A hazard screening assessment was performed to confirm which hazards can be screened out from PSA, and identify which hazards need to be assessed by a PSA. This includes non-reactor sources as well;
- Level 1 of the PSA assesses the frequency of varying degrees of fuel failures, which lead to release of radioactivity into containment; and
- Level 2 of the PSA assesses the frequency and magnitude of the release of this radioactivity from containment to the outside environment.

OPG’s safety goals in Table 1 for PSA correspond to the Level 1 and Level 2 PSA results.

Level 1 PSAs have been prepared for full reactor power operation for the following types of IEs based on the hazard screening results:

- Internal IEs (e.g., steam line break, LOCA);
- Seismic events;
- Internal fire (fires initiated by in plant sources, e.g., electrical equipment);
- Internal flooding (floods originating from water sources internal to the plant); and
- High winds (including both straight line winds and tornadoes).

The methodologies for the detailed Level 1 PSAs are summarised in Section 5.0 of this report.

An assessment of risk while a single unit is in GSS was prepared for internal IEs. Outage PSAs have not been prepared for seismic events, high winds, internal fires, and internal flooding for the reasons described below:

- An outage seismic PSA was not performed as the risk from a seismic event while a unit is shutdown is acceptably low or is bounded by the seismic risk for an at-power unit. The key factors supporting this assertion are that:
    1. A seismic event and failure to remain shutdown is not a significant contributor to risk. This results from the provision of two reliable lines of defense to prevent criticality.
    2. Given the above, seismic risk is dominated by sequences involving the failure of all heat sinks.
        - A seismic event will have a similar effect on the heat sinks for shutdown and at-power units.
        - The SCDF for at-power seismic events is 1.2E-06/yr.
            - Non-seismically qualified[4] (NSQ) SSCs are credited in seismic events of low magnitude as follows:
                - The plant response to low-intensity earthquakes with magnitude below 0.1g PGA is assumed to be similar to the transient following the forced shutdown (FSD) initiating event modelling in PARA-L1P.
                - Following the FSD event, both seismically qualified (SQ) and NSQ mitigating functions are credited.
                - The seismic robustness of the NSQ SSCs up to the earthquake magnitude of 0.1g PGA is assessed based on a sample of representative SSCs.
                - The plant response to strong earthquakes with magnitude greater than 0.1g PGA credits only SQ SSCs and EME.
        - Initial reactor power is at least two orders of magnitude less for a shutdown unit than for an at-power unit. Therefore, the fuel temperature will be lower, accident progression will be slower, and the amount of energy deposited into containment will be lower. This reduces the potential for consequential challenge to containment integrity from a severe accident in a single shutdown unit.
        - Containment failure and releases to the environment occur, if at all, much later for a shutdown unit than for an at-power unit.

---

[4] The PNGS-A has not been seismically qualified during the design stage. However, SSCs required for a safe shutdown after a seismic event were identified and assessed in the PNGS-A SMA [R-7]. This assessment is equivalent to a seismic qualification as per CSA N289.1-18 [R-8]. Seismically assessed SSCs will be, therefore, referred further as seismically qualified (SQ).

    - The inventory of radioactive material available for release to the environment is less for a shutdown unit due to the decay of short-lived isotopes.
    - The operation of key containment systems is largely unaffected if a single unit is shutdown.
  3. On average, a unit is shutdown for an outage (planned or forced) for approximately 22% of the operating cycle. Therefore, the exposure to low frequency events such as seismic events is much lower for a shutdown unit than for an at-power unit.
  4. Risk management programs are adequate to control the risk from a seismic event while a unit is shutdown.
- An internal fire outage PSA was not performed as the risk from an internal fire while a unit is shutdown is either acceptably low or is bounded by the risk from internal fires for an at-power unit. The key factors supporting this assertion are that:
  1. An internal fire and failure to remain shutdown is not a significant contributor to risk. This results from the provision of two reliable lines of defense to prevent criticality.
  2. Given the above, the fire risk is dominated by sequences involving the failure of all heat sinks.
    - An internal fire event will have a similar effect on the heat sinks for shutdown and at-power units.
    - The SCDF for at-power fire events is 4.65E-06/yr.
    - Initial reactor power is at least two orders of magnitude less for a shutdown unit than for an at-power unit. Therefore, the fuel temperature will be lower, accident progression will be slower, and the amount of energy deposited into containment will be lower. This reduces the potential for consequential challenge to containment integrity from a severe accident in a single shutdown unit.
    - Containment failure and releases to the environment occur, if at all, much later for a shutdown unit than for an at-power unit.
    - The inventory of radioactive material available for release to the environment is less for a shutdown unit due to the decay of short-lived isotopes.
    - The operation of key containment systems is largely unaffected if a single unit is shutdown.
  3. On average, a unit is shutdown for an outage (planned or forced) for approximately 22% of the operating cycle. Therefore, the exposure to low frequency events such as fires is much lower for a shutdown unit than for an at-power unit.
  4. Risk management programs are adequate to control the risk from an internal fire while a unit is shutdown.
- An outage internal flood PSA was not performed as the risk from an internal flood while a unit is shutdown is either acceptably low or is bounded by the flood risk for an at-power unit. The key factors supporting this assertion are that:

1. An internal flood and failure to remain shutdown is not a significant contributor to risk. This results from the provision of two reliable lines of defense to prevent criticality.
2. Given the above, the risk from internal floods is dominated by sequences involving the failure of all heat sinks.

    - An internal flood event will have a similar effect on the heat sinks for shutdown and at-power units.

    - The SCDF for at-power flood events is 2.04E-06/yr.

    - Initial reactor power is at least two orders of magnitude less for a shutdown unit than for an at-power unit. Therefore, fuel temperatures will be lower, accident progression will be slower, and the amount of energy deposited into containment will be lower. This reduces the potential for consequential challenge to containment integrity from a severe accident in a single shutdown unit.

    - Containment failure and releases to the environment occur, if at all, much later for a shutdown unit than for an at-power unit.

    - The inventory of radioactive material available for release to the environment is less for a shutdown unit due to the decay of short-lived isotopes.

    - The operation of key containment systems is largely unaffected if a single unit is shutdown.

3. On average, a unit is shutdown for an outage (planned or forced) for approximately 22% of the operating cycle. Therefore, the exposure to low frequency events such as floods is much lower for a shutdown unit than for an at-power unit.
4. Risk management programs are adequate to control the risk from an internal flood while a unit is shutdown.

- An outage high wind PSA was not performed as the risk from a high wind while a unit is shutdown is low and it is bounded by the risk from high winds while a unit is at high power. The key factors for this assertion are that:

    1. A high wind event and failure to remain shutdown is not a significant contributor to risk. This results from the provision of two reliable lines of defense to prevent criticality.

    2. Given the above, the risk from high winds is dominated by sequences involving the failure of all heat sinks.

        - A high winds event will have a similar effect on the heat sinks for shutdown and an at-power units

        - The SCDF for at-power high winds events is 2.3E-05/yr.

- Initial reactor power is at least two orders of magnitude less for a shutdown unit than for an at-power unit. Therefore, fuel temperatures will be lower, accident progression will be slower, and the amount of energy deposited into containment will be lower. This reduces the potential for consequential challenge to containment integrity from a severe accident in a single shutdown unit.

- Containment failure and releases to the environment occur, if at all, much later for a shutdown unit than for an at-power unit.

- The inventory of radioactive material available for release to the environment is less for a shutdown unit due to decay of short-lived isotopes.

- The operation of key containment systems is largely unaffected if a single unit is shutdown.

3. On average, a unit is shutdown for an outage (planned or forced) for approximately 22% of the operating cycle. Therefore, the exposure to low frequency events such as high winds is much lower for a shutdown unit than for an at-power unit.

4. Risk management programs are adequate to control the risk from a high winds event while a unit is shutdown.

For PNGS-A, a detailed Level 2 PSA was prepared for internal events while both reactors are at full power. Reduced scope at-power Level 2 assessments have been prepared for seismic events, outage internal events, internal fires, internal flooding and high winds as follows:

- The Level 2 assessment for seismic events considers the likelihood of consequential failure of containment due to an earthquake, and then provides a bounding assessment of LRF due to seismic failure modes of containment following severe core damage caused by an at-power seismic event. It is conservatively considered that the LRF estimate is equal to the SCDF estimate.
- The Level 2 assessment of outage internal events reviews the potential for unique containment challenges or bypass pathways in the outage state caused by severe core damage from an internal initiating event occurring while the reactor is in the GSS and provides an estimated LRF.
- The Level 2 assessment for internal fire events is built on the Level 1 quantification to consider the Level 2 at-power impacts of fire scenarios and provides a bounding estimate of LRF.
- The Level 2 assessment for internal flooding provides an estimate of the LRF from internal floods at-power given a subdivision of the Level 1 quantification results into different types of sequencies (single-unit, multi-unit) and based on the insights from the PNGS-A and PNGS-B Level 2 at-power PSAs.
- The Level 2 assessment for high winds is based on a combination of the Level 1 high wind PSA results with insights from the PARA Level 2 at-power study and provides a bounding LRF estimate.

Additionally, bounding assessments for non-reactor sources (IFB and used fuel dry storage) were performed. The methodologies for these assessments are summarised in Sections 6.2 to 6.7 of this report.

In the following sections, the methods used for hazard screening, Level 1 and Level 2 Internal Events PSAs, hazard PSAs, and Non-Reactor Sources PSA are described.

4.0 HAZARD SCREENING METHODS

A hazard is an event or natural phenomenon that has the potential for causing an undesirable consequence. Hazards can be divided into two groups: external and internal. External hazards include events such as flooding and fires external to the plant, tornadoes, earthquakes, and human induced events such as aircraft crashes or transportation accidents. Internal hazards include events such as equipment failures, operator induced events, flooding and fires internal to the plant. The purpose of hazard screening analysis is to determine which hazards can be screened out from PSA, and identify which hazards need to be assessed by a PSA. The screening assessment addresses both the reactor and non-reactor sources. In the latter category, the following two sources are considered in the PNGS-A PSA:

(a) Fuel in wet storage in the Irradiated Fuel Bays (IFBs); and

(b) Fuel in dry storage in the Used Fuel Dry Storage (UFDS) facility.

These sources were assessed because, following an initiating event, these non-reactor sources have the potential to release Cs-137 higher than the threshold for a large release (1E+14 Bq).

4.1 External Hazard Screening for Reactor Sources

External hazards are defined as hazards that are initiated outside the OPG exclusion zone or are hazards that are outside the plant’s direct control. These hazards could be in the form of natural hazards (ice-storms, flood, etc.) or man-made hazards (chlorine leak from a rail-car derailment, aircraft crashes, etc.).

4.1.1 Overview of External Hazards Screening Method

The external hazards screening method involves three main steps:

1. Identify all the external hazards applicable to the site.
2. Determine consequences of hazards and accident scenarios. Screen-out events qualitatively based on the consequence of events.
3. Determine the likelihood of an event occurring. Screen-out events quantitatively based on the likelihood of the event occurring, or on the likelihood of the event leading to a severe accident (e.g., SCDF) or Conditional Core Damage Probability (CCDP).

The hazard screening flow diagram of steps is shown in Figure 3. A generic list of the hazards is developed based on a literature review and is reviewed and rationalized by a group of risk assessment experts to come up with a refined master list. Once the hazards are identified, the screening process begins with qualitative assessment of hazards impact and consequences of events, followed by quantitative assessments.

The qualitative screening steps QL1 to QL7 discussed below are the criteria for qualitative screening.

[QL1] The first qualitative criterion is if the event is of equal or lesser damage potential than similar events for which the plant has been designed.

After the hazards are identified and determined their impact could be beyond the design basis of the plant, the scenarios need to be defined for each hazard, and it needs to be determined how far from the station they take place and how they can potentially impact the plant's operation.

[QL2] For each scenario, it has to be determined if there are other bounding events. If the hazard imposes lower risk (frequency and consequence) than another hazard, it can be screened out.

[QL3] Once the hazard distance is determined, it can be assessed whether it can be screened based on the distance from the plant. For screening purposes a screening distance value (SDV) is defined by the OPG Hazard Screening Guide, which is the distance from a facility beyond which, potential sources of a particular type of external event can be ignored. The SDV is different for different hazards. Generally, the safe distance is a distance beyond which a hazard source is too weak to impact nuclear safety.

[QL4] If the event is included in the definition of another event or bounded by other event, it can be screened out from any further assessment.

[QL5] Events that progress slowly and it can be demonstrated that there is sufficient time to eliminate the source of the threat or provide an adequate response, can be screened out.

[QL6] If the event does not cause an initiating event (or the need to shutdown), "and" does not result in loss of a safety system, it can be screened out.

If the event were to cause an initiating event, and not cause loss of a safety system, then the event would be similar to a transient (such as a turbine trip or loss of offsite power) in the internal events PSA.

[QL7] If the hazard does not result in actuation of a front-line system (i.e., a system that directly performs accident mitigating functions), then it is not necessary to evaluate the consequences of the hazard, and it can be screened out.

At this stage of the screening, all qualitative criteria are examined and if the hazard still has not been screened out by any of the seven deterministic criteria, quantitative screening would be required as per Table 2.

Those hazards subjected to all qualitative and quantitative criteria, but cannot be screened out will require a more detailed assessment using a PSA.

4.1.2 Human-Induced External Hazards

All human-induced (man-made) external hazards identified for PNGS-A are reviewed and examined against the methodology described in Section 4.1.1. All human-induced external hazards are screened out, and do not require further analysis. A list of the human-induced hazards assessed is presented in Table 3.

4.1.3 Natural External Hazards

A Review Level Condition (RLC) needs to be defined for each natural hazard during screening assessment and is used to assess the impact on nuclear safety. The RLC is normally defined as a beyond-design-basis event, as the natural hazards within the design basis should not have any significant impact on the plant's operation and safety. The concept of RLC implies a particular level of hazard which challenges the systems, structures and components (SSCs) on the site. Selection of RLC is based on:

- Canadian and International regulations and standards,
- Information on credible hazards at the plant site,
- Or alternatively, the RLC can be established for the corresponding screening frequency.

PSA screening analysis for natural external hazards was conducted in accordance with the methodology described in Section 4.1.1. A set of RLCs were defined and used in the screening analysis. All natural external hazards have been screened out, except for seismic events, extreme low and high temperatures, high wind events (including hurricanes and tornadoes), ice storms, and lake animals. A list of the natural external hazards considered is presented in Table 4. Seismic and high wind (including straight-line winds and tornados) PSAs have been developed for PNGS-A, see details in Section 5.5 and Section 5.6, respectively. In addition, the effects of ice storms, extreme temperatures, and lake animals are modelled in the internal events PSA (see Section 5.1).

4.1.4 Combined External Hazards

Combinations of external hazards may have a significant impact on diverse safety systems at the same time. Therefore, evaluation of the combination of events is an essential part of the external hazards screening for PSA to ensure the consequences of combinations are not disproportionate. Combined external hazards include combinations of human induced hazards with natural hazards, human induced hazards with other human induced hazards, as well as, combinations of natural hazards. In particular, some combinations of natural hazards can be correlated (e.g., high winds and flooding can both occur in summer storms) and could potentially produce the most severe impacts challenging the safe operations of the nuclear plants. Review of the international practices shows that combinations of external hazards are considered only if the hazards are correlated and dependent. Independent combinations of beyond design basis hazards usually have an extremely low likelihood of occurrence. The objective of the assessment was to ensure the combinations would not have significant impacts on diverse safety systems at the same time, and do not impose disproportional risks to the station's safe operation. Several hundred combinations of external hazards were assessed. The combined hazard assessment did not identify any hazard combination that requires additional PSA assessments.

4.2 External Hazards Screening for Non-Reactor Sources – IFB

Screening assessments for the hazards for the IFB is based on the following considerations and insights:

- Loss of IFB Heat Sink
- Loss of IFB Water Inventory

The above conditions can adversely impact the ability to prevent IFB fuel to uncover, as follows:

- Reduced IFB water level can result in increased radiation fields in and near the IFB with the potential to inhibit corrective operator field actions such as equipment repair and IFB inventory make-up.
- Boiling of IFB water can result in harsh environment with the potential to cause IFB equipment failure and inhibit corrective operator field actions.
- IFB inventory leakage events (e.g., pipe break) can cause IFB equipment failure and inhibit corrective operator field actions

4.2.1 Human-Induced External Hazards

The methodology used for screening the human-induced external hazards for IFB is the same as described in Section 4.1.1. A list of the human-induced external hazards assessed is presented in Table 5.

The hazards not screened out in Table 5 were addressed in the Non-Reactor Source PSA (see Section 6.7).

4.2.2 Natural External Hazards

A list of natural external hazards were assessed through a hazard screening assessment to determine if they are applicable to the IFB at the PNGS-A.

Similar to Section 4.1.3, the RLCs defined for the reactor units are considered applicable to the IFB because the reactor units and IFB are at the same site. The list of natural external hazards can be found in Table 6.

The hazards that were not screened out in Table 6 were addressed in the Non-Reactor Source PSA (see Section 6.7).

4.2.3 Combined External Hazards

Specific combinations of external hazards are not explicitly reviewed. Instead, it is judged that the effect of any combination of hazards (correlated, consequential, and coincidental) would be bounded by the IFB Loss of Heat Sink scenario.

4.3 External Hazards Screening for Non-Reactor Sources – Used Fuel Dry Storage (UFDS)

Once the fuel has resided in the IFBs for a minimum of ten years, the residual decay heat is sufficiently low to allow this fuel to be moved to dry storage. The hazards are postulated during the following three stages of the Used Fuel Dry Storage (UFDS):

- On-site transfer operations;
- Operations inside the Dry Storage Containers (DSCs) processing building; and
- Dry Fuel Storage (long-term storage).

In order to release Cs-137, which is the radionuclide of concern for the LRF in a PSA, the fuel would need to be melted. The fuel in the DSCs no longer generates enough heat to require active cooling. The DSCs are arranged in the dry storage buildings to ensure sufficient air flow to keep the containers cool, so the temperature would need to be raised by an external source. The hazard screening for the UFDS, therefore, makes use of this condition, i.e., if the hazard cannot raise the temperature of the dry fuel, then the hazard can be screened out.

4.3.1 Human-Induced External Hazards

Table 7 has been developed to align the listing of the human induced external hazards for the UFDS with those for the reactor in Section 4.1.2. All human-induced external hazards with a potential to impact UFDS are screened out, and do not require further analysis.

4.3.2 Natural External Hazards

Table 8 lists the natural external hazards and provides their screening analysis based on the approach adopted for the analysis of the natural hazards in Section 4.1.3. All natural external hazards are screened out, and do not require further analysis.

4.3.3 Combined External Hazards

Given that individual external hazards do not involve the high temperatures required for a large release of Cs-137 from the UFDS, the combinations of external hazards do not need to be assessed for the UFDS.

4.4 Internal Hazards Screening for Reactor Sources

4.4.1 Overview of Internal Hazards Screening Method

The internal hazards screening method is similar to the external hazards screening method and involves three main steps:

1. Identify all the internal hazards applicable to the site.
2. Determine consequences of hazards and accident scenarios. Screen-out events qualitatively, based on the consequence of events.
3. If the event could not be screened out based on qualitative screening criteria, then use quantitative screening criteria for the event screening.

The screening flow diagram of steps is the same as for the external events as shown in Figure 3. A preliminary list of the hazards is developed based on a literature review, as well as a walk down to review vulnerable areas within the powerhouse to identify any additional hazards. As many internal hazards have already been assessed in detail by the different PSA studies (e.g. internal fires, internal floods), the hazard screening only considered internal hazards not already assessed in PARA.

For each of the hazards identified, one or more parameters are selected that define the internal hazard and/or its potential impact, and for which discrete and quantifiable criteria can be developed. The qualitative criteria are the same as those for the external events as described in Section 4.1.1. If all qualitative criteria have been examined and the hazard has not been screened out by the seven deterministic criteria, the quantitative screening is required. The five quantitative screening criteria are presented in Table 2.

4.4.2 Internal Hazards Screening Results

The internal hazards identification included mechanical, chemical, electrical hazards, etc., initiated from the inside of the plant; an updated operating experience (OPEX) review was also conducted. The internal hazards identified are listed below:

- Mechanical Missile Impacts;
- Explosions within the Generating Station Main Buildings;
- Release of Oxidizing, Toxic, Radioactive or Corrosive Gases and Liquids from On-site Storage;
- Release of Stored Energy;
- Dropped or Impacting Loads;
- Transportation;
- Electromagnetic Interference; and
- Static Electricity.

The above internal hazards were assessed and all of them were screened out. As a result of the screening assessment, no new internal hazards were identified to be included in the PARA.

4.5 Internal Hazards Screening for Non-Reactor Sources - IFB

Screening assessments for the hazards for the IFB is based on the following considerations and insights:

- Loss of IFB Heat Sink (for example, resulting from random IFB cooling and support system failures, human errors, internal IFB fires, internal IFB flooding, reactor hazards that may impact IFB cooling system equipment operation); or
- Rapid/Slow Loss of IFB Inventory (for example, resulting from random IFB piping breaks, loss of inventory make-up, damage due to heavy load drops – for example, craning accidents). In principle the same hazard types are considered as for the existing reactor PSAs.

The above conditions can adversely impact the ability to prevent IFB fuel to uncover, as follows:

- Reduced IFB water level can result in increased radiation field in and near the IFB with the potential to inhibit corrective operator field actions such as equipment repair and IFB inventory make-up;
- Boiling of IFB water can result in harsh environment with the potential to cause IFB equipment failure and inhibit corrective operator filed actions; and
- IFB inventory leakage events (e.g., pipe break) can cause IFB equipment failure and inhibit corrective operator filed actions.

The internal hazards that were not screened out were assessed further as part of the non-reactor sources PSA (see Section 6.7). A list of screening of the internal hazards for IFB is presented in Table 9.

4.6 Internal Hazards Screening for Non-Reactor Sources - UFDS

The hazard screening assessment for internal hazard is similar to the assessment conducted for UFDS for external hazards (see Section 4.3).

All internal hazards with the potential to impact UFDS have been screened out based on the criterion stated in Section 4.3. As such these hazards do not require a PSA for the UFDS. A list of screening of the internal hazards for UFDS is presented in Table 10.

5.0 LEVEL 1 PSA METHODS

The goal of the PNGS-A Level 1 PSA is to identify IEs at the plant that can cause a transient at the plant that would challenge fuel cooling, identify what systems can be credited to mitigate the event, determine what the impact of the transient may be on the mitigating systems, and to determine and quantify the degree of fuel damage that would occur if the mitigating systems fail.

Typically, the PSA study for a station begins with the Level 1 At-Power internal events PSA. One of the Major tasks in Level 1 PSA is to develop models of station systems and their failure modes for a given transient. In other PSAs, e.g., internal fire, internal flood, seismic events, and high winds, much of the effort is associated with determining the impact of these events/hazards on the station systems. The methodology and requirements for the various Level 1 PSA studies are discussed in detail in the subsections.

The Level 1 At-Power PSA model was used in the development and quantification of the internal events outage, seismic events, internal fires, high winds, and internal flood PSAs.

5.1 Level 1 At-Power PSA for Internal Events

The Pickering NGS A Level 1 At-Power Internal Events PSA has been developed following the methodology for preparation of a Level-1 At-Power PSA as described in the OPG PNGS-A Internal Events At-Power PSA Guide.

The major activities of the PARA-L1P were:

(a) Identification of IEs based on a review of station-specific OPEX, generic industry OPEX and knowledge gained from previous risk assessment studies. The identification of IEs is discussed in Section 5.1.1.

(b) Development of a scheme to group sequences into a manageable number of consequence categories based on degree of fuel damage. A discussion of fuel damage categories in PARA is presented in Section 5.1.2.

(c) Development of Event Trees (ETs). ET diagrams establish the consequences that can occur following a particular initiating event, given success or failure of the systems credited with mitigating the initiating event. Development of the PARA ETs is discussed in Section 5.1.3.

(d) Development of system-level fault trees (FTs) needed to quantify the probability of failure of the station systems credited in the ETs. The development of the FTs is discussed in Section 5.1.4.

(e) Development of a component reliability database using, to the extent possible, information specific to PNGS-A. The reliability database is needed to support the FT analysis mentioned above. The sources of the data in the component reliability database are discussed in Section 5.1.4.

(f) Assessment of the effect of human error on accident progression and system performance using Human Reliability Analysis (HRA). The potential for human errors must be incorporated along with hardware failures in the ETs and system-level FTs. Human errors are referred to as “human interactions” in PARA. The HRA is discussed in Section 5.1.5.

(g) Integration of the ETs with the system-level FTs, and risk quantification. This step combines the accident sequences developed in the ETs with the system logic contained in the FTs to produce integrated FTs representing each of the fuel damage categories. The frequency of each fuel damage category is then determined by quantifying the corresponding integrated FTs. The integration process is described in Section 5.1.6.

Although the activities listed above are generally carried out in the indicated order, the PSA process is iterative in nature and entails re-assessing the results of an earlier task based on insights gained from a later task.

The major activities of the Level-1 At-Power methodology are summarized in the subsections below.

5.1.1 Initiating Events Identification and Quantification

An IE is a disturbance at the plant that challenges reactor operation or fuel integrity either by itself or in conjunction with other failures. Identifying the IEs and quantifying the frequency of IEs are the first steps in a Level 1 PSA.

In the PARA-L1P, the IEs primarily consider plant failures that could lead directly, or in combination with other failures, to damage to fuel in the reactor. The list of PARA IEs includes events leading to a hostile environment in the powerhouse, i.e., steam line breaks and feedwater line breaks.

Although PARA-L1P is an internal events PSA, it does include events associated with loss of off-site power (loss of the bulk electrical system) and events leading to failures in the service water intake. This is consistent with standard practice in PSA for nuclear power plants.

The objective of the initiating event selection task is to obtain as complete coverage as possible of credible IEs. To develop the initiating event list, past OPG PSAs were reviewed, as were the other published PSAs, and plant OPEX and station condition records. In addition, insight from the FT modelling, discussed in Section 5.1.4, identified other IEs. The complete set of IEs used in the PARA-L1P is listed in Table 12.

The IEs were quantified primarily using Bayes’ Theorem. In a Bayesian approach, an assessment is made of generic (prior) experience which is then updated with station-specific experience. This technique allows general experience and knowledge about a given event to be combined with actual OPEX gained at the station under study. It is especially useful for quantifying the frequency of IEs unlikely to be experienced within the lifetime of a single station. This is the industry standard method.

5.1.2 Fuel Damage Categorization Scheme

Each accident sequence, consisting of an initiating event and failures of credited station systems, may result in a different end state at the plant. The plant end states may vary in terms of the severity and the timing of fuel damage. Fuel damage categorization is carried out to simplify the subsequent evaluation of consequence and risk.

Each Fuel Damage Category (FDC) represents a collection of event sequences judged to result in a similar degree of potential fuel damage. The FDCs are used as end-states in the Level 1 ETs, as discussed in Section 5.1.3. In addition, groupings of the fuel damage categories are used to transition from the Level 1 PSA to the Level 2 PSA (see Section 6.1).

All ET end states, which result in severe core damage, are allocated to either FDC1 or FDC2. The categories are defined in Table 11. A Core Structural Integrity Maintained (CSIM) category is assigned to all sequences that do not end in FDC1 or FDC2. The FDCs are also used to calculate the frequency of severe core damage, used for comparison to the relevant OPG's safety goal. Severe core damage is defined to be the sum of the FDC1 and FDC2 frequencies. Frequencies for the CSIM end state are not derived in PARA-L1P.

5.1.3 Event Tree Analysis

The potential for an accidental release of fission products contained in the nuclear fuel constitutes the main risk from a nuclear power plant. In the Level 1 PSA, ETs are used to systematically review the possible ways that radioisotopes can be released from the fuel and to distinguish between varying levels of fuel damage.

Since a nuclear plant is a complex system, the search for accident sequences must be conducted in a systematic and structured manner. This analysis requires both a thorough understanding of the plant design, operation, maintenance and testing, and the ability to translate that understanding into a model of the plant that captures the logic of the sequences leading to fuel damage.

The accident sequences are constructed using inductive logic. The graphical representation of this inductive logic is called an ET. The start of this inductive method is the initiating event (IE). Following the identification of the IEs, the next step is to identify the systems required to mitigate the event and show how the accident could progress if failures of the mitigating systems were also to occur, until a previously defined end state is reached.

ET analysis requires the following to be predefined:

(a) The list of IEs to be considered.

(b) The definition of sequence end states.

(c) The identification of mitigating systems and corresponding ET branch point labels.

A generic ET for a large LOCA at a CANDU plant is presented in Figure 4. LOCA is typically a pipe break in the HTS. Following a large LOCA, three systems can mitigate fuel damage: the SDSs, the ECIS and the heat sink function of the moderator system. The potential plant state must be assessed if one or more of these mitigating systems fail. These three systems form the branch points in the ET.

The ET is read from the left, starting at the initiating event “IE-LOCA”. Moving to the right, the first systems credited with preventing fuel damage are the SDSs. Failure of both SDSA and SDSE is represented by the ET branch point “SD”. The convention used to interpret an ET is that success of the system is the top path and failure is the lower. If the SDSs fail, rapid loss of core structural integrity is expected. This sequence is assigned to the FDC1 end state. If reactor shutdown is successful, the decay heat must still be removed from the fuel to prevent fuel damage. Two systems are credited for this function: the ECIS and the moderator as a heat sink. If both systems fail, a slow loss of structural integrity is expected. This sequence is assigned to the FDC2 end state.

If either the ECIS or the moderator as a heat sink is successful, core structural integrity is maintained. These sequences are assigned to the CSIM end state.

In the PARA-L1P, an ET was prepared for each of the IEs listed in Table 12.

Once the Level 1 ETs have been created, the station systems that have been identified in the ET analysis require FT modelling to calculate the probability of failure of the mitigating function. This is achieved using FT analysis as described in the next section.

5.1.4 Fault Tree Analysis

A FT is a logic diagram that is used to model the possible causes of a particular fault and to estimate the probability that the fault occurs.

In PARA, FTs are used to quantify the probability of failure of the credited station systems that appear in the event tress discussed in Section 5.1.3. Figure 5 depicts the relationship between the ETs and the FTs. System FT analysis is used to calculate the probability of an ET branch point given a specific set of events that fail the system. Table 13 lists the systems modelled by FTs in the PARA-L1P.

Each FT is a logic diagram developed for a failure mode of interest, and is based on the understanding of system design and operation. At the top of the diagram the event itself is noted and termed the “Top Event”. The process of FT analysis is a deductive, systematic way of failure analysis whereby an undesired state of a system is specified (i.e., top event), and the system is analyzed in context of its environment and operation to find all credible ways in which the undesired state can occur. Thus, through this process, the contributors to the top event are identified.

The “CAFTA” software code is used for developing and quantifying the FTs [R-14].

For example, consider the moderator dump function of SDSA. For this system, the failure mode of interest is “moderator dump fails to shutdown the reactor following a SDSA trip”. Figure 6 shows a partially completed FT with this event at the top. Starting from this top event, the FT analyst poses the question “*How can this event occur?*” The answers to this question are inputs to this top event. For example, Figure 6 shows that the moderator dump function of SDSA can fail if the dump valves fail, the SDSA logic fails, or if a combination of SDSA logic failures and dump valve failures occur. For each of these contributors, the process of examining how they can occur is repeated until no further insights can be obtained about the behaviour of the system. Typically, the FT is developed either to predefined system boundaries, or to individual system components.

The basis for system capability and the failure criteria, e.g. the number of dump valves that must open in Figure 6, is based on analysis from a variety of sources. In the PARA-L1P, these sources included the PNGS-A Safety Report, the Operational Safety Requirements (OSRs), the Abnormal Incidents Manuals (AIMs), and other assessments and regulatory submissions.

In principle, the FT analysis technique is straightforward. An undesired event is postulated and then, deductively, its contributors are identified. However, this process requires a detailed understanding of the system design and function, and how it behaves under fault conditions.

Once the FT is constructed, it is linked with a database containing the information required to calculate the probability of each event in the FT. In PARA, failure rate, test data and maintenance data are assigned to the FT primary events from a central type-code table that is linked to the system reliability database. The use of the CAFTA compatible reliability database and a central type-code table ensures that the same type of component is assigned the same failure rate for the same failure mode in all system FTs.

The FTs include both equipment failures that occur prior to the IE and equipment failures that occur following the IE. Failures that occur following the IE are called mission failures. In the Level 1 PSAs for PNGS-A, the mission time in the reliability analysis was chosen to either reflect the expected mission of a particular system, e.g. approximately one hour for the BECS, or as 72 hours.

The nuclear industry has adopted a Bayesian approach for obtaining component failure rates. The Bayesian approach is based on both generic “prior knowledge” and plant-specific data in deriving failure rates. In the PARA-L1P, generic data was obtained from the U.S. Nuclear Regulatory Commission (NRC) [R-9], the T-Book and the Westinghouse Savannah River generic database [R-10]. The PNGS-A plant-specific data documented in the 2021 Annual Reliability Report [R-11] was used for the Bayesian update.

The reliability database also contains information on human errors modelled in the FTs and ETs. The analysis of human errors and their quantification is discussed in the next section of this report.

5.1.5 Human Reliability Analysis

Human errors can affect the performance of systems, and in some cases can be significant contributors to risk. Thus, the potential for human errors must be incorporated along with hardware failures in the system level FTs. Human interactions and human error probabilities must be systematically identified and assigned.

The overall objective is to include all human interactions that can potentially lead to a significant increase in the probability of component or system failure and that are not already reflected in the plant failure rate database.

In principle, every piece of equipment or system in the plant is susceptible to failure because of human error; however, human errors that contribute directly to the failure of individual components are included in the equipment reliability database (i.e., reflected in the components' failure rates) and need not be identified in FTs.

The human errors of interest to the FT analyst arise under five sets of circumstances:

(a) Where an otherwise operable component, subsystem or system can be disabled (e.g., prevented from performing its design function) prior to an initiating event;

(b) Where an equipment failure occurs but the operator does not respond to the failure prior to an initiating event;

(c) Where an operator action or closely related series of actions can cause more than one piece of equipment in parallel or redundant pathways to fail or become disabled simultaneously prior to an initiating event;

(d) Where the operator can fail to make the appropriate response to return the plant to a stable state following an initiating event (by not taking any action at all or by taking the required action but in an inappropriate way); and,

(e) Where the operator can plausibly interfere with correct responses by inhibiting or activating a system.

A human interaction in a FT identifies an opportunity for a human to make an error. Only those opportunities which arise in carrying out established plant operating practice are included, specifically errors that can be made in carrying out maintenance, testing, normal plant control, and post initiating event control activities. In most cases, these would be potential errors in carrying out formal procedures. Random, spurious, wilful, or vengeful actions are not included.

In order to systematically quantify the human interactions in PARA, OPG used a human interaction taxonomy. This taxonomy classified human interactions in PARA-L1P into three sections:

- Part 1 contains the simple interactions (which are, by definition, pre-initiating event);
- Parts 2 and 3 contain the complex interactions (which may be either pre- or post-initiating event).

Simple human interactions have the following characteristics:

(a) They are based on written or learned procedures (as opposed to cognitive or creative tasks);

(b) They involve directly manipulated components (e.g., a valve handwheel or a handswitch) or directly viewed MCR display devices; and,

(c) They occur prior to an IE.

The task of assigning preliminary (screening) human error probabilities for the simple human interactions uses a simple method requiring only the selection of an unmodified basic Human Error Probability (HEP) and predefined modifying factors. This method quantifies the human interaction based on the type of task, the location where the task is performed, whether the error can be detected in the MCR, and if any annunciations or inspections can detect the error. The simple human interactions are reviewed by the Human Reliability Assessment (HRA) Specialist. In some cases, the probability is requantified using the Technique for Human Error Rate Prediction (THERP) described in [R-13].

For the complex human interactions that occur prior to an IE, the same process may be followed to obtain a preliminary (screening) quantification. These human interactions are complex because they include system-level functions that involve more than just direct physical manipulation of a component, such as the setting of computer control program parameters or modes. The preliminary quantifications are then reviewed by the HRA Specialist on a case-by-case basis and if required are requantified using THERP methodology described in [R-13].

Post-initiating event complex human interactions usually occur during abnormal conditions and are, therefore, more difficult to identify, analyze, and quantify. Additionally, interactions involved in handling unit upsets are also unlike other interactions as they may take place in dynamic and uncertain situations. These actions are knowledge-based; they are based on fundamental principles of process and safety system operation and on an understanding of the interactions amongst these systems. For the post-initiating event complex human interactions, the preliminary (screening) human error probabilities are assigned based on three criteria: complexity of the task, the time available, and the quality of indication available in the MCR to indicate that action is required.

OPG also developed a simplified human reliability analysis process specific to EME deployment. This process is based on a methodology [R-12], which has been accepted by CNSC, for evaluating the failure probability associated with the retrieval, transportation and installation of the EME.

Human interactions that are identified as risk significant can be further refined by the HRA Specialist on a case-by-case basis using a methodology such as Technique for Human Error Rate Prediction (THERP).

5.1.6 Fault Tree Integration and Evaluation

The FT and associated failure rate data contain the information necessary to calculate the top event probability and identify the dominant contributors to failure for the individual system. Integration is the process of merging the system FTs with the ETs to create a logic model and calculate the frequency of occurrence of each of the end states for the fuel damage (i.e., Level 1) and release categories (i.e., Level 2). Combining the information in one model allows dependencies between systems to be identified and quantified correctly.

The information required to quantify the fuel damage categories is stored in the FTs and ETs. In order to combine the two, the ET logic is first converted into FT logic with a top event for each FDC. These FTs are referred to as the high level logic. The events in the high level logic are the IEs and the branch points from the ETs. The high level logic is then integrated with the mitigating system FTs; the top events in the mitigating system FTs are inserted where the mitigating system branch point labels exist in the high level logic model. Finally, the support systems are added to the integrated high level logic. Figure 7 illustrates this process.

In PARA-L1P, the evaluation of the FTs are conducted using the CAFTA software suit (version 6.0b) [R-14] and the FTREX solution engine (version 1.9) [R-15]. Those software programs were developed by Electric Power Research Institute (EPRI).

The solution of a FT is expressed as a listing of the combination of an initiating event, equipment failures, and human errors that leads to the occurrence of the FT top event. Each combination contains the minimum number of failures that have to occur to cause the top event. Such combinations are called minimal cutsets.

The solution of the FT calculated using CAFTA is truncated. That is, contributors below a certain frequency are not included in the solution. Truncation is necessary because of computational limits. The truncation limit selected should be low enough that all significant contributors are captured. The Level 1 At-Power Internal Events PSA guide recommends that the solution of the integrated FT for each FDC be truncated at either four orders of magnitude below the most likely minimal cutset in that FDC or at 1E-12 occ/yr, whichever is the highest. For FDC2 in PARA-L1P, the frequency of the top minimal cutset was 6.67E-08 occ/yr and a truncation of 6.7E-12 occ/yr was used.

Following the development of the baseline PSA results, an additional understanding of the station risk is obtained by supplementing the baseline solution with the following:

- Accident sequence quantification to provide sequence by sequence cutset ranking.
- Importance analysis to identify systems and components that are important to the FDC results.
- Parametric uncertainty analysis to determine the lower and upper limits of the two-sided 90% confidence interval for the frequency of each FDC; and
- Sensitivity analysis to evaluate the impact on the results of a number of potentially critical assumptions made in the ET analysis and FT analysis, as well as assumptions impacting the quantification of IEs, undeveloped events, and human error events.

Recall from Section 3.0 that risk has two components: the frequency of occurrence and the consequences. Section 5.1.1 to 5.1.6 describe the methods used to quantify the frequency of occurrence of the fuel damage categories. The Level 1 analysis is used as an input to the Level 2 analysis (see Section 6.0). The remaining subsections in Section 5.0 describe the differences in methodology for Level 1 assessment for the outage state, for internal fire, internal flood, seismic, and high wind IEs.

5.2 Outage Internal Events

The PARA-L1P considers internal events occurring at 100% full power operation. However, the PNGS-A has periods of planned outage to perform routine maintenance and testing that cannot be done during full power operation. The reactor power continues to decrease exponentially after reactor trip. Reactor power is typically around 0.6% full power on the first day of an outage.

The PARA-L1O considered internal events occurring while a reactor is in the GSS. At PNGS-A, a reactor is in the GSS for approximately 22% of the operating cycle.

The PARA-L1O was prepared following the methodology for preparation of a Level 1 Outage PSA as described in the OPG Pickering A Outage PSA Guide. The 2018 PARA-L1O bounding assessment is the starting point for the 2023 revision described in section 5.2.8.

The Outage PSA uses many of the same techniques as used in the At-Power PSA. The PSA process for outage uses IEs, ET analysis and FT analysis, like the At-Power PSA. However, different IEs can occur in the outage state, and the ET and FT analysis must reflect the plant configurations during the outage (e.g. HTS pressurized or depressurized). The plant configurations modelled as part of the outage PSA are typically described as Plant Operational States (POS).

Determining the possible plant configurations is a major part of the outage probabilistic safety assessment and is described in the next section.

5.2.1 Plant Operational State Identification and Analysis

The purpose of POS analysis is to manage the dynamic nature of an outage, specifically the varying system configurations, process parameters and system failure mechanisms. This is achieved by defining the various outage plant scenarios and grouping them into fewer, representative and bounding states for which the plant status, configurations and system failure criteria are considered sufficiently stable. In the definition of the POSs, only normally planned plant configurations are considered.

The first step in the POS analysis is to define Pre-Plant Operational States (Pre-POSs). Pre-POSs are defined as unique outage plant configurations during which all parameters of interest are stable for the duration of the state. Pre-POSs are the highest resolution of the outage states. The Pre-POSs are then grouped into POSs. A POS is a representative shutdown state wherein system configurations and parameters are considered bounding and sufficiently stable for the purposes of an Outage PSA. In the PARA-L1O, six pre-POSs were identified and have been grouped into three representative POSs. The three POSs are used in other aspects of the Outage PSA, including accident sequence analysis using ETs. Table 14 provides a summary of the final POSs used in the 2023 PARA-L1O model.

5.2.2 Initiating Event Identification and Quantification

The development of a Level 1 Outage PSA requires the identification, grouping and quantifying outage IEs, which can occur during the identified POSs. An outage initiating event is defined as a malfunction that can, either independently or in conjunction with other plant conditions or configurations, lead to fuel damage when the unit is in the GSS.

Identification and quantification of IEs for an Outage PSA is similar to the methodology as for a Level 1 At-Power Internal Events PSA (Section 5.1.1 of this report). However, it is important to note that there are a number of IEs unique to the Outage PSA, for example, ice plug failure or failure of the primary shutdown heat sink. Human initiated events (by incorrect operator action and/or maintenance activities) which occur during shutdown require explicit identification. Heavy load drops have been identified as potential initiators which have a low likelihood of occurrence, but which may have significant consequences (e.g., lifting a heat transport pump over the reactivity mechanism deck).

At-Power IEs may need to be adapted to account for shutdown state configurations. Lastly, given all OPG stations are multiunit, IEs from adjacent operating units (for example, steam line breaks) which may impact on the shutdown unit were reviewed. Table 15 lists the outage IEs used in the PARA-L1O and lists the POSs in which each IE can occur.

5.2.3 Event Tree Analysis and Fuel Damage Category (FDC) Analysis

The process for ET analysis for Outage PSA is consistent with the methodology used for the at power ETs described in section 5.1.3. However, a separate ET must be prepared for each unique IE/POS combination.

The PARA-L1O did not model loss of core structural integrity due to failure to shutdown, i.e. FDC1. FDC1 was not modelled due its very low frequency. The very low frequency results from the provision of two very reliable lines of defence to prevent the reactor from regaining criticality, i.e. the GSS and the SDS.

In a shutdown unit, the SDS is only required to prevent a reactor from regaining criticality. The SDS is not required to lower power following a total loss of heat sinks. If the reactor remains in the GSS, power is only a function of the decay heat level which itself is only a function of the time since shutdown.

5.2.4 Outage System Fault Tree Analysis

The development of an internal outage PSA requires the preparation of a FT for each branch point in the outage ETs. FT analysis is used to calculate the probability of ET branch points.

FT analysis for PARA-L1O follows the same steps and general methodology as for the at-power PSA (see Section 5.1.4). However, the outage FT models are significantly different from the at-power models to reflect the outage configurations of the system. For example, the automatic logic of the ECIS is usually blocked during an outage; therefore, only manual initiation of ECIS can be credited in the ECIS FT for a shutdown unit.

Table 13 lists the systems modelled by FTs in PARA-L1O.

5.2.5 Reliability Data Analysis

The objective of reliability data analysis is to derive the reliability data assigned to the primary events modelled in the PARA-L1O system FTs. Primary events include basic events (e.g., component hardware failures), conditioning events (i.e., events used to specify a condition or restriction that applies to the FT logic), developed events (i.e., specific fault events related to external interfaces which are typically developed in separate FT models), and undeveloped events (i.e., specific fault events not amenable to further development and so quantified using specialized methods).

Like in the at-power PSA, a Bayesian approach is used for obtaining component failure rates. Conditioning events, developed events, and undeveloped events, for which component failure rates are not applicable, are also quantified using one of the following methods:

- Operational events are quantified from observation of OPEX;
- Analytical events have a probability of occurrence that is determined from the results of analytical models outside of the FT, engineering judgement, or both.

5.2.6 Human Reliability Analysis

The possibility of component or system failure due to human error is recognized by the inclusion of human interactions in the FTs and ETs. The scope of the Human Reliability Analysis (HRA) includes inadvertent errors by plant operators or maintainers that may contribute to the failure of systems or components but excludes consideration of arbitrary or wilful actions. Ultimately, the human error probabilities are combined with equipment failures in the system FT to provide the overall probability of the top event. In the ETs, the human error probabilities are combined with system and/or equipment failures in the ET to provide accident sequence frequencies.

Human reliability analysis for an Outage PSA follows the same steps and general methodology as for the at-power PSA model (see Section 5.1.5). The human interactions during outage states require the consideration of the many testing and maintenance activities, procedures, and manual initiation of certain mitigating systems. The HRA specialist considers the outage POSs and system configurations to better understand required operator actions, recall actions, and possible testing and maintenance activities during a given POS. FT Integration and Evaluation Integration is the process of merging the system FTs with the ETs to create a logic model for each FDC. The goal of integration is to use the logic model to calculate the frequency of occurrence of each FDC. Combining the information in one model allows dependencies between systems to be identified and quantified correctly.

5.2.7 Model Integration, Quantification, and Additional Analyses

Once the ETs and FTs are developed, they are linked to determine the frequencies with which various fuel damage consequence categories can occur. Categories, here, are groupings of sequences with similar consequences. As the linked models can be of large size, computer aided methods are used to carry out the computations. The results are expressed in terms of the expected number of occurrences of the consequence category per unit time (i.e., frequency). Only those failure combinations that have frequencies greater than a certain cut-off value are listed. The frequency of the consequence category is obtained by summing the frequency of each sequence belonging to that category.

For each consequence category, the magnitude of the associated consequence needs to be calculated. The product of frequency and consequence is calculated for each category and summed to obtain an overall estimate of risk. These are used in absolute terms to assess the overall safety design adequacy, and in relative terms to identify the dominant risk contributors. The acceptability of the PNGS-A risk estimates is judged based on comparison with the safety goals established by OPG.

FT integration and evaluation for the outage PSA follows the same steps and general methodology as for the at-power PSA model (see Section 5.1.6). However, it is important to note that:

1. Only the frequency of FDC2-SD was estimated in the PARA-L1O.
2. The integration was performed for FDC2-SD separately for each POS.
3. The estimated SCDF is time averaged. That is, the SCDF for each POS is weighted according to the fraction of a year that a unit is expected to be in that POS.

5.2.8 Level 1 Outage Internal Events PSA Bounding Assessment

The 2023 PARA-L1O update is a bounding assessment, undertaken in accordance with the principle in REGDOC-2.4.2 that the level of detail in a PSA should be consistent with the level of risk. The OPG Outage PSA Guide forms the general basis for conducting the outage PSA update. Given the relatively low risk from outage units compared to other contributors to station risk – this bounding assessment meets a graded approach for the 2023 PARA-L1O update.

The overall objective of 2023 PARA-L1O analysis was to provide an updated SCDF estimate reflecting the current Pickering A design and operation to the extent practical for a limited scope bounding assessment.

5.3 At-Power Internal Fire

The purpose of a fire PSA is to establish whether the design and operation of the plant poses an acceptable level of risk to the public and to identify the major sources of risk due to fires. The 2023 PARA-Fire was prepared following the methodology described in the OPG's Internal Fire PSA Guide for PNGS-A. The methodology described in the PNGS-A Fire PSA Guide has been developed based on the United States Nuclear Regulatory Commission (U.S. NRC) Fire PSA methodology, NUREG/CR-6850 [R-16]. The major activities of the Fire PSA methodology and its application in the development of the PARA-Fire assessment are summarized in the subsections below.

An internal fire PSA model is built from the internal events at-power PSA model. The scope of the PARA-Fire model is limited to internal fires initiated with the analysis unit at power with the potential to cause severe core damage. Internal fires considered are those resulting from fixed ignition sources within fixed equipment (e.g., electrical panels, pumps, etc.) as well as transient ignition events resulting from human activities in the plant (e.g., combustible material storage, hot work, etc.).

The PNGS-A Fire PSA Guide prescribes a phased evaluation of internal fire risks. In each phase, appropriate technical bases and methods are applied; the difference is in the degree to which simplifying assumptions are made as the significant contributors to risk are addressed.

The PARA-Fire model considers sequences that result in Severe Core Damage (SCD). Severe core damage is defined as the sum of the FDC1 and FDC2 frequencies. The fire PSA mainly focuses on sequences that result in severe core damage due to failure to remove decay heat, that is, the Fuel Damage Category 2 (FDC2). Sequences involving failure to shutdown the reactor, referred to as the Fuel Damage Category 1 (FDC1), represent a very small portion of the sequences leading to SCD due to the low frequency in the internal events model. The fail-safe design of the two SDSs (e.g., SDSA and SDSE) and the physical separation of SDSA and SDSE make it unlikely that a fire could impact both systems. This limited the number of fire scenarios with the potential to impact more than one channel of one SDS and reduced the probability of a fire-induced failure to trip.

The Fire PSA methodology is broken into 18 tasks:

- Task 1 – Plant Boundary Definition and Partitioning
- Task 2 – Fire PSA Component Selection
- Task 3 – Fire PSA Cable Selection
- Task 4 – Qualitative Screening
- Task 5 – Fire-Induced Risk Model
- Task 6 – Fire Ignition Frequencies
- Task 7 – Quantitative Screening
- Task 8 – Scoping Fire Modelling
- Task 9 – Detailed Circuit Failure Analysis
- Task 10 – Circuit Failure Mode Likelihood Analysis
- Task 11 – Detailed Fire Modelling
- Task 12 – Post-Fire Human Reliability Analysis
- Task 13 – Seismic-Fire Interactions Assessment (outside the scope of the PARA-Fire; a seismically-induced internal fire and internal flood risk evaluation is undertaken as part of the PNGS-A Seismic PSA)
- Task 14 – Fire PSA Level 1 Quantification
- Task 15 – Uncertainty and Sensitivity Analysis
- Task 16 – Fire PSA Documentation
- Task 17 – Fire PSA Level 2 Quantification
- Task 18 – Alternate Unit Assessment

The integration of these tasks is shown in Figure 8. The PARA-Fire was prepared following an iterative approach. Several of the tasks listed above involved calculation of SCDF due to fires in various plant locations. With each subsequent iteration, the methods used to estimate risk for the various scenarios were refined. This iterative approach is used to identify high risk areas and to focus the detailed fire analysis on these areas. A brief summary of the methodology used for PARA-Fire is provided in the following sections.

5.3.1 Plant Boundary Definition and Partitioning (Task 1)

The first step in an Internal Fire PSA is to define the physical boundary of the analysis, and to divide the area within that boundary into physical analysis units (PAUs, also referred to as fire zones). This requires defining the overall analysis boundary to ensure that those plant locations where a postulated fire could impact the PSA are included in the analysis. Once the overall analysis boundary is defined, the buildings that are within the boundary are examined for potential sub-division into PAUs.

The PAUs used in the PARA-Fire were based on those identified in the PNGS-A Fire Hazard Assessment (FHA). This approach allowed the PARA-Fire to rely on the existing programmatic controls and design requirements for maintaining the integrity of the associated compartment boundaries.

5.3.2 Fire PSA Component Selection (Task 2) and Cable Selection (Task 3)

In these tasks, the components and associated cables necessary for safe shutdown and long-term decay heat removal following a fire is identified. A fire can affect the equipment credited for safe shutdown by either being in the same area as the credited equipment or by being in the same area as the cables related to the credited equipment.

In the PARA-Fire, components and cables were divided into two groups:

1. Group B is the set of systems and components credited in the Fire Safe Shutdown Analysis (FSSA) for safe shutdown and decay heat removal following a fire. For these systems cable routing data was available from the FSSA.
2. Group A is the set of systems and components that, although not credited in the FSSA, may be capable of mitigating events initiated by a fire scenario. These systems were only credited for fires which could be shown not to affect cables.

   The additional mitigating systems and corresponding functions selected for credit are:

   i) Front-Line Systems:

      - HTS Liquid Relief Valve (LRV) function to reclose after opening on overpressure and remain closed for the mission; and

      - Calandria Spray System (Moderator).

   ii) Support Systems Required for Operation of the Selected Front-Line Systems:

- Power supply provided by Class III SGs, Class II distribution and Class I batteries;
- LPSW;
- Firewater; and,
- HPIA[5].

iii) EME (Phase 1):

- Makeup from the EME to the boilers and calandria, including the injection path; and,
- Makeup from the Firewater System to the boilers and calandria, including the injection path.

iv) Interim Heat Sinks to Support EME Deployment

- BECS;
- Gravity-fed boiler makeup from the Deaerator Storage Tank; and,
- Gravity-fed makeup to the HTS from the Emergency Coolant Injection (ECI) Storage Tank.

In addition to the explicit selection of mitigating systems, a Multiple Spurious Operation (MSO) assessment has been performed as part of the 2023 PNGS-A Fire PSA. The MSO assessment started with a list of generic CANDU MSOs and created a PNGS-A specific list of MSO events. Then, the MSO assessment continued with dispositioning of the MSO events such that each scenario was either dispositioned, or considered for consequence assessment. Further, a bounding consequence assessment was performed such that no additional circuit analysis and cable tracing was required as part of the 2023 PARA-Fire update. More details on this task are discussed in Section 5.3.8. The screened in MSO scenarios were incorporated in the PARA-Fire model.

5.3.3 Qualitative Screening (Task 4)

This task involves the identification and screening of PAUs that can be shown to have little or no risk significance without the need for quantitative analysis. The PAUs can be screened out if they do not contain PSA credited components or cables, and cannot propagate fires into PAUs containing such components and cables, and if they cannot lead to a plant trip due to either plant procedures, an automatic trip signal, or plant operating policies and principles (OP&P) requirements. This task was not performed in the PARA-Fire; all PAUs were conservatively retained for later tasks.

---

[5] Modeling of the HPIA System is treated differently than the other systems which rely on electrical power supplies and control circuits.

5.3.4 Fire-Induced Risk Model (Task 5)

This task involves the development of a logic model that reflects plant response following a fire. This includes modelling the plant response to fire-induced events and modifying the internal events PSA model to reflect postulated equipment failures.

The PARA-L1P model was modified and manipulated to produce a fire-induced risk model incorporating the modified human error event probabilities as described in Section 5.3.10, and incorporating model logic changes specific to the fire analysis such as the addition of fire specific failure modes (e.g., hot shorts). It also included the identification of events in the fire model to be set to “failed” to represent the unavailability of the equipment should they be failed in the fire scenarios. This model was used to calculate the CCDP for each postulated fire initiating event in the Fire PSA quantification (Task 14).

5.3.5 Fire Ignition Frequencies (Task 6)

To calculate the risk due to an internal fire, fire ignition frequencies (FIFs) for each PAU identified in Task 1 must be assessed.

Unit 4 is used as the reference unit for PNGS-A with consideration of applicable shared systems and areas that could impact Unit 4 operation. The calculation of FIFs for Unit 4 required calculation of FIFs for all of the PAUs that are within the analysis boundary. This was accomplished, as per guidance provided in PNGS-A Fire PSA Guide, NUREG/CR 6850 [R-16], its supplement [R-17], and NUREG-2169 [R-18]. Key steps in the development of fire ignition frequencies include:

- Plant walkdowns to identify ignition sources;
- Transient fire ignition frequency development based on engineering judgment from site personnel who are familiar with the daily activities of the plant; and,
- Bayesian updating of generic ignition frequencies with the most current site-specific fire experience data.

The fixed ignition sources fire frequency, the transient ignition sources fire frequency and the total fire ignition frequency were calculated for each PAU identified in Task 1.

5.3.6 Quantitative Screening (Task 7)

In the PARA-Fire, this task was performed in conjunction with Task 8.

In this task, a bounding assessment is made of the risk impact of fires in each PAU. The bounding assessment assumes that the FIF for each PAU is the sum of the FIFs for all equipment inside the PAU and that all credited equipment in the PAU fails. If the SCDF based on the bounding assessment is very low, then no further analysis is performed for the PAU and the conservatively estimated SCDF is carried forward for use in Level 1 quantification (Task 14).

Quantitative screening was not explicitly performed as a separate task. This task was implicitly performed during the initial scoping fire modelling (Task 8). Some bounding scenarios are still retained in this PARA-Fire update.

5.3.7 Scoping Fire Modeling (Task 8)

This task is intended to provide a conservative and simplified means to develop an initial refinement to the bounding treatment in Task 7. It involves the use of generic fire models for various fire ignition sources such that simple rules can be used to define and screen fire ignition sources (and therefore fire scenarios) in an unscreened PAU. The generic fire models can be also used to develop simplified treatments for specific fire ignition sources and their impact on nearby targets (cables) and thereby eliminate the need for numerous explicit detailed fire modeling analysis. The information from these models was combined with walkdown information using raceway identifiers to characterize the extent of fire impact to plant systems.

This task has two main objectives:

- To screen out those FISs that do not pose a threat to the targets within a specific fire compartment; and
- To assign severity factors to unscreened Fixed Ignition Sources (FISs).

To meet these objectives, Task 8 develops fire scenarios for the unscreened PAUs from Task 7 quantitative screening and assigned CCDP cases to each scenario. This task was not performed in the PARA-Fire; instead, detailed fire scenarios were developed in Task 14 – Fire Level 1 PSA Quantification, as needed.

5.3.8 Detailed Circuit Failure (Task 9) and Failure Mode Likelihood Analysis (Task 10)

The development of a fire PSA requires detailed circuit failure analysis and circuit failure mode and likelihood analysis. The purpose this task is to conduct a more detailed analysis of circuit operation and functionality to determine equipment responses to specific cable failure modes. This added level of resolution is then used to further refine the original cable selection by screening out cables that cannot prevent a component from completing its credited function. Tasks 9 and 10 only need be applied to cables associated with the components that were not previously assessed in the FSSA.

No additional analyses on Tasks 9 and 10 were required for the 2023 PARA-Fire update; the circuit analysis and cable selection results from the previous PARA-Fire were used as discussed below:

- Cables required to support the components credited and identified in the FSSA for which the circuit analysis was performed as part of the FSSA.
- Cables required to support additional non-FSSA components selected for credit in the previous PARA-Fire for which the circuit analysis was performed as part of the previous PARA-Fire.

5.3.9 Detailed Fire Modeling (Task 11)

Detailed fire modeling was used to perform fire ignition source (scenario) specific fire modeling to address risk-significant scenarios in cases where the scoping fire modeling (Task 8) described in Section 5.3.7 produced overly conservative results. Detailed fire modeling was performed only in those instances where such analyses produce substantially improved results as compared to those obtained from Task 8.

In the PARA-Fire, three fire-related scenarios were developed in greater detail:

1. Hot Gas Layer (HGL) Formation.

   The HGL analysis evaluated the potential for temperature related failures of equipment and cables due to the formation of an HGL. HGL formation increases the zone of influence of an ignition source fire, potentially increasing it to the whole of the PAU.

2. Multi-Compartment Analysis (MCA).

   The main objective of MCA is to evaluate the potential for a HGL formed in one PAU affecting a second PAU following the failure of a barrier. This can further increase the zone of influence of an ignition source.

   Non-HGL interactions between two PAUs were separately analysed in Task 8.

3. MCR Abandonment.

   A fire in the MCR may force the operators to abandon the MCR. This degrades the capability of operations staff to control the configuration of the plant, including the deployment of emergency heat sinks.

   In the PARA-Fire, MCR abandonment times were assessed for electrical fires and transient combustibles within the MCR envelope.

In the PARA-Fire, the following scenarios were also developed and detailed fire modeling was performed to improve the characterization or the fire consequences:

- Catastrophic turbine generator oil (TGO) fire scenario;
- Catastrophic TG hydrogen fire scenario;
- Risk significant pump oil fire scenarios;
- Fire scenarios that only damage standby equipment;
- Self-ignited cable fire scenarios;
- Electrical panel fire scenarios; and
- HGL fire scenarios.

In the 2023 PARA-Fire, the parameters that were introduced for the detailed fire modelling refinements were reviewed and the results from the fire modelling were incorporated into the fire scenario consequence assessment performed as part of CCDP case development and risk quantification in Task 14.

5.3.10 Post-Fire Human Reliability Analysis (Task 12)

The purpose of this task is to evaluate the impact of fire scenarios upon the human actions addressed in fire induced risk model (Task 5) and to identify and quantify new actions to be performed as part of the plant fire mitigation plans and procedures. The probability of failure of each of these actions is estimated and used as input to the Level 1 Fire PSA quantification (Task 14).

A review of PARA-L1P model was performed to identify the post-initiator operator actions modelled as human failure events along with their associated Human Error Probabilities (HEPs); pre-initiator operator actions and operator actions associated with non-fire induced events were excluded from consideration.

For each fire-related basic event that represents a post-initiator operator action modelled as human failure, HEP multipliers were developed for fire PSA adjustments. The multipliers have been developed considering the following factors:

- Location (either inside the MCR actions or outside the MCR actions);
- Time available (based on PARA-L1P HRA documentation);
- Complexity of the action;
- Availability of indications and controls necessary to diagnose and execute the action; and
- Availability of the path to the equipment for field actions.

Based on the factors above, the baseline HRA value from the PARA-L1P may be retained, the HRA value may be multiplied by a factor in the range of 2 to 30, or no credit for the operator action may be taken (failure of operator action assigned a probability of 1).

In addition, a fire-specific evaluation of the human action for deployment of the EME was carried out to calculate the HEP for EME deployment following a fire event.

5.3.11 Fire Level 1 PSA Quantification (Task 14)

The development of a fire PSA requires the integration of the fire risk model with the damage consequences calculated for each scenario. The development of the fire risk quantification is typically an iterative process. As various analysis refinement strategies are developed, they are incorporated into the fire risk model.

The scope of work for fire quantification involves the use of the fire PSA model and the performance of the model quantifications for the purposes of obtaining SCDF estimates for each modeled fire initiating event.

The scoping fire modeling (Section 5.3.7) provided a conservative and simplified means to develop an initial risk estimate. Additional model quantifications to calculate the SCDF are performed iteratively as additional analysis refinements are incorporated. This includes information gathered during walkdowns conducted for scoping modelling (Section 5.3.7) and additional analysis of other PNGS-A design inputs (e.g., equipment and cable tray layout drawings) to refine treatment of PAUs that had high estimated SCDFs in the initial bounding assessment in the quantitative screening (Section 5.3.6). This refinement typically divided risk significant PAUs into multiple fire IEs (scenarios) to represent individual fire ignition sources. In some cases, multiple fire ignition sources in a PAU were grouped and treated as a single fire initiating event so long as such grouping did not result in overly conservative risk estimates.

The SCDF contribution from the PAUs that were screened out as part of quantitative screening analysis was included in the final fire-induced SCDF estimate.

5.3.12 Uncertainty and Sensitivity Analysis (Task 15)

The development of a risk assessment inherently results in the introduction of uncertainty in the analysis results. In general, the sources of uncertainty for each of the fire PSA development tasks are discussed in the industry reference document NUREG/CR-6850 [R-16]. In the PARA-Fire, the uncertainty has been mitigated to a large degree through a careful selection of input parameters. Where refinements have been made to the fire scenarios to reduce conservatism, it has been performed using industry standard approaches. Consequently, the treatment of uncertainty and sensitivity in Task 15 was focused on the parameters with a significant importance to the SCDF and/or LRF results.

In the 2023 PARA-Fire, parametric uncertainty analysis, sensitivity analysis, importance analysis and a cliff-edge effect analysis were performed. The parametric uncertainty analysis and importance analysis for human actions, components, and systems are consistent with the requirements of PARA-L1P.

5.3.13 Level 2 Analysis (Task 17)

This task is built on the results of the Level 1 quantification to consider the Level 2 impacts of fire scenarios in terms of LRF. If scenarios were identified in the Level 1 that would affect multiple units such as fires impacting the MCR or fire impacting common systems and/or common cable trays, then the multi-unit impact on Level 2 functions was quantified. More details on this task are discussed in Section 6.3.

5.3.14 Alternate Unit Analysis (Task 18)

The scope of work resulted in specific numerical results for the Unit 4 PAUs and other site PAUs that are common to all four units. Currently PNGS-A station consists of two operating units (Units 1 and 4), two permanently safe storage units (Units 2 and 3) and common areas that support both operational units (e.g., the MCR complex located between Units 2 and 3).

Quantification of separate SCDFs and release frequencies for Unit 1 was not specifically included. Because fire risk characterization is needed for the entire plant site, the anticipated symmetry / consistency in the design and construction of the two operating units is relied upon to support a qualitative approach to evaluating the applicability of the Unit 4 results to Unit 1.

The expectation is that Unit 1 would be a generally similar, mirror image of Unit 4. To confirm the plant symmetry between Units 1 and 4, a side-by-side comparison of the Unit 1 PAUs to the analyzed Unit 4 PAUs was performed. This was extended to also include a comparison of analogous PAUs in Units 2 and 3 for the purposes of determining whether there may be an asymmetrical impact from these PAUs on Units 1 and 4.

A side-by-side comparison of the Unit 1, 2 and 3 PAUs to the analyzed Unit 2 PAUs was created using fire zone information from the Fire Hazard Analysis (FHA) and the PNGS-A Fire Safe Shutdown Analysis (FSSA). In addition, a walkdown was conducted in support of Task 18 as part of the 2023 PARA-Fire update. The purpose of the walkdown was to identify the differences between the units. The comparison of Units 1 and 4 from the fire risk perspective along with the walkdown observations confirmed that the units are generally symmetrical and consistent in their construction. The differences in equipment placement and cable routing are relatively minor and are not expected to have a significant impact upon risk. Therefore, the Unit 4 fire risk analysis can be used as a surrogate for an evaluation of the fire risk for Unit 1.

5.4 At-Power Internal Flood

The PNGS-A Internal Flood PSA Guide describes the methodology used to quantify the risk due to internal flooding. Similar to the fire PSA, the guide prescribes using a two phased approach. If the results of the first phase are satisfactory, then only the first phase is implemented. For PNGS-A, a Phase 2 Flood PSA was not required.

The 2023 PARA-Flood assessment was developed following the methodology for preparation of an Internal Flood PSA as described in the PNGS-A Flood PSA Guide. The 2018 analysis was used as the starting point for the 2023 PARA-Flood update. The updated flood risk model was built on the 2023 PARA-L1P model.

Like the fire PSA described in Section 5.3, the impacts of internal flooding events are related to the physical location of equipment in the plant. The station must be divided into areas, and the potential initiators in each area assessed, and the impacts of the initiators determined. The Level 1 Internal Events PSA is used to determine which components need to be evaluated for flooding impacts, and is also used as the basis for the quantification of the internal flooding severe core damage frequency.

The PARA-Flood analysis is focused on two primary objectives: areas of the plant that contain equipment from both Group A and Group B systems (referred to as “pinch points”), or areas which might completely disable all of Group A or Group B, as these areas represent the highest potential for degradation of the plant mitigation capability; and conservative estimation of risks associated with the other areas of the plant. The impact of flooding events on Phase 1 EME deployment is also considered.

The construction of the Internal Flood PSA requires the following steps:

- Identification of flood areas and affected systems structures and components (Task 1);
- Identification of flood sources (Task 2);
- Plant walkdowns (Task 3);
- Qualitative screening (Task 4);
- Flood scenario characterization (Task 5);
- Internal flooding initiating event frequency estimation (Task 6);
- Flood consequence analysis (Task 7);
- Evaluation of flood mitigation strategies (Task 8);
- PSA modelling of flood scenarios (Task 9); and
- Level 1 flood PSA quantification (Task 10).

These tasks are briefly described in Sections 5.4.1 to 5.4.10 of this report. The relationship between these tasks is shown in Figure 9.

The assessment of the seismic-flood interactions is outside the scope of the PARA-Flood and is undertaken as part of the PNGS-A Seismic PSA.

The Internal Flood PSA focuses on sequences that lead to severe core damage (FDC1 and FDC2) caused by an internal flood. Failure to shutdown sequences (FDC1) are not quantified as the potential for flooding events to adversely affect the fail-safe SDSs is minimal. Including FDC1 sequences in IFPSA does not provide any additional insight in this assessment with the minimal impact of flooding.

5.4.1 Identification of Flood Areas and Affected SSCs (Task 1)

The first step of the PARA-Flood was to partition the plant into the flood areas that form the basis of the analysis. Flood areas are defined based on physical barriers, mitigation features, and propagation pathways. The flood areas were initially based on the partitions in the FSSA.

Once the flood areas were defined, the SSCs in each flood area modelled by the internal event PSA were identified. In the PARA-Flood, the SSCs that can mitigate the consequences of a flood were classified as being either:

- Group B – these are the systems that support flood mitigation in PNGS-A but that are supplied from PNGS-B. In the PARA-Flood, these systems were the EBWS, the Inter-Station Transfer Bus (ISTB) and the HHPECI; or
- Group A – all other systems credited in the forced shutdown ET of the PARA-L1P.

The potential for floods originating in PNGS-A and affecting Group B mitigating equipment located in PNGS-B was also addressed. The 2023 PARA-Flood considered partial failures in Group A and Group B systems in the postulated flooding scenarios.

For the PARA-Flood model, once the flood areas were identified, they were screened using qualitative screening criteria as described in the following section. After the initial screening, those unscreened areas were reviewed for the impact on equipment credited in the PSA, and the possible flood sources in the area.

5.4.2 Identification of Flood Sources (Task 2)

This task identified the potential flood sources in the plant and the associated flooding mechanisms and included the following sub-tasks:

- Identifying or confirming the flood sources in each flood area;
- Determining or confirming the flooding mechanisms associated with each flood sources;
- Determining or confirming the characteristics of each flooding mechanism;
- Identifying drains and sumps in each flood area and determining the capacity of the mitigating functions; and
- Identifying flood propagation paths.

In addition, the potential for floods from Units 2 and 3, currently in safe storage, and the potential for floods originating in PNGS-B propagating to PNGS-A were considered in this task.

5.4.3 Plant Walkdowns (Task 3)

This task supports the other PARA-Flood tasks by identifying or confirming plant data by observing it at the plant during walkdowns. The output from this task includes all the necessary information for flood scenario development, flood consequence assessment, flood mitigation, and flood initiating event characterization, and flood scenario quantification. To support the 2023 update of the PARA-Flood, a walkdown was performed. The scope of the walkdown was established to support Tasks 1, 5 and 7.

5.4.4 Internal Flood Qualitative Screening (Task 4)

This task involved a qualitative screening considering the sources of flooding, the flood propagation pathways and the consequences of the flood. The objective is to qualitatively screen out many low risk internal flood scenarios. The following rules were used when screening:

- Screening criteria for flood areas:

- Any flood areas with no credible flood source or no sources that could propagate from one area to another; and
- The flood area does not cause an initiating event or the need for immediate plant shutdown.
- Any area that the postulated flooding of the area neither causes an initiating event nor a need for an immediate plant shutdown with the following conditions applied:
  - a) The area contains flooding mitigation systems capable of preventing unacceptable flood levels, and the nature of the flood does not cause equipment failure;
  - b) A technical basis is provided to justify that the mitigation systems credited for screening out flood areas have sufficient capability;
  - c) The nature of flood does not cause the failure of the mitigating systems or any other equipment required to prevent core damage for flood initiated sequences; and
  - d) There are no propagation pathways to other flood areas.

- Screening criteria for flood sources:
  - The flood source is insufficient to cause failure of SSCs;
  - The area flooding mitigation systems are capable of preventing unacceptable flood levels and the nature of the flood does not cause equipment failure through other failure mechanisms;
  - The flood only affects the system that is the flood source and the Internal Events PSA addresses this type of failure, and need not be treated as a separate internal flood-initiating event; and
  - Mitigating human actions can be shown to be effective if all of the following can be shown:
    - i) Flood indication is available in the control room;
    - ii) The flood source in the area can be isolated; and
    - iii) The mitigation action can be performed with high reliability.

5.4.5 Flood Scenario Characterization (Task 5)

This task identified and characterized the potential flood scenarios to be included in the analysis. The consequences for each flood-induced initiating event were characterized by considering the following factors:

- The specific flood area, flood source, flood source failure mode and flood magnitude.
- The type of flood failure mechanism, e.g. spray, jet or major flood.
- The consequences of the flood, including:
    - Flood propagation;
    - SSCs damaged by the flood; and
    - The initiating event for the purpose of formulating event sequences leading to severe core damage. The initiating event could be the direct consequence of the flood or an immediate plant shutdown, which could trigger an adverse event sequence.
- Operator and mitigation system responses to terminate the flood, limit damage to SSCs and to recover the plant from the effects of the flood event;
- The means to be used to define the interface with the PARA-L1P model for calculating the probability that the flood leads to severe core damage.

In addition to flood characterization, the flood scenario was described to include the potential propagation paths of the flood, to consider any possible operator actions to mitigate the flood propagation sequence, and to account for the impact of flood events on equipment. This was conducted as the consequence analysis in Task 7 and discussed in section 5.4.7. Additional details on the Human Interactions (HIs) were provided in the flood mitigation strategies analysis, which is described in section 5.4.8 below.

5.4.6 Initiating Event Frequency Estimation (Task 6)

This task identified the flood-induced IEs and estimated their frequencies.

In the 2023 PARA-Flood, the latest available EPRI pipe failure rates [R-19] were utilized to update the frequencies of the flood IEs. The frequencies of internal flood IEs were estimated by multiplying pipe rupture rates, expressed in units of per foot of piping per year, by the length of the piping within a specific flood area. Separate frequencies were estimated based on the categorization of a flood as spray, flood or major flood mode.

Based on the maximum break discharge, if a particular scenario was identified as a major flood mode, then the possibility that the same pipe failure might result in a smaller break discharge (e.g., flood) was also considered. Similarly, if more than one flooding mode was applicable, the failure rate for each applicable mode was summed to calculate the flood initiating event frequency.

5.4.7 Consequence Analysis (Task 7)

This task characterized the consequences for each flood-induced IE by considering the type of flood source, spill rate, flood location, time to reaching a critical flood volume, and the impact on the SSCs modeled in the PSA.

5.4.8 Flood Mitigation Strategies (Task 8)

This task identified and evaluated the strategies that can be employed by plant operators to mitigate the consequences of a flood. These actions can include terminating the source of the flood by isolating the break, stopping the pumps that supply the flood source, or opening doors to divert water away from sensitive equipment.

The evaluation of human failure events in the PARA-Flood was similar to that used in the Internal Events PSA; however, flood scenario-specific impacts on Performance Shaping Factors (PSFs) were considered for both control room and ex-control room actions based on the following items:

- Additional workload and stress above that for similar sequences not caused by internal floods;

- Availability of indications;

- Effect of flood on mitigation, required response, timing, and recovery activities (e.g., accessibility restrictions, possibility of physical harm); and

- Flooding-specific job aids and training (e.g., procedures, training exercises).

Human reliability analysis (HRA) was performed for actions taken by MCR operators as well as by field operators to terminate the flood and place the plant in a safe stable configuration. Ultimately, consistent with the proper HRA techniques, the plant procedures and operator training programs specific to flood response were used to determine how well operations personnel respond to internal flood conditions.

5.4.9 PSA Modelling of Flood Scenarios (Task 9)

This step included the finalization of flood scenario development and completing internal flood accident sequence models based on modifying the Internal Events PSA model. ET logic for the flooding IEs was developed using the 2023 PARA-L1P Forced Shutdown (FSD) ET logic. These ETs modelled the possible mitigating actions described in Section 5.4.8. Based on success or failure of the mitigating actions, equipment availability was determined.

In the PARA-Flood, the flood induced risk model was limited to scenarios that may result in severe core damage due to the failure of all heat sinks. Sequences involving failure to shutdown were not modelled as the potential for flooding events to adversely affect the fail safe feature of a SDS was judged to be minimal.

5.4.10 Level 1 Flood PSA Quantification (Task 10)

This task involved the construction of an integrated PSA model to evaluate the risk from internal flooding. To quantify the internal at-power flood model, new flooding events were added to the existing integrated loop cut internal events model and this was integrated with the high level logic developed from the flood specific ETs. A qualitative uncertainty, sensitivity, importance, and cliff-edge effects analyses was conducted as part of the 2023 PARA-Flood.

5.5 At-Power Seismic

The PARA-Seismic assessment has been developed following the methodology for preparation of a PSA-based Seismic Margin Assessment (SMA) as described in the OPG PNGS-A PSA Guide for Seismic Events. The major activities of the PSA-based SMA methodology and its application in the development of the PARA-Seismic assessment are summarized in the subsections below.

The primary steps in developing the PSA-based SMA are identifying the seismic hazard at the site, constructing an ET and FT model of the plant to represent the credited heat sinks following a seismic event, and creating new equipment failure modes based on the likelihood of equipment failure due to the seismic event. The PSA-based SMA is created based on the Internal Events At-Power PSA (PARA-L1P).

The PARA-Seismic model considers sequences that result in severe core damage (FDC1 and FDC2). Based on seismic capacity evaluations of the PNGS-A shutdown systems, however, the failure to shutdown sequences (FDC1) were ruled out. OPG prepared the seismic assessment following a phased approach with two phases defined:

- **Phase 1 – PSA-Based Seismic Margin Assessment** – In Phase 1, a Probabilistic Safety Assessment-based Seismic Margin Assessment (PSA-based SMA) is performed based on the methodology described in NUREG/CR-4482 [R-26]. This focused approach uses a plant model based on PARA-L1P with the addition of new seismic failure modes. The seismic failure events are developed from a seismic margin approach with generic variabilities and the time average seismic risk is calculated in terms of a point estimate of SCDF that does not include a full uncertainty analysis.

- **Phase 2 - Seismic PSA (SPSA)** – In Phase 2, significant conservatisms due to simplifying assumptions in the Phase 1 analysis are reduced, where feasible, in an effort to increase the computed seismic capacity of plant SSCs included in the seismic model; computed fragilities are refined for risk-significant SSCs based on the refined analysis; and the seismic model is extended as needed to provide a reasonably realistic estimate of plant seismic SCDF and allow a quantitative evaluation of significant uncertainties.

The decision to implement a Phase 2 study is based on the results of the Phase 1 study. For PNGS-A, a Phase 1 PSA-based SMA study was performed and the results showed that there was no need to transition into Phase 2.

The major activities of the PSA-based SMA methodology and its application in the development of the PARA-Seismic assessment are summarized below:

- Seismic hazard characterization (Task 1);
- Plant logic model development (Task 2);
- Seismic response characterization (Task 3);
- Plant walkdown and screening reviews (Task 4);

- Seismic fragility development (Task 5); and
- Seismic risk quantification (Task 6).

These tasks are briefly described in Sections 5.5.1 to 5.5.6 of this report. The integration of these tasks is shown in Figure 10.

In addition to the above tasks, the impact of seismically-induced internal fires and seismically-induced internal floods on seismic risk at PNGS-A has been evaluated qualitatively, considering potential significant sources at the station.

5.5.1 Seismic Hazard Characterization (Task 1)

The first step in the PSA-based SMA is to model the site-specific seismic hazard. The seismic hazard is a representation of the possible earthquakes and seismic activity that can be experienced at the site. The seismic hazard is a plot of the peak ground acceleration versus the annual frequency that the ground acceleration will be exceeded (typically described as the frequency of exceedance). Figure 11 shows a typical seismic hazard curve. The curve shows that very small ground accelerations are more likely than very large ground accelerations.

The site-specific seismic hazard curve is used to define the earthquake characteristics used in the PSA-based SMA. The earthquake ground motion under analysis is greater than the seismic design of the plant in order to understand the plant capacity to survive a beyond design basis earthquake. The beyond design basis earthquake under consideration is referred to as the Review Level Earthquake (RLE) or Reference Earthquake (RE).

The RLE (or RE) is the earthquake selected to represent the fundamental seismic input (demand) for calculating seismic response and fragilities of the credited equipment and structures. The plant level seismic capacity is further determined. The seismic hazard curve for the station is used to translate these results into a point estimate of the SCDF due to seismic events.

5.5.2 Plant Logic Model Development (Task 2)

This task involved two related but separate sub-tasks: development of the high-level plant logic and development of the Seismic Equipment List (SEL). The SEL identifies the structures, systems and components (SSCs) credited in the PSA-based SMA. This task relies upon the internal events PSA and other safe shutdown analyses to define the SSCs required to mitigate seismic IEs.

The seismic ET was developed to display and account for the seismic impact on SSCs important to subsequent ability to provide key safe shutdown functions. The seismic ET addresses:

- The seismically induced failure of buildings and other structures. The collapse of a building was assumed to result in the failure of all equipment contained in that building.

- The seismically induced failure of the seismic route. The seismic route is a qualified pathway that allows operators to safely travel to areas of the plant in which manual field action is required to maintain the long-term post-accident heat sink.
- The seismically induced failure of non-seismically qualified equipment. For example, seismic events were assumed to cause a loss of Class IV power. The loss of Class IV power, in turn, fails many other systems, e.g. main HTS pumps and main boiler feed pumps.
- The seismically induced failure of the HTS and/or the main steam system.
- The seismically induced failure of rugged equipment. This branch point represents the plant equipment screened in Task 4.
- The failure, seismically induced and random, of equipment in the systems that mitigate the consequences of a seismic event.

In this study, the seismic ET has been developed only for the Level 1 aspect of PSA, whereas the development of the seismic equipment list is applicable to both Level 1 and Level 2 PSA aspects. An ET is not needed for the Level 2 portion of this study as the robustness of containment is assessed using a simplified approach.

5.5.3 Seismic Response Characterization (Task 3)

The next step in the seismic PSA is to characterize how the station buildings respond to a seismic event. The response of the building will not be the same on each elevation. For example, the small earthquakes occasionally experienced in southern Ontario are typically undetectable to people in the basement or lower floors of buildings, but can be easily detected by people in the higher floors of tall buildings.

The ground oscillation of any seismic event can be described by a combination of frequencies. This is called the spectrum of the seismic event. Each potential seismic event may have a different spectrum. The different frequencies in an earthquake’s spectrum will be transferred to the building in different ways. The response of site buildings determines how the earthquake will affect the credited equipment in the PSA-based SMA and is used to calculate the probability of equipment failure due to a seismic event.

In Phase 1, a generalized scaling approach is used to calculate the response of the site structures. This method is based on the existing design basis earthquake seismic response analyses for the site structures, prepared as part of the Pickering A Seismic Assessment performed between 1995 and 1998, with updates to reflect the shapes of the new seismic hazard curves. In addition to characterizing the site structures response, this task defines the local accelerations for the credited equipment.

5.5.4 Plant Walkdown and Screening Reviews (Task 4)

Plant walkdowns were required to assess the relative vulnerability of equipment to seismic challenges. The walkdowns were performed by fragility experts in order to document the basis for screening equipment in (based on susceptibility) or out (based on ruggedness) of the PSA-based SMA. The plant walkdowns included taking photos and recording observations of the SEL items which were located in accessible areas. The screening level chosen needs to be high enough such that the contribution from screened-out SSCs is not significant to overall seismic risk. In addition, equipment required for crediting EME was also assessed during the walkdown.

The purposes of the plant walkdown are to:

- Observe as many of the SEL items as possible and record any deficiencies;
- Screen the inherently seismically rugged equipment items from the seismic model;
- Define the failure modes (e.g., functionality, structural integrity, or anchorage failure) of the SEL items that are not screened out, and identify further evaluations required;
- Identify SSC correlation considerations (e.g., identical equipment with same configuration/orientation/anchorage on same level of same building);
- Identify equipment or structures that are not included in the SEL, but whose structural failure could potentially impact the nearby SEL items (i.e., seismic interaction concerns).
- Examine operator response pathways for potential seismic-induced interference (e.g., potential for collapse of block walls or other obstructions due to unrestrained equipment).
- Perform “walk-by” of selected samples of generically screened items to ensure no conditions exist that invalidates the screening.
- Perform “walk-by” of SSCs that are not designated as the lead items to check for anomalies in the similarity basis of an equipment grouping.
- Address issues of seismic-induced fires and seismic-induced flooding.

The results of the walkdowns were recorded using Screening Evaluation Worksheets (SEWS) tailored to each equipment class according to the applicable standards.

5.5.5 Seismic Fragility Development (Task 5)

The likelihood that a given piece of equipment will fail for a given seismic hazard is based on the fragility of the equipment. The seismic fragility of a piece of equipment is the conditional probability that the equipment will fail when subjected to a specific acceleration caused by a seismic event. The likelihood that equipment will fail increases as it is subjected to greater seismic acceleration.

Figure 12 shows an example fragility curve. This example shows that if the given equipment is subjected to an acceleration of 1g, its failure probability is 80%.

The fragility analysis conducted for a PSA-based SMA is limited to that of the Conservative Deterministic Failure Margin (CDFM) method, whereby the seismic capacity is calculated in terms of a High Confidence of Low Probability of Failure (HCLPF) value using a generic representation of the variability according to the applicable standards and practices [R-20].

5.5.6 Seismic Risk Quantification (Task 6)

The seismic risk is evaluated using a PSA-based SMA model. To build the PSA-based SMA model, the information on the seismic response of the buildings and the seismic fragility of the equipment is used to calculate the probability of equipment failures. The process of evaluating seismic risk is similar to that used for the PARA-L1P (see Section 5.1.6) and involves the following steps:

- The branches of the seismic ET that result in severe core damage are converted to high level logic in the form of a FT.
- The high level logic is then integrated with the FTs for the mitigating systems and their support systems. It is important to note that the system FTs are revised to include seismically induced failures of SSCs based upon Tasks 4 and 5.
- The cutsets including seismically induced failures are reviewed using the MIN-MAX method to identify the limiting accident sequence and the plant level HCLPF.
- The plant level HCLPF is convolved with the mean seismic hazard curve (Task 1) to estimate the seismically induced SCDF.
- Non-seismic cutsets, representing random failures of credited system, are also considered in the determination of SCDF following a seismic event, in the same manner as they are for internal events PSAs.
- Human error probabilities are adjusted by a series of multipliers dependent upon the severity of the earthquake and time available to complete the task.
- A discrete approximation of the hazard curve is made by dividing the hazard curve into nine bins as shown in Table 17.
- The total SCDF is the sum of seismically induced SCDF and the SCDF from the cutsets that include non-seismically induced failures.

Qualitative uncertainty, sensitivity, importance, and cliff-edge effects analyses were carried out for the SCDF estimation.

5.6 At-Power High Wind

The PNGS-A High Wind PSA (PARA-Wind) was prepared following the methodology for preparation of a high wind PSA as described in the OPG High Wind Hazard PSA Guide. The major activities of the high wind PSA methodology and its application in the development of the PARA-Wind assessment are summarized in the subsections below.

The primary steps in developing the high wind PSA are identifying the high wind hazard, identifying the high wind targets, developing windborne missile fragilities for the high wind targets, evaluating the pressure fragilities of the high wind targets, developing the high-level plant logic, and quantifying the high wind scenarios. The high wind PSA model is created based on the Internal Events At-Power PSA model (PARA-L1P).

The methodology for high wind hazard assessment follows six main tasks as follows:

- High Wind hazard analysis (Task 1);
- Analysis of windborne missile risk (Task 2);
- High Wind fragility and combined fragilities (Task 3);
- Plant logic model development (Task 4);
- Plant response model quantification (Task 5); and
- Estimate of High Wind LRF (Task 6).

These tasks are briefly described in Sections 5.6.1 to 5.6.5 of this report. The relationship between these tasks is shown in Figure 13.

In addition, a plant walkdown is required as an important support task to provide information on the special layout of the site, structural vulnerability and the potential for missile generation. Several site walkdowns of the Pickering site were conducted in 2012, 2013, and 2014 as part of the development of the earlier versions of the PNGS-A and B high wind PSA studies. A site walkdown of the PNGS site (i.e. PNGS-B and PNGS-A) was completed in October 2021 in support of the 2023 PARA-Wind update.

5.6.1 Task 1 - High Wind Hazard Analysis

The purpose of this task is to evaluate the frequency and intensity of occurrence of various straight winds (thunderstorms and extratropical cyclones), hurricane and tornado wind hazards based on site-specific and region-specific data.

In accordance with the High Wind PSA Guide, the hurricane wind hazard is not modeled because the Pickering site is not subject to hazardous hurricane winds.

In the PARA-Wind, the spatial extent of these hazards was analyzed or estimated based on available data sets from sources such as Environment Canada, Ontario Climate Centre, US National Weather Service Storm Prediction Centre, US National Oceanic and the Atmospheric Administration Storm Prediction Center. The wind hazard curve is developed for peak gusts in open terrain at 10 m height. Terrain, height, and averaging time adjustments were performed to adjust gust wind data to 3 second gust speed at a height of 10 m in flat open terrain. Figure 14 shows an example of high wind hazard curves.

The high wind hazard analysis is used as the basis for defining a set of high wind IEs for the high wind plant response model. The separate curves for tornadoes and straight winds were discretized into several subintervals of wind speeds for each hazard type. IEs were defined for the subintervals of each hazard type and were inserted into the high wind plant response model.

5.6.2 Task 2 - Analysis of Windborne Missile Risk

The purpose of this task is to develop wind-borne missile fragilities for the plant targets.

Windborne missile fragility is defined as the probability of target damage (failure) from windborne missiles for a given value of the reference wind speed used in the hazard analysis.

Windborne missile risk includes:

1. Flying missiles that hit/damage an exterior target.
2. Flying missiles that enter a building and hit an interior target.
3. Flying missiles that originate within a building and hit an interior target.

A list of high wind targets was generated in Task 4 - Plant Logic Model Development. The missile risk was derived based on missile sources, plant layout, and plant design information taking into account applicable uncertainties.

Windborne missile risk does not include consideration of failure or collapse of a building onto its own interiors. Windborne missile risk does not include collapse of stacks or other tall structures onto plant SSCs. These failure modes are considered structural interactions and are modelled as part of wind pressure fragility analysis.

Fragility functions are developed for each SSC subject to windborne missile risk. Interior SSCs in highly vulnerable structures may be represented by a single fragility function that does not separately consider missiles, provided the building failure is judged to occur prior to (or simultaneously with) the initiation of significant missile hazard at the site.

The EPRI-developed TORMIS methodology was utilised to estimate the probability of tornado missile impact and damage to plant structures and components ([R-21] and [R-22]). The updated TORMIS model for the 2023 PARA-Wind reflected the missile inventory data from the latest site walkdown and incorporated new targets for SSCs added to the High Wind Equipment List (HWEL).

5.6.3 Task 3 - High Wind Pressure Fragility and Detailed Rainwater Fragility Analysis

The purpose of this task is to evaluate the fragility of buildings and/or HWEL SSCs due to high wind pressure effects, including the aerodynamic forces produced by the dynamic pressure component of the wind flow and where appropriate, Atmospheric Pressure Change (APC) that may occur from the low central pressure region within tornadoes.

In 2023 PARA-Wind, the wind pressure fragilities are developed for both non-tornado and tornado winds for each of the credited SSCs. An advanced code-based methodology [R-23] has been applied in the development of the PNGS-A wind pressure fragilities. 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. Basic fragility functions are developed for each cladding material within each pressure zone on the building envelope.

Additionally, a detailed wind pressure fragility analysis was performed for the PNGS-A and PNGS-B Powerhouses and PNGS-B EWPS building in order to develop wind driven rain fragilities of the safety-related equipment inside these buildings. Those fragilities were used to quantify the structural interaction failure of electrical equipment located within these buildings. The wall cladding and roof fragilities for those buildings were further refined with a detailed rainwater fragility analysis, to reduce the conservatism and uncertainty associated with using code-based fragilities for application to these water-sensitive electrical components.

5.6.4 Task 4 - Plant Response Model Development

The high wind plant response model is built on the PARA-L1P model for severe core damage. It is modified to reflect wind-caused IEs and to incorporate high wind failures and other wind analysis aspects that are different from the corresponding aspects in the Internal Events PSA model.

The PARA-Wind plant response model was constructed by modifying the accident sequence logic from the PARA-L1P Forced Shutdown (FSD) ET. The PARA-Wind plant response model is a fully integrated single-top FT that includes accident sequence logic for a set of high wind IEs, combined with mitigating and support system FT logic that has been modified to incorporate wind-related failures of equipment and to reflect high wind impacts on human error probabilities. The plant response model provides the means for estimating the SCDF in Task 5.

5.6.5 Task 5 - Plant Response Model Quantification

This task is performed to finalize and quantify the high wind scenarios developed by modifying the integrated severe core damage (FDC2) model of PARA-L1P. This task involves the integration of the high wind hazard and fragility information with the overall plant PSA logic model. This involves linking the fragility information to appropriate sequences and basic events in the plant logic model. The high wind hazard curve used in the high wind hazard characterization is then integrated with the plant logic model containing the fragility information to determine high wind risk in terms of Severe Core Damage. In addition to providing the overall frequencies for each sequence, this quantification identified dominant accident sequences, component failures, and human actions with respect to high wind risk.

The quantification of high wind accident sequence frequencies requires first quantifying the frequency of occurrence of each initiating event and the logic models developed to represent the failure probabilities of the ET top events.

The ET top event failure probability models include not only the impact of wind speed on plant failure probabilities, but also of random failures unrelated to the wind speed. The high wind initiating event frequencies and ET top event probabilities are then combined similar to the approaches followed for non-high wind IEs. By combining the frequencies of high wind sequences over all high wind IEs, the end state frequencies for high wind risk are determined.

The parametric uncertainty analyses are carried out for the SCDF result. A number of sensitivity analysis cases are performed to examine the risk significance of key assumptions from the high wind plant logic model development and quantification on the High Wind results.

Sensitivity cases were selected in part based on a review of assumptions with a potential for a large increase in SCDF given a small change to the assumption demonstrate that there are no significant cliff-edge effects related to the risk estimation results.

5.6.6 Task 6 - Estimate of High Wind LRF

The purpose of this task is to estimate the High Wind LRF based on the results form the Level 1 High Wind PSA. The approach involves manual interrogation of the high wind FDC2 cutsets and use of insights from the full scope PARA-L2P study (section 6.1). More details on this task are discussed in Section 6.6.

6.0 LEVEL 2 PSA METHODS

Section 5.0 described the methods used for the Level 1 PSA assessments of PNGS-A. In the Level 1 PSA, the goal is to quantify the frequency of fuel damage. Once the fuel has been damaged, there is the potential for radioactive material to be released from the fuel into containment. The Pickering A NGS design includes a containment system (described in Section 2.14.3) designed to prevent the release of any radioactive material from the station into the environment.

A Level 2 PSA studies the system failures and accident phenomena that might result in an airborne release of radioactive material to the environment, and the timing and magnitude of the release. This information is combined with the PARA-L1P model to quantify the frequency of possible releases.

6.1 Level 2 At-Power Internal Events PSA

The PNGS-A Level 2 At-Power Internal Events PSA (PARA-L2P) model has been developed following the methodology for preparation of a Level-2 PSA as described in the OPG Pickering A Leve 2 PSA Guide. The consequence assessment is performed by simulating the accident sequences using the MAAP5-CANDU version 5.00a code. The major activities of the Level-2 PSA methodology and its application in the development of the PARA-L2P are summarized in the subsections below.

6.1.1 Interface with Level 1 PSA

The PARA-L1P identifies a set of accident categories that represent various degrees of damage to fuel in the reactor core and estimated their frequency. These sequences form the starting point of the PARA-L2P.

The PARA-L1P categorizes the severe core damage states into fuel damage categories (FDCs), described in Section 5.1.2. For Pickering A, the only sequences that are binned as FDC1 and FDC2 are considered for inputs into the Level 2 PSA. The first step of a Level 2 PSA is to assign the sequences in these FDCs to Plant Damage States (PDSs). The PDSs are the interface between Level 1 and Level 2, and are used as a means to reduce the number of the sequences assessed in the Level 2 analysis to a manageable number while still reflecting the full range of possible accident sequences and their impacts on the plant.

Four PDSs are assigned in the PARA-L2P. FDC1 is conservatively assumed to cause early consequential containment failure and is assigned to a unique PDS, PDS1. For PDS 1, which represents severe core damage due to failure to shutdown, MAAP-CANDU simulations are not performed to assess the consequences related to failure to shutdown. The consequence of PDS1 with containment failure is addressed conservatively by assigning PDS1 to a release category containing sequences involving severe core damage and containment impairment. The consequence of PDS1 without containment failure is assigned to a release category containing sequences involving severe core damage and no containment impairment. The containment impairment branch is assigned RC1. With no early containment impairment, the PDS1 sequence is assigned to NRC. NRC is termed as “No Release Category” which represents end states that do not contribute to Small Release Frequency (SRF) or LRF. Hence, the PDS 1 sequences are not subjected to consequence analysis using a bridging or a CET.

FDC2 is not assumed to result in immediate containment failure and is subdivided into three PDSs (2-4) to examine the potential for random and consequential failures of containment systems that could eventually lead to enhanced release to the environment:

- PDS2 represents sequences resulting in severe core damage at a single unit as the result of failure of all heat sinks. That is, single unit sequences in FDC2 that do not result in a bypass of containment were assigned to PDS2.
- PDS3 represents sequences resulting in severe core damage at more than one unit. That is, multi-unit sequences in FDC2 were assigned to PDS3. In the PARA-L2P, PDS3 was subdivided into two categories:
    - i) PDS3-2U which represents severe core damage at Units 1 and 4, but not severe core damage at any Pickering B units.
    - ii) PDS3-6U which represents sequences where multiple units at Pickering A and B have severe core damage.
- PDS4 represents sequences resulting in severe core damage at a single unit as the result of failure of all heat sinks with a release pathway that bypasses containment, e.g. boiler tube leaks.

PDS2 is further sub-divided into eight, labeled PDS2A to PDS2H, to reflect various random containment system failures. The defining attributes of PDS2A through to PDS2H are captured by use of a Bridging Event Tree (Figure 15).

It is important to note that the branch points in the Bridging Event Tree that represent failures of the FADS are subsequently eliminated from the PARA-L2P as it was not expected to affect the LRF results for any plant damage state. FADS is designed to maintain containment pressure below atmospheric pressure in the longer term primarily for design basis accident sequences after accident progression is terminated. The use of the system during severe accident progression raises questions about its ability to continue to function as designed given the conditions to which it might be exposed. In the PARA-L2P study, FADS showed minimal risk benefit and so was no longer credited in the accident sequences.

For Level 2 analysis, the characteristics of each PDS are represented by a single representative accident sequence. By design, the plant damage states group sequences expected to generate similar magnitude and timing of fission product release to containment and containment response. However, the frequency and releases for each sequence will vary to some extent.

The Level 1 PSA is used to identify IEs that are significant contributors to the frequency of the plant damage state. These sequences are then reviewed to select a representative sequence that bounds the consequence. The hybrid approach follows the guidance of the IAEA as this method selects a sequence that “largely bounds” the PDS. The representative sequences chosen for each PDS are summarized in Table 18.

6.1.2 Containment Event Tree Analysis

In Level 2 PSAs, Containment Event Trees (CETs) are used to delineate the sequence of events and severe accident phenomena after the onset of core damage that challenge successive barriers to radioactive release to the environment. They provide a structured approach for the evaluation of the capability of a plant, specifically its containment boundary, to cope with severe core damage accidents. The entry points into the CETs are the plant damage states that involve severe core damage.

A CET is a logic model that addresses uncertainties in the ability to predict the potential impacts of accident progression and associated physical phenomena on containment response. Figure 16 shows a generic CET.

CET top events are not built from system based “success criteria” but from questions that are intended to ascertain the magnitude of phenomenological challenges to the containment boundary (e.g., “Is containment integrity maintained?” or “Does core concrete interaction occur?”). The CET branch points represent major events in accident progression and the potential for fission product release to the environment. The CET also represents the evolution of the progression with time so the same nodal question may appear more than once in the tree as conditions inside containment change. The focus of the CET is to estimate the probabilities of the various ways that containment failure may occur leading to a release of radionuclides to the environment.

Most of the CET branch points represent alternative possible outcomes of a given physical interaction. Depending on the availability of suitable models and data for a given physical interaction or phenomenon, the methods of branch point quantification can vary. The acceptability of these probability estimates is supported via an expert review process.

6.1.3 Containment Fault Trees

Containment system FTs are required to quantify the frequencies of the end-states of PDS2A – PDS2H in the Level 1/Level 2 PDS2 Bridging Event Tree. The Bridging Event Tree, shown in Figure 15, has branches representing the following failures:

CEI:	Impairment of Containment Integrity
PRV:	Pressure Relief Valves (PRVs) Fail to Open to Limit Containment Pressure for LOCA Events
ACU:	Failure of the air cooling system
IGN:	Failure of the hydrogen igniters system to regulate hydrogen concentration

The FT models are prepared following the same general methodology as the FTs for the PARA-L1P (Section 5.1.4). The FT models used in the quantification of the Level 2 PSA are listed in Table 13. Where systems are shared between PNGS-A and PNGS-B, the FTs from the PNGS-B At-Power Internal Events PSA were used. FT representations for failure of these containment functions have been developed, reflecting the likelihood that random equipment failure or human error will prevent the operation of the system on demand or during the mission. Containment failures arising as a consequence of severe accident progression are addressed in the CET.

6.1.4 Release Categorization

The CET analysis generates a multitude of end states associated with each specific severe accident sequence. The CET end states are binned into Release Categories (RCs), to facilitate comparison with safety goals (Table 1) and for use in subsequent applications. The RCs are defined based on two criteria:

- The magnitude of release in Becquerel (Bq) of specific radionuclides considered important to offsite impacts (e.g., isotopes of cesium or iodine); and
- The timing of the release, either early in the accident sequence (where “early” is less than 24 hours) or late (after 24 hours).

The release categories in the PARA-L2P were limited to those that result in a large release of radioactive material to the environment. Table 19 presents the release categories used in the PBRA-L2P analysis. LRF is defined to be the sum of RC1 through RC3.

6.1.5 MAAP-CANDU Analysis

MAAP-CANDU (Modular Accident Analysis Program – CANDU) is a severe accident simulation code for CANDU nuclear stations [R-24]. It is used to calculate the consequence of severe accidents and is designated as a CANDU Owners Group (COG) Industry Standard Toolset (IST) code. MAAP-CANDU originated from MAAP developed for Pressurized Water Reactor (PWR) and Boiling Water Reactor (BWR) systems by Fauske and Associates (FAI).

MAAP-CANDU can simulate the response of a CANDU power plant during severe accident sequences. The code quantitatively predicts the evolution of a severe accident starting from full power conditions given a set of system faults and IEs through events such as core melt, HTS failure, calandria vessel failure, shield tank failure, and containment failure. Severe accident analysis carried out using MAAP-CANDU is the cornerstone of the Level 2 PSA. There are at least five distinct roles for the code, as outlined below:

- To establish the baseline accident progression for each plant damage state and the potential impact of associated physical phenomena on CET top events;
- To determine the sensitivity of phenomena to reasonable variations in key parameter values to support CET branch point quantification;
- To calculate releases to the environment for those sequences for which a non-zero probability of a containment failure mode has been estimated to support categorization of releases;
- To generate results to support systematic sensitivity and uncertainty analysis; and
- To provide information related to plant environmental conditions.

6.1.6 Severe Accident Management Guidelines

SAMG are entered when plant conditions reach the point where actions being attempted using AIM procedures and/or EME guidelines are no longer effective and severe core damage is considered imminent. The goals of SAMG are to terminate fission product releases from the plant, maintain or return containment to a controlled, stable state, and return the core to a controlled and stable state.

SAMG documentation is treated as guidance, compared to AIM response, which uses procedures. The type of actions included in SAMG range from recovery of systems typical in the prevention of severe core damage (i.e., ECI, moderator cooling) to crediting systems or injections lineups in non-traditional ways that are not typically included in the AIM response.

While Phase 1 EME is used prior to the entry into SAMG as a prevention mechanism, it can also be used within the SAMG framework if not successful in preventing severe core damage.

Credit for SAMG actions has been incorporated into the Level 2 PSA model.

6.1.7 Integration of the Level 1 and 2 PSA

The purpose of integration is to link the Level 1 ETs with the PDSs via the Level 1/Level 2 Bridging Event Tree and containment FTs, and then with the RCs via the CET end-states using the results of the branch point quantification. The product is a complete set of sequences that contribute to each RC, from which the frequency of each RC can be determined.

Importance analysis is performed to identify the dominant contributors to each RC.

Sensitivity and uncertainty analysis is performed on both the frequency quantification and on the MAAP-CANDU consequence assessment.

6.2 Level 2 Outage Assessment

Given the low risk of fuel damage from internal events occurring while the unit is in GSS, a full Level 2 study of the outage risks is not performed. Instead, a reduced scope consequence assessment was undertaken for a limited number of representative sequences occurring during each of the PNGS-A outage POSs. The focus of the analysis was on modeling of accident progression and source term estimation with the following goals:

1. Determine if severe accidents while in a shutdown POS progress more slowly than severe accidents in high power units. If this is the case, then the risk from a multi-unit event occurring while a single unit is operating in a shutdown POS is driven by the transients in the high power units.
2. Determine if severe accidents while in a shutdown POS pose unique challenges to the containment boundary. If no unique challenges are identified, then it is reasonable to assume that the LRF for a shutdown POS will be much lower than the already extremely low shutdown state SCDF.

The plant configuration in each POS is reviewed for potential containment failures (random failures, containment bypass, or consequential containment failure). A limited number of outage specific considerations are identified that might impact the severe accident progression. In addition, the consequence assessment is performed by simulating the accident sequences using the MAAP-CANDU 5.00a code.

6.3 Level 2 Fire Assessment

This assessment is built on the results of the PARA-Fire Level 1 quantification described in Section 5.3.11 to consider the Level 2 impacts of fire scenarios in terms of LRF. If fire scenarios are identified in Level 1 that would affect multiple units (e.g., MCR and other Unit 0 scenarios), the multi-unit impact on Level 2 must be identified.

The assessment of the LRF contribution for each fire scenario from the Level 1 quantification involves evaluating each fire scenario against the potential mechanisms by which a severe core damage event could progress to a large release in the scenario. The analysis identifies the following large release mechanisms following core damage:

1) FDC1 accident sequences progress to large release;

2) The potential for the fire scenario to result in a multi-unit severe core damage event;

3) The impact of the fire scenario on equipment credited in the PARA-L2P model;

4) Random probability (not induced by the fire) of failure for equipment credited in the PARA-L2P model;

5) The probability of occurrence of severe accident phenomenological events that can lead to an Early Calandria Vessel Failure (ECVF).

The LRF estimate is performed using a simplified LRF ET and conditional containment failure probabilities based on the insights from the PARA-L2P model.

In addition, qualitative uncertainty, sensitivity, and importance analyses are carried out for the LRF estimation.

6.4 Level 2 Seismic Assessment

The Level 2 seismic assessment is intended to characterize the likelihood of a significant radioactivity release given a seismically-induced severe core damage event.

Due to the correlated and multi-unit nature of the seismic initiating event at the PNGS site (i.e., concurrent PNGS-A and PNGS-B units response following a seismic event), it is conservatively assumed that the seismic event will impact similarly all reactors on the PNGS site. It is postulated, therefore, that both PNGS-A units and all four PNGS-B units, will experience the same accident progression. Since the PNGS containment cannot survive the overpressure transient created by such a scenario, it is conservatively assumed that the LRF estimate is equal to the SCDF estimate, and no detailed calculation is performed.

In accordance with the PNGS-A PSA Guide for Seismic Events, an alternative analysis of containment robustness in response to seismic event is performed. This is done based on fragilities of the containment SSCs using an additional Level 2 metric - the Seismically-Induced Containment Failure Frequency (SCFF). Walkdowns and fragility calculations, using the same techniques as those described in Section 5.5.5, were used to assess the seismic fragility of containment components.

HCLPF values for containment structures, systems and components were evaluated to determine the limiting HCLPF for containment integrity. A convolution of the plant-level limiting containment fragility with the mean hazard curve for the station produced the PNGS-A SCFF. The SCFF is estimated to be 4.6E-08 per year over the range of events up to and including those with recurrence frequency of 1E-04 per year. This demonstrates that the containment is structurally robust and can survive earthquakes significantly stronger than the Design Basis Earthquake (DBE) for PNGS-B[6].

6.5 Level 2 Flood Assessment

A bounding estimate of the LRF at PNGS-A from internal flooding IEs is performed using SCDF cutsets interrogation and insights from PARA-L2P.

To estimate LRF due to internal flooding, the cutsets are classified into one of the following three groups:

- Cutsets involving single unit with flooding event inside the Reactor Building (RB);
- Cutsets involving single unit with flooding event outside RB; and
- Cutsets involving two units.

Cutset interrogation is performed to determine the fraction of each type of sequence that progresses to a large release. The sum of the contribution from each group is then used to estimate LRF caused by internal flooding.

---

[6] Although PNGS-A has not been designed to seismic events, the containment is common for both PNGS-A and PNGS-B. Therefore, the comparison is made to the PNGS-B DBE.

In addition, qualitative uncertainty, sensitivity, and importance analyses are carried out for the LRF estimation.

6.6 Level 2 High Wind Assessment

The Level 2 high wind assessment is performed to estimate the LRF based on the results from the Level 1 High Wind PSA.

Per guidance provided in the OPG High Winds PSA Guide, it has been a common practice for OPG's PSAs for external events, e.g., high winds and seismic events, to assume that all units at a multi-unit station are perfectly correlated, i.e., the accident sequence is exactly the same in all affected units.

The high wind hazard analysis is performed based on the Pickering NGS site as a whole, and the high wind IEs were assumed to initially affect all units. The methodology involves manual interrogation of the high wind FDC2 cutsets and use of insights from the full scope PARA-L2P study. The following are considered:

- The number of units involved in the accident;
- The potential for consequential containment failure after both single and multi-unit accidents, e.g., combustion of hydrogen; and
- The potential for random containment failure, e.g., random containment envelop impairment.

The parametric uncertainty analysis is carried out for the LRF estimate. A number of sensitivity cases are performed to confirm there were no cliff-edge effects associated with key assumptions used in the development of the LRF estimate for PARA-Wind.

6.7 Non-Reactor Source PSA

While the hazard screening analysis had screened out all hazards associated with the UFDS facility, selected internal and external hazards for the fuel in the IFBs were screened in. Consequences of these hazards are characterized as a loss of IFB heat sink or a loss of IFB water inventory. Bounding simplified quantitative assessments were used for the following hazards:

- Small Aircraft Impact
- Rail Transportation Accident – Cold Toxic Gas Release: Chlorine, Sulphuric Acid and Sulphur Dioxide
- Earthquake
- Flooding - Due to Run Off
- Flooding - Due to Combined Events

- Meteorological Extremes - High and Low Temperature, Rainfall, Snow, Freezing Rain, Snowpack
- Meteorological - Hurricanes / Tornadoes, Ice Storms
- Mist
- White Frost
- Frazil Ice
- Geomagnetic Storm
- Bio-fouling
- Combined Hazards Events
- Random IFB Cooling System Failures
- Random IFB Support Systems Failures
- Human Errors
- Internal IFB Fires
- Internal IFB Flooding
- Reactor Hazards That May Impact IFB Cooling System Equipment Operation
- Random Loss of IFB Water Inventory

An assessment of interactions between accident progressions in reactor units and IFBs was also conducted. Cliff-edge effects were analyzed, and it was concluded that there were no cliff-edge effects requiring further actions to better characterize their effects or to develop mitigating actions. An LRF estimate based on the bounding simplified quantitative assessments for the hazards listed above was performed, and the results are presented in Table 25.

7.0 SUMMARY OF RESULTS AND CONCLUSIONS

7.1 Severe Core Damage and Large Release Frequencies

The PARA study uses two measures to assess the acceptability of risk. These two measures correspond to the OPG risk-based safety goals:

- Frequency of severe core damage (SCDF); and

- Frequency of large release (LRF).

Table 20 compares the results of the Internal Events PSA studies described in Sections 5.0, and 6.0, with the OPG safety goals.

OPG has safety goals for the severe core damage and large release frequencies. The safety goal represents the tolerability of risk exposure above which actions shall be taken to reduce risk.

The Internal Event PSAs assess the full range of fuel damage and release categories defined in Table 11, Table 16 and Table 19. The frequency of fuel damage for the At-Power Internal Events PSA (PARA-L1P) is presented in Table 20. The results show that failure to shutdown is a negligible contributor to SCDF.

As described in Section 6.1, the fuel damage categories used as end states in the Level 1 PSA are partitioned into PDSs to use as inputs into the Level 2 PSA. Table 22 presents the frequencies of the PDSs, and Table 23 presents the results of PARA Level 2 At Power (PARA-L2P).

The risk results for internal fires, seismic events, internal flooding, and high wind events are presented in Table 24. The fire, seismic, flood, and high winds results are all below the OPG safety goals for severe core damage and large release frequencies.

While the LRF due to a seismic event is bounded by the SCDF, the assessment of the containment fragility concluded that containment is robust and can survive earthquakes significantly stronger than the design basis earthquake.

7.2 Conclusions

The PNGS-A PSA complies with the CNSC Regulatory Document REGDOC-2.4.2 [R-1]. The PSA addresses Level 1 and Level 2 PSA aspects for various internal and external events, both at-power and outage operating conditions, including internal events, internal fires, internal flooding, seismic, high winds and non-reactor sources. In addition, an external and internal hazard screening assessment has been performed.

As described in Section 7.1, the 2023 PARA results satisfy OPG’s safety goal for all internal and external hazards considered, and hence represent very low public risk. OPG continues to meet industry best practices through periodic PSA updates to account for OPEX and changes at the station.

8.0 REFERENCES

[R-1] Canadian Nuclear Safety Commission, “Probabilistic Safety Assessments (PSA) for Nuclear Power Plants”, Regulatory Document REGDOC-2.4.2, May 2014.

[R-2] CSA Group, “Management System Requirements for Nuclear Facilities”, CSA N286-12.

[R-3] CSA Group, “Quality Assurance Program Requirements for the Supply of Items and Services for Nuclear Power Plants, Category 1”, CSA N299.1-16.

[R-4] CSA Group, “Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants”, CSA N286.7-16.

[R-5] CSA Group, “Probabilistic Safety Assessment for Nuclear Power Plants," N290.17-17, April 2017.

[R-6] Canadian Nuclear Safety Commission, Probabilistic Safety Assessments (PSA) for Nuclear Power Plants, Regulatory Standard S-294, April 2005.

[R-7] OPG, "Seismic Assessment of Pickering A Nuclear Generation Station Summary Report," CD# NA44-REP-02004-0073, Volumes 1-7, 1998.

[R-8] CSA Group, "General requirements for seismic design and qualification of nuclear power plants," N289.1-18, May 2018.

[R-9] United States Nuclear Regulatory Commission, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants", NUREG/CR-6928, January 2007.

[R-10] Westinghouse Savannah River Company, "Savannah River Site Generic Database Development", File # WSRC-TR-93-262, Revision 1, May 1998.

[R-11] Ontario Power Generation, “Pickering NGS – 2021 Annual Risk and Reliability Report”, P-REP-09051.1-00021, R000, April 2022.

[R-12] Ontario Power Generation, "Simplified Human Reliability Analysis Process for Emergency Mitigation Equipment (EME) Deployment", N-REP-03611-10021, Revision 001, October 2014.

[R-13] United States Nuclear Regulatory Commission, "Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications", NUREG/CR-1278, August 1983.

[R-14] CAFTA 6.0b, Software Manual, EPRI, Palo Alto, CA: 2014. Software Product ID # 3002004316.

[R-15] FTREX User Manual - Version 1.9 EPRI, Palo Alto, CA and KAERI, Daejeon, South Korea: 2013. Software Product ID #: 3002012968.

[R-16] United States Nuclear Regulatory Commission, EPRI/NRC-RES Fire PSA Methodology for Nuclear Power Facilities, NUREG/CR-6850/EPRI 101-1989, Volumes 1 and 2, September 2005.

[R-17] EPRI, Fire Probabilistic Risk Assessment Methods Enhancements, Palo Alto, California USA and United States Nuclear Regulatory Commission Office of Nuclear

Regulatory Research (RES), Rockville, Maryland USA, EPRI TR-1019259 and NUREG/CR-6850 Supplement 1, September 2010.

[R-18] Nuclear Power Plant Fire Ignition Frequency and Non- Suppression Probability Estimation Using the Updated Fire Events Database: United States Fire Event Experience Through 2009. EPRI, Palo Alto, CA and U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Washington, D.C.: 2014. 3002002936/NUREG-2169.

[R-19] Electric Power Research Institute, "Pipe Rupture Frequencies For Internal Flooding Probabilistic Risk Assessments," EPRI 3002012997 Revision 4, Palo Alto, CA, September 2018.

[R-20] Electric Power Research Institute, Seismic Fragility and Seismic Margin Guidance for Seismic Probabilistic Risk Assessments, EPRI 3002012994, Palo Alto, CA, September 2018 (Corrected 2023).

[R-21] Electric Power Research Institute, "Tornado Missile Risk Analysis and Appendices", NP768 and NP-769, 1978.

[R-22] Electric Power Research Institute, "Tornado Missile Risk Evaluation Methodology Volumes 1 and 2", NP-2005, 1981.

[R-23] Twisdale, L.A., (2017). “Non-Parametric Method for Wind Pressure Fragility Analysis,” ANS 2017 International Topical Meeting on Probabilistic Safety Assessment and Analysis, Pittsburgh, PA, September 24-28, (2017).

[R-24] MAAP5-CANDU Modular Accident Analysis Program for CANDU Power Plant Volume 1: User Guidance, EPRI, February 2018

[R-25] Electric Power Research Institute, "Identification of External Hazards for Analysis in Probabilistic Risk Assessment (Update of EPRI Report 1022997)", EPRI 3002005287, 2015.

[R-26] United States Nuclear Regulatory Commission, Recommendations to the Nuclear Regulatory Commission on Trial Guidelines for Seismic Margin Reviews of Nuclear Power Plants, NUREG/CR-4482, Lawrence Livermore National Laboratory, Livermore, CA, 1986.

[R-27] IAEA, External Human Induced Events in Site Evaluation for Nuclear Power Plants, No. NS-G-3.1, 2002.

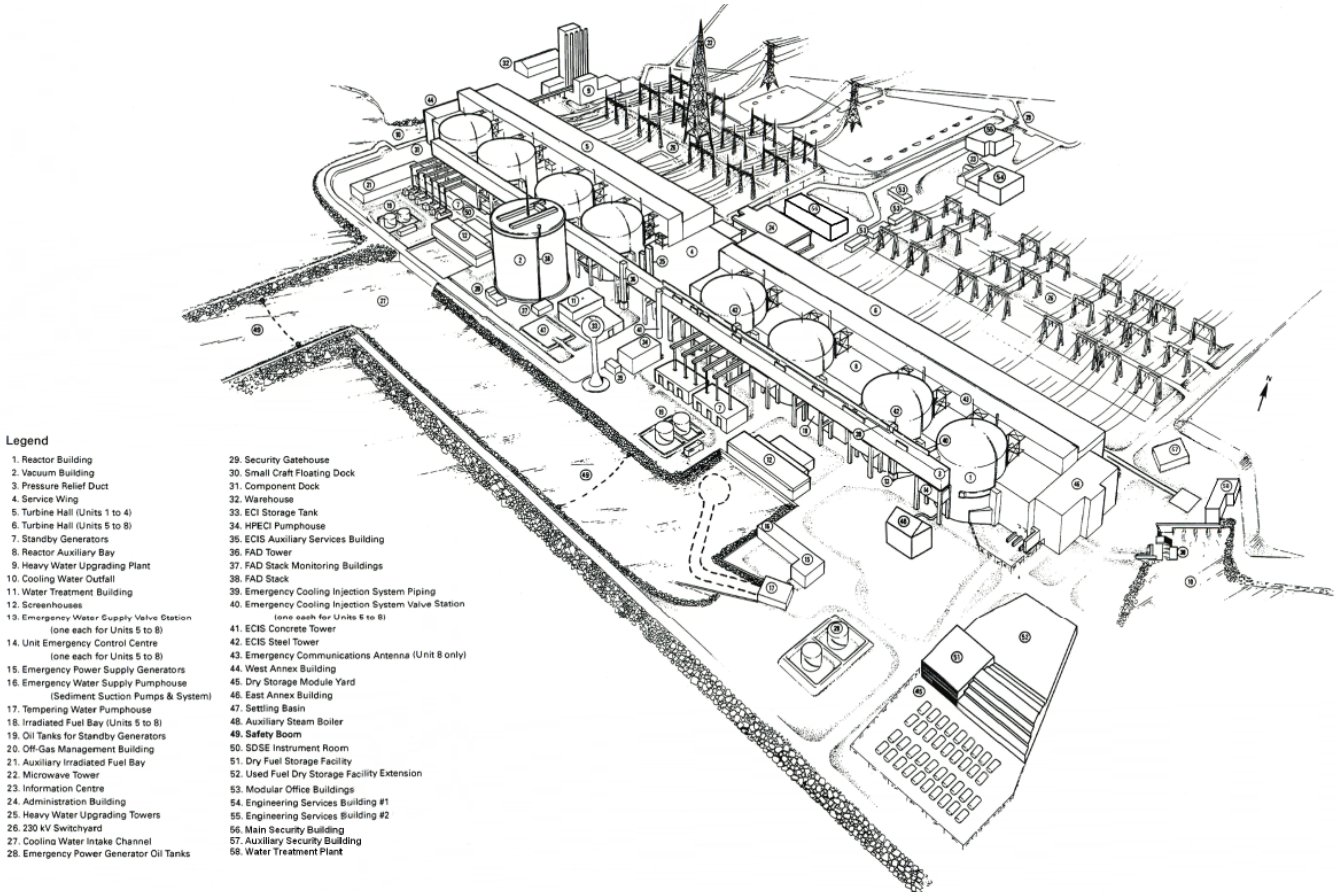


Figure 1: Pickering Site Layout

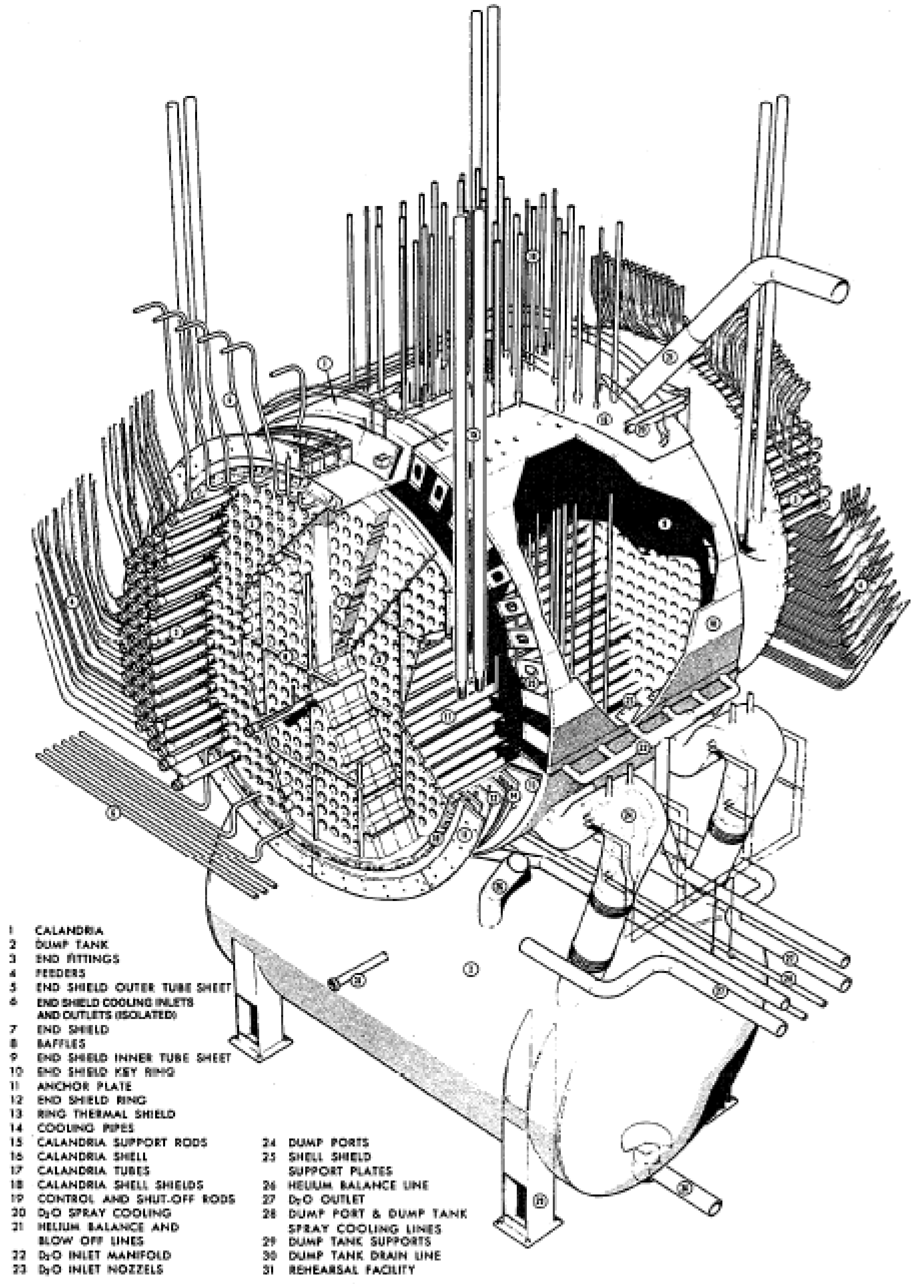


Figure 2: Pickering NGS ‘A’ Reactor Assembly

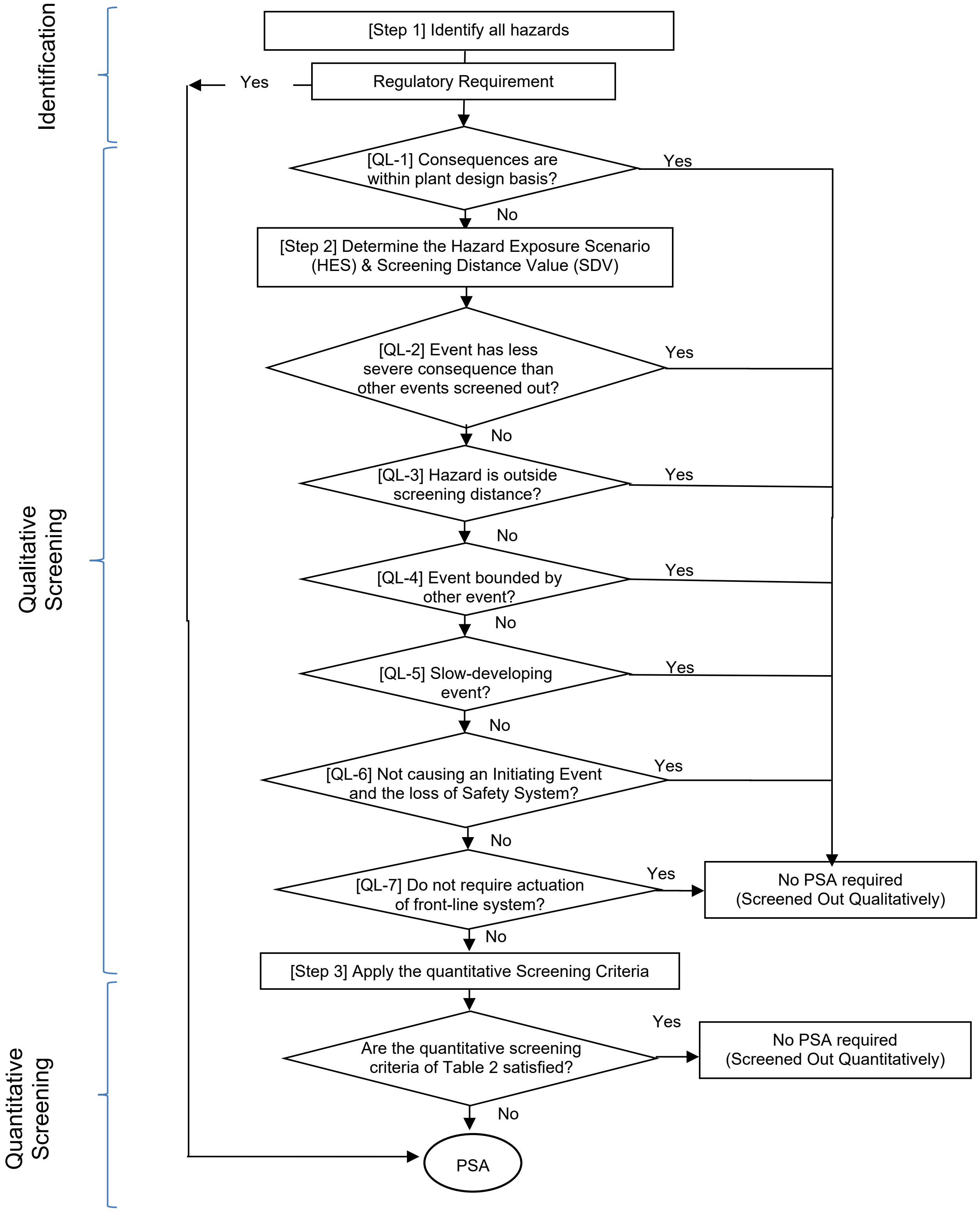


Figure 3: Hazards Analysis Steps

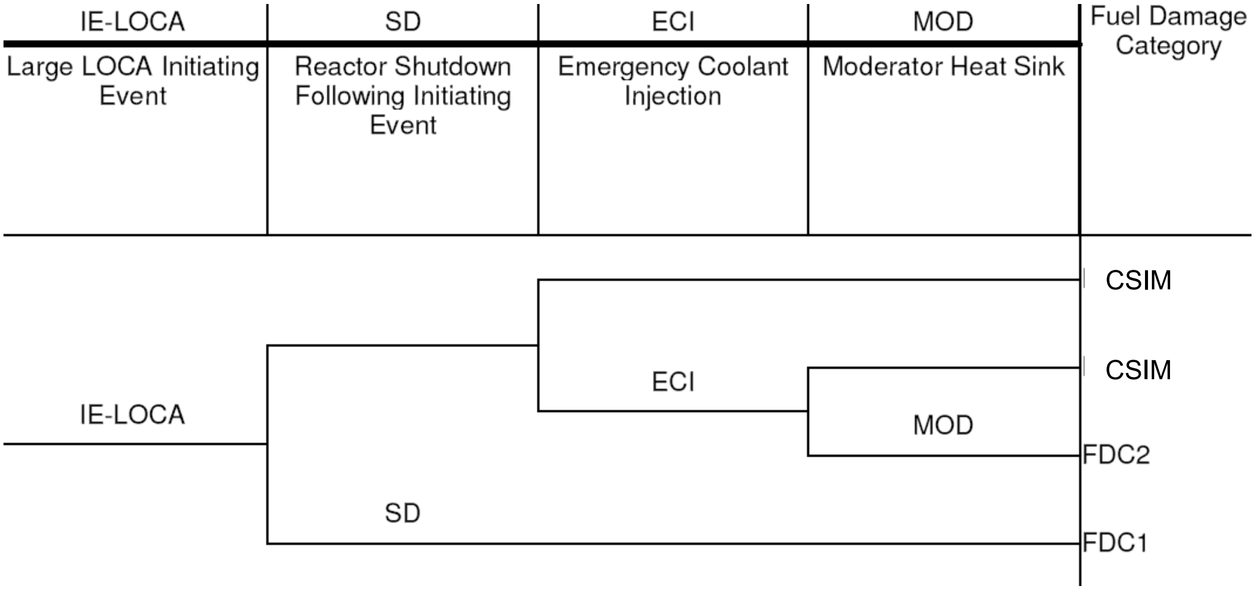


Figure 4: Example LOCA Event Tree

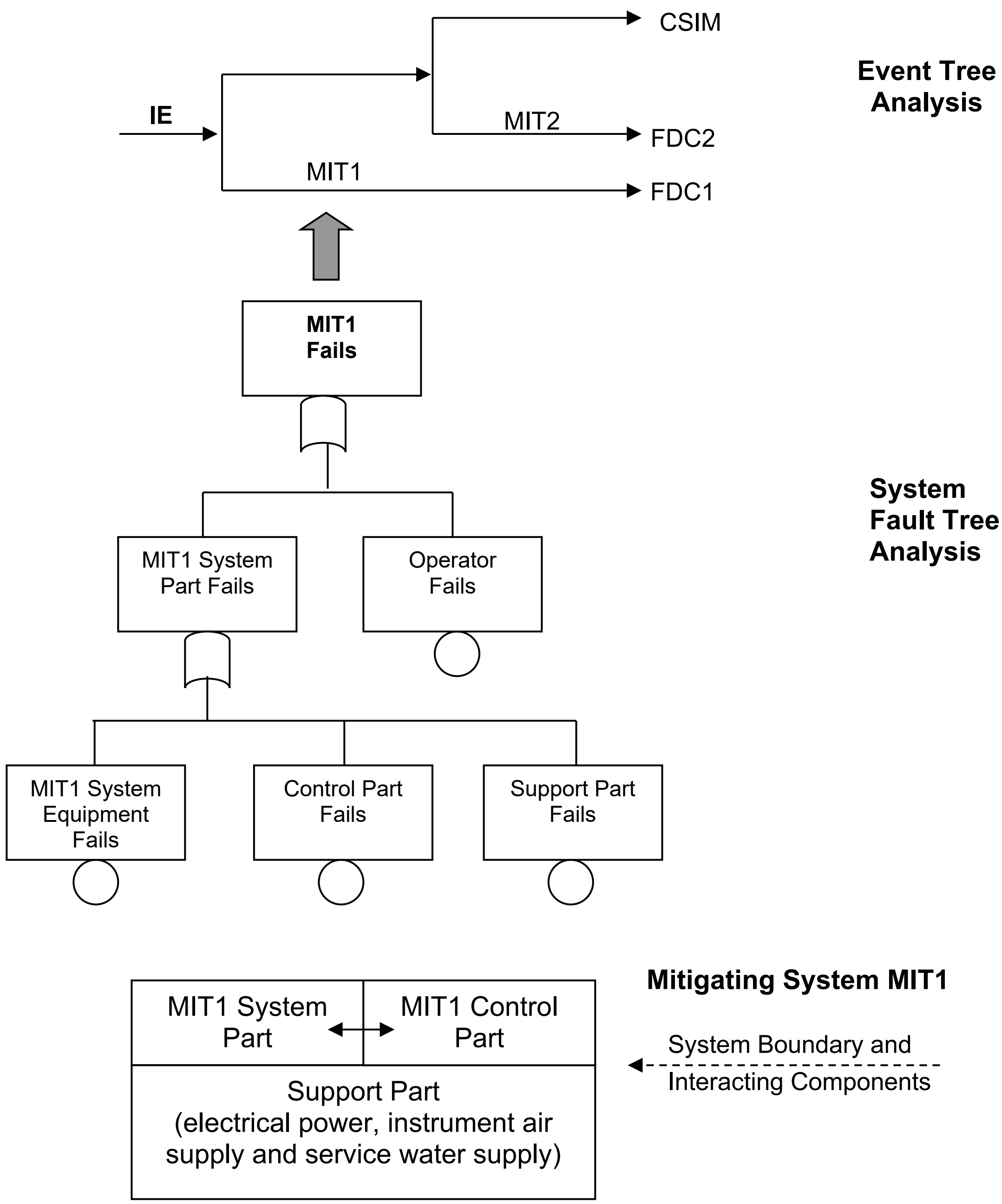


Figure 5: Fault Tree and Event Tree Integration

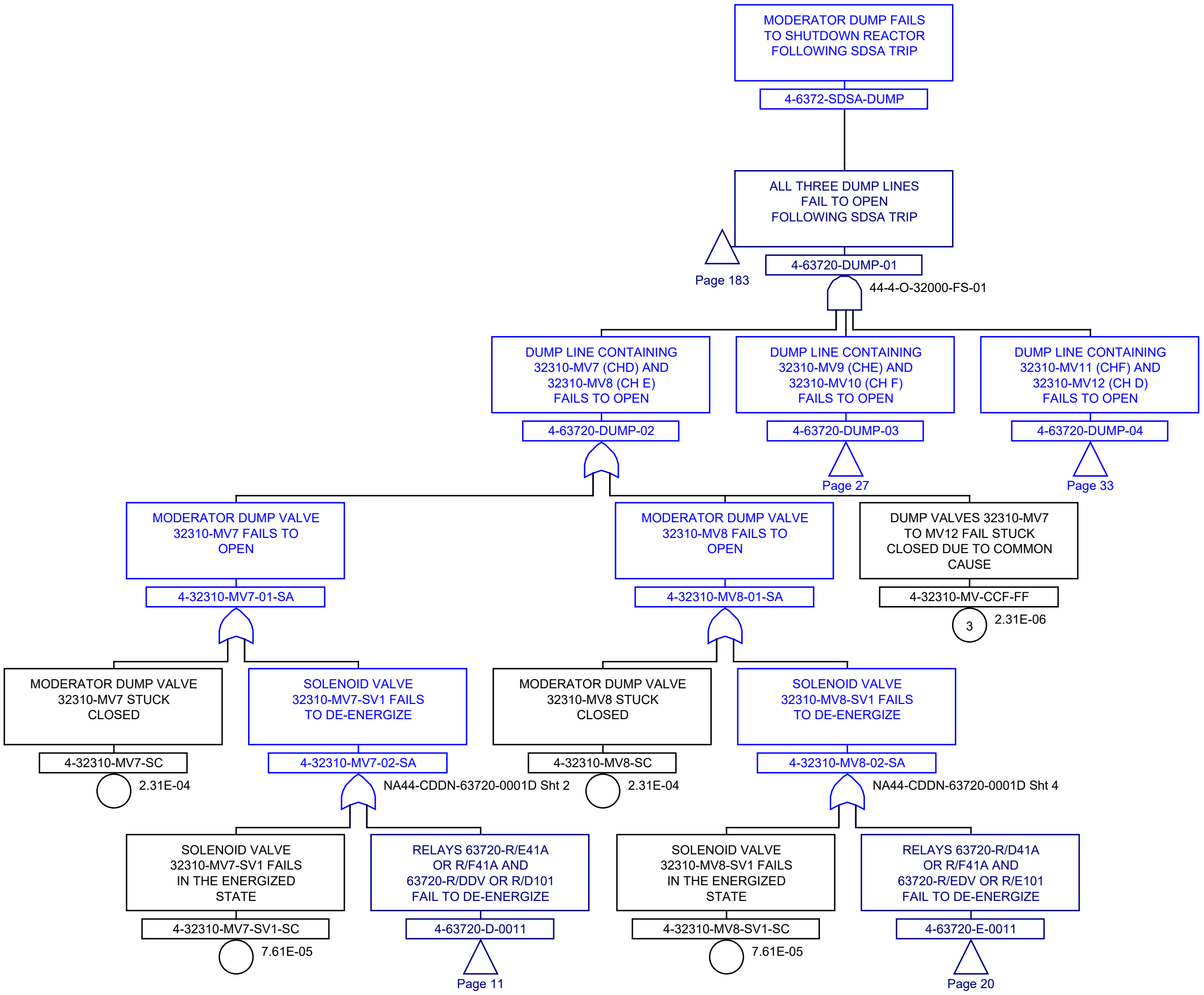


Figure 6: Example Fault Tree

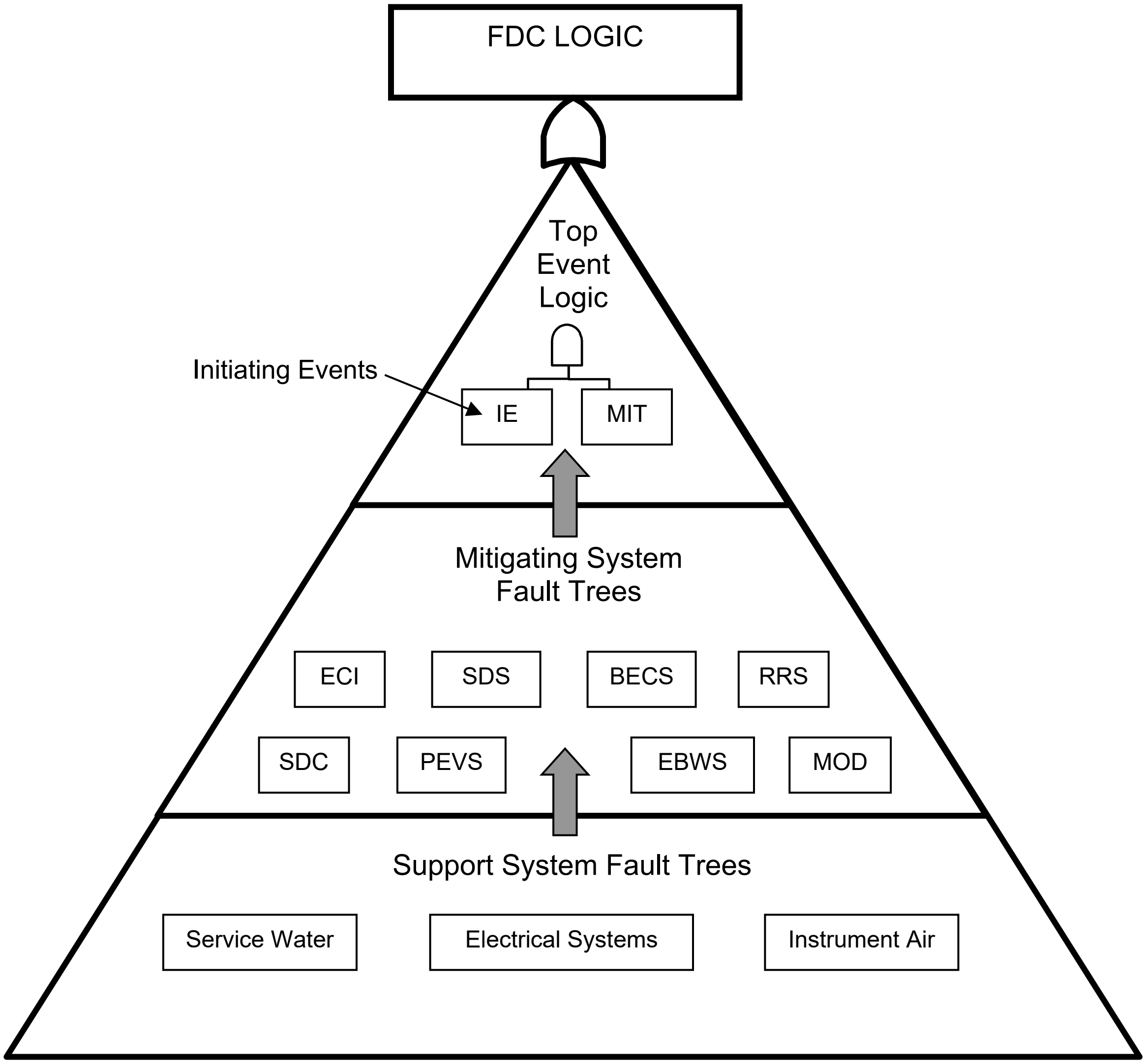


Figure 7: Fault Tree Integration

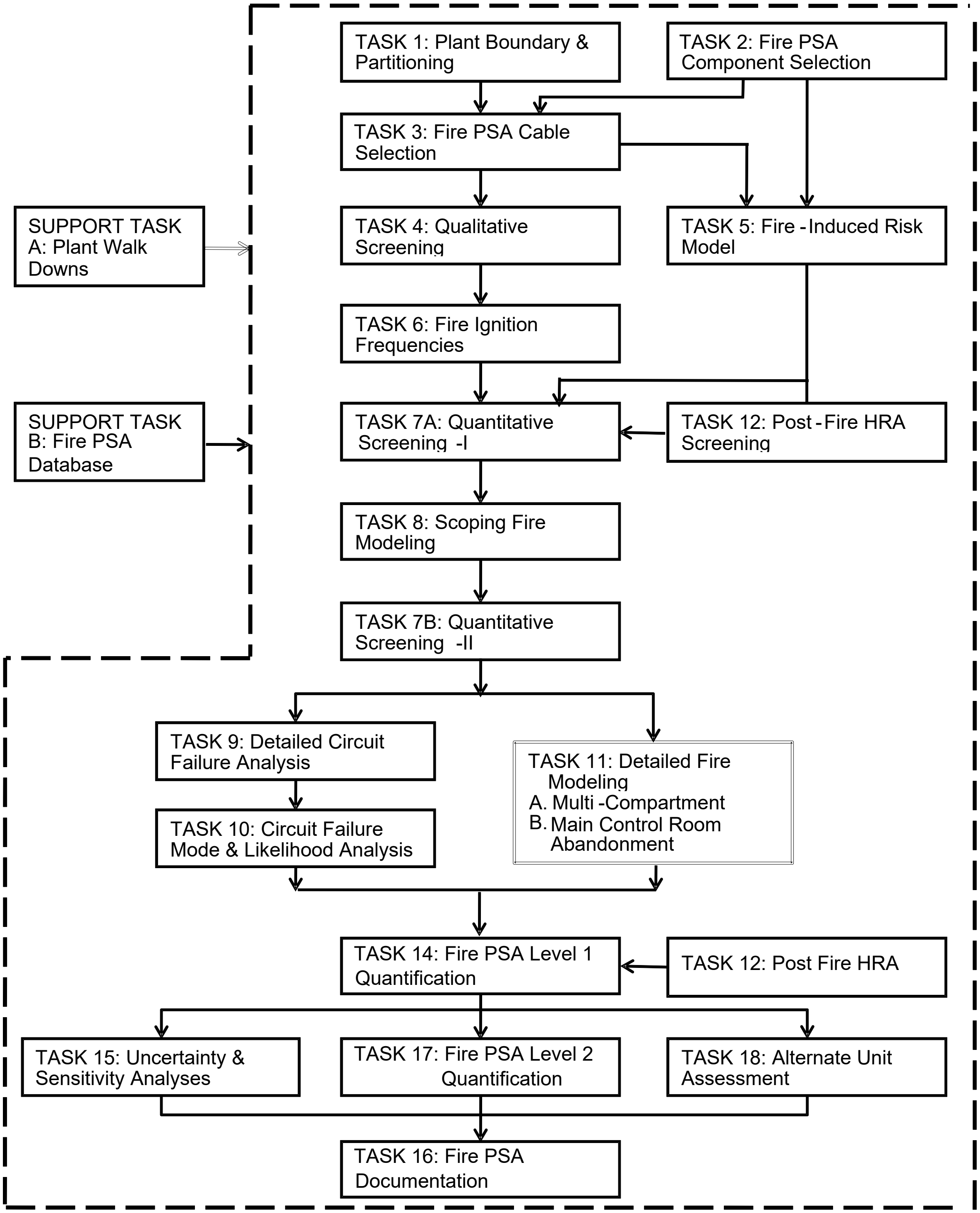


Figure 8: Fire PSA Tasks

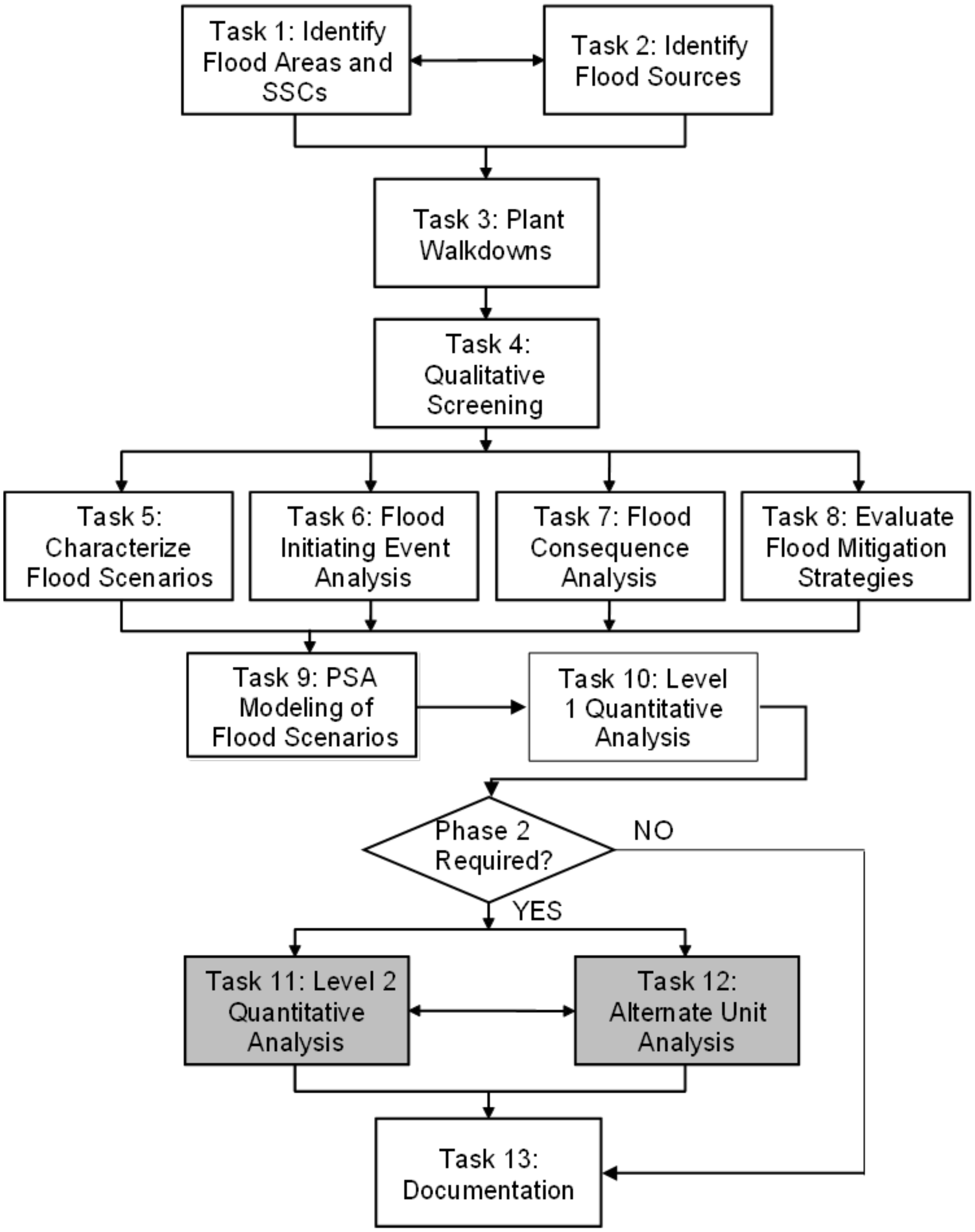


Figure 9: Internal Flood PSA Tasks

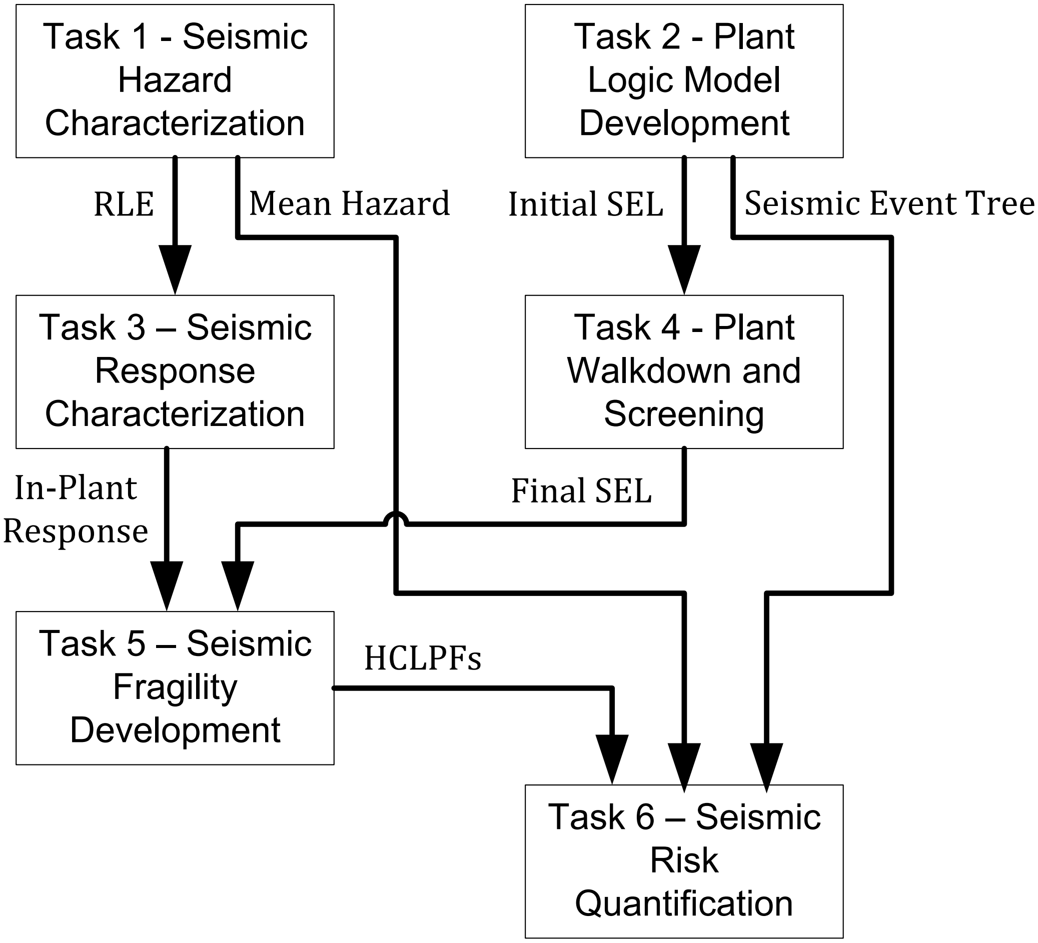


Figure 10: PSA-based SMA Tasks

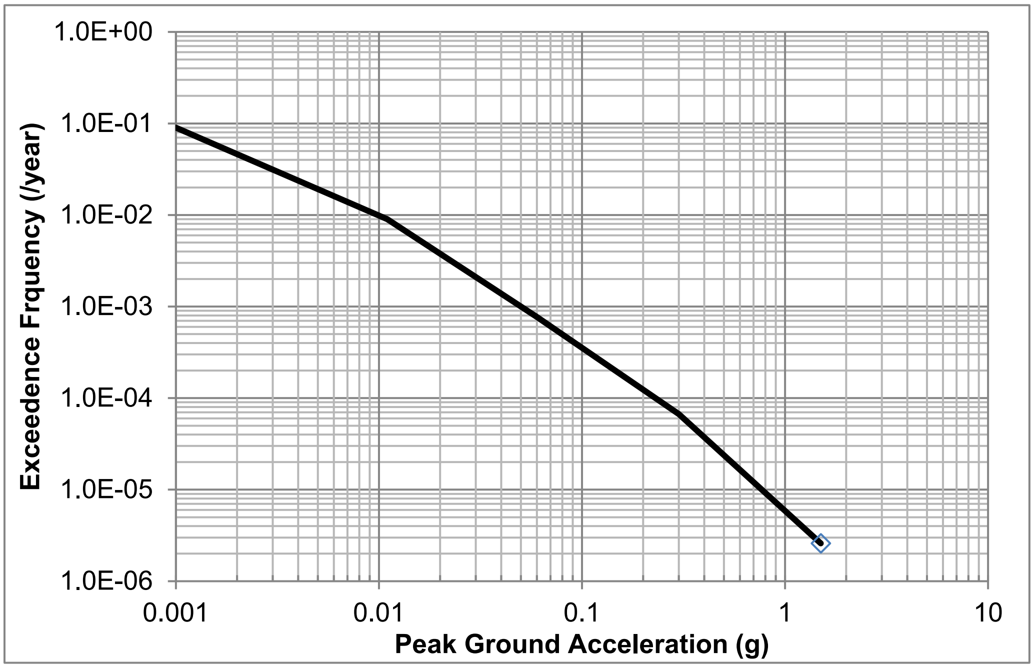


Figure 11: Example Seismic Hazard Curve

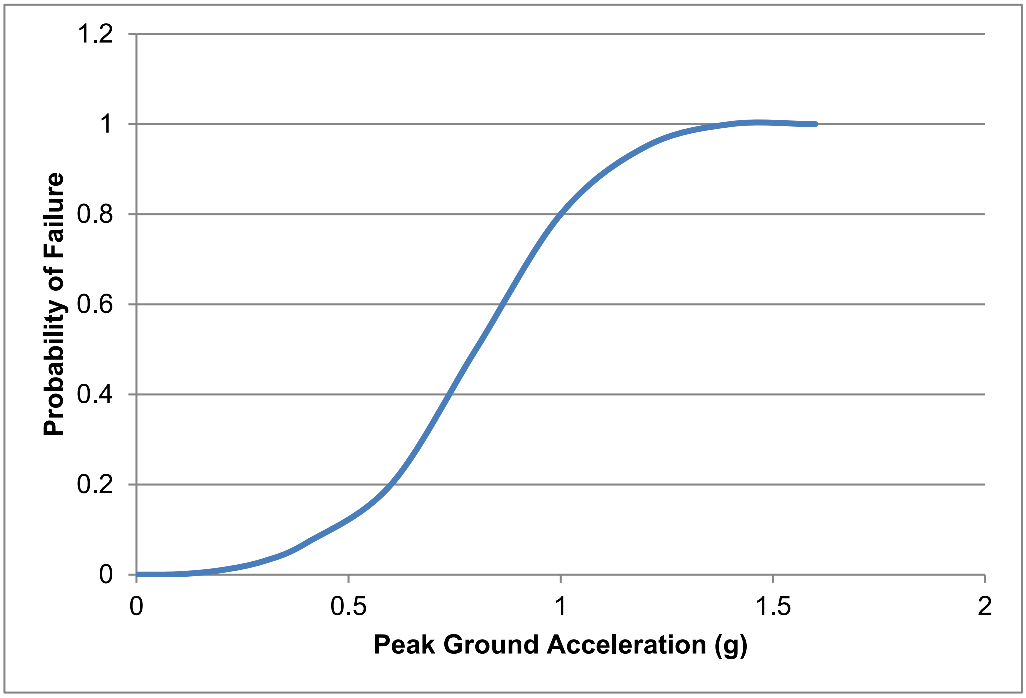


Figure 12: Example Fragility Curve

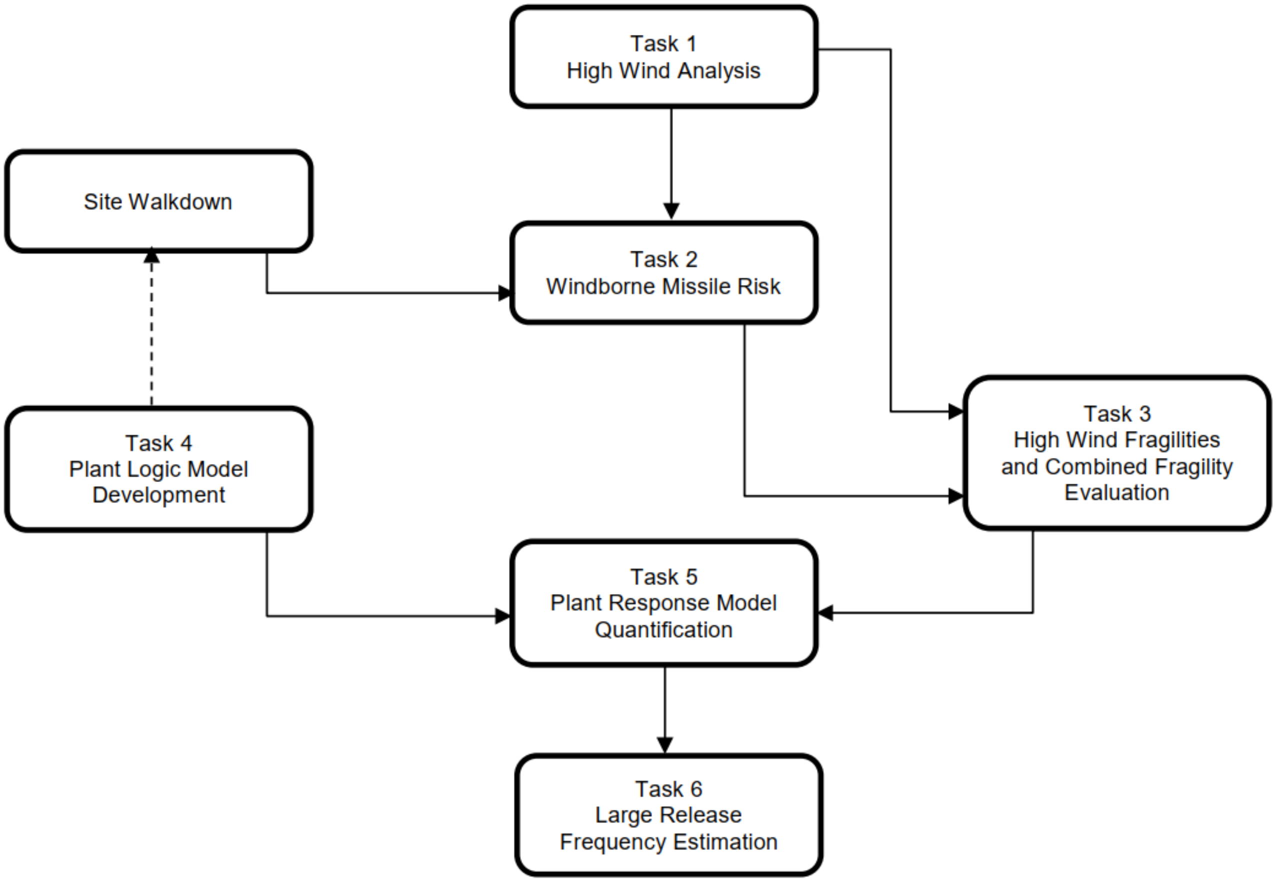


Figure 13: High Wind Hazard PSA Tasks

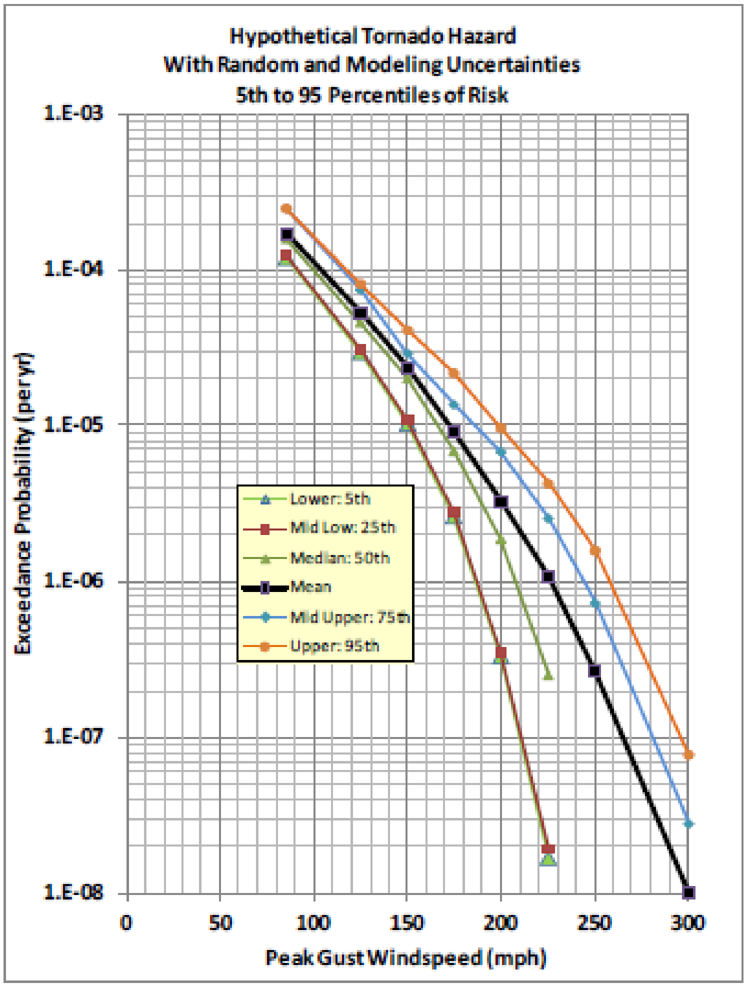
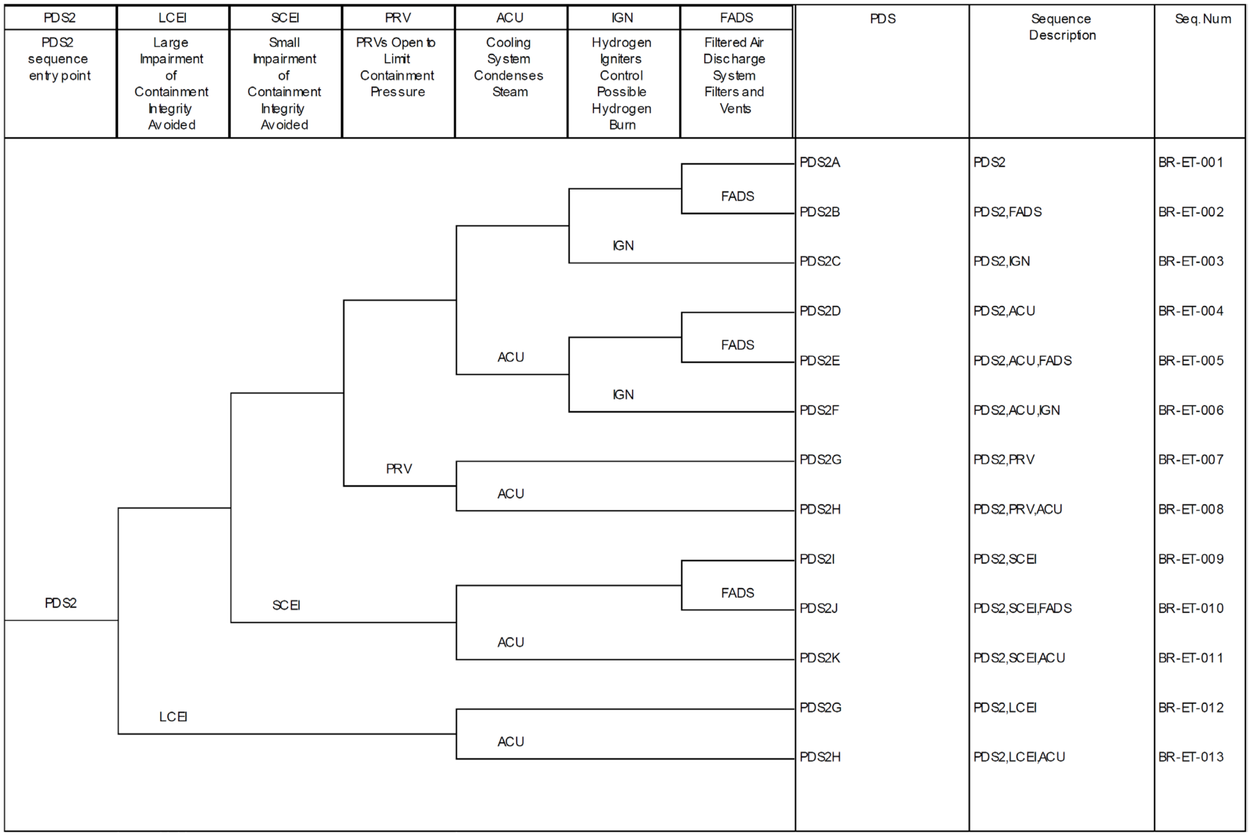


Figure 14: Example of High Wind Hazard Curves



PDS	Sequence Description	Seq. Num
PDS2A	PDS2	BR-ET-001
PDS2B	PDS2,FADS	BR-ET-002
PDS2C	PDS2,IGN	BR-ET-003
PDS2D	PDS2,ACU	BR-ET-004
PDS2E	PDS2,ACU,FADS	BR-ET-005
PDS2F	PDS2,ACU,IGN	BR-ET-006
PDS2G	PDS2,PRV	BR-ET-007
PDS2H	PDS2,PRV,ACU	BR-ET-008
PDS2I	PDS2,SCEI	BR-ET-009
PDS2J	PDS2,SCEI,FADS	BR-ET-010
PDS2K	PDS2,SCEI,ACU	BR-ET-011
PDS2G	PDS2,LCEI	BR-ET-012
PDS2H	PDS2,LCEI,ACU	BR-ET-013

Figure 15: Pickering NGS A Bridging Event Tree

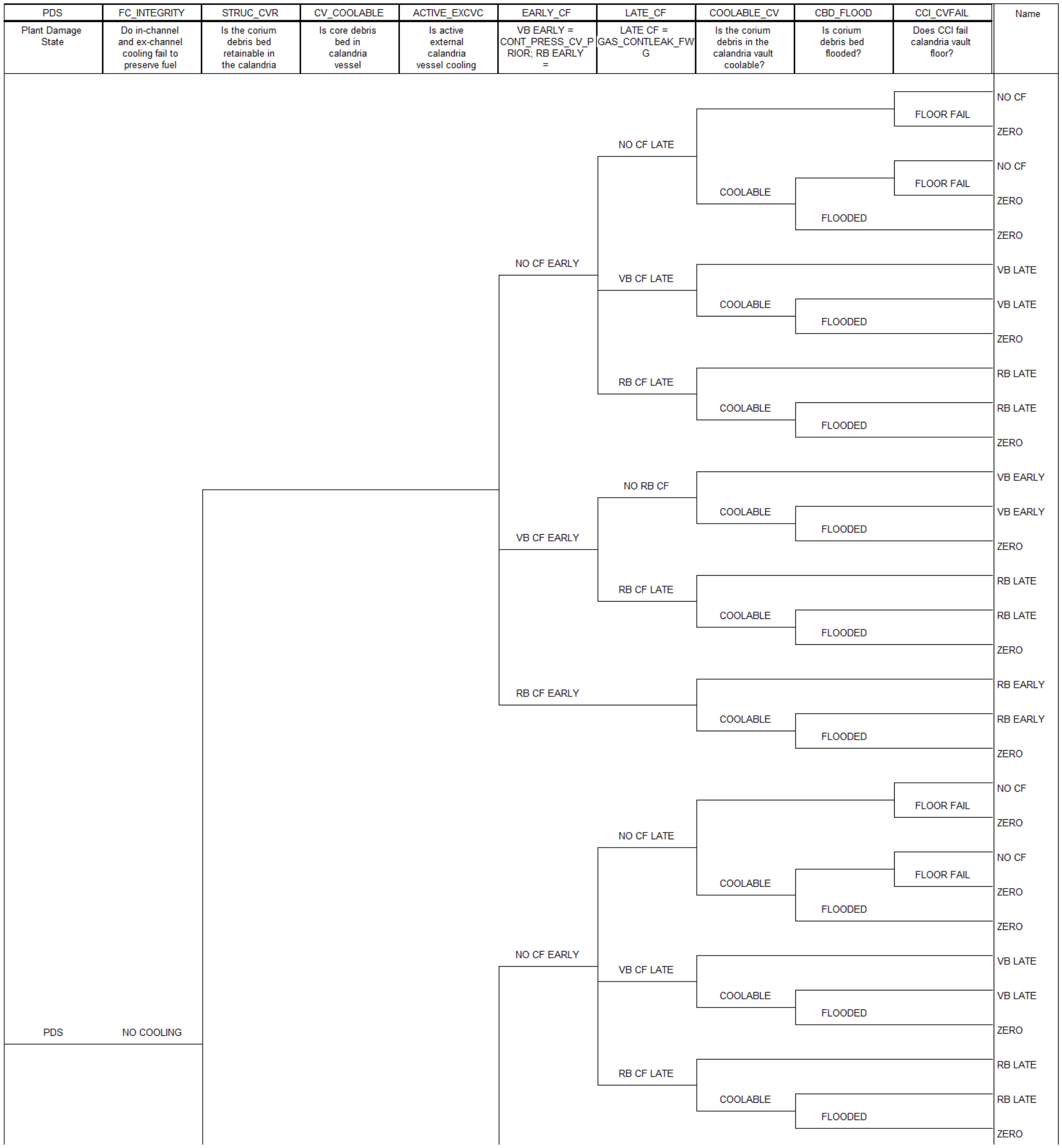


Figure 16: Generic Containment Event Tree

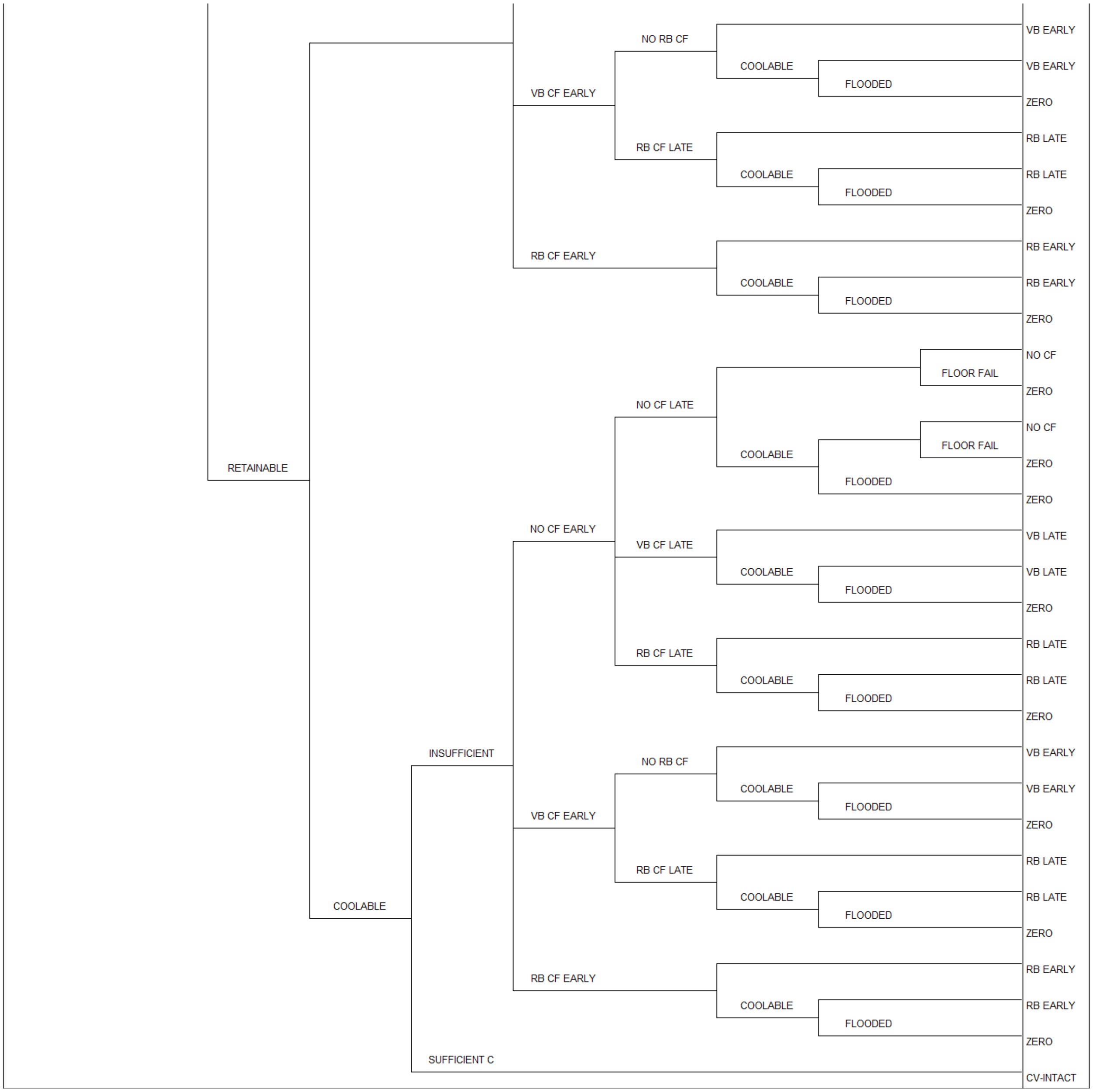


Figure 16: Generic Containment Event Tree (cont’d)

Table 1: OPG Risk Based Safety Goals

Criteria	**Average Risk (per year)**
	Safety Goal
Severe Core Damage[1] (per unit)	10^{-4}
Large Release[2] (per unit)	10^{-5}

[1] Severe Core Damage is the loss of core structural integrity.

[2] Large Release is a release greater than 1E14 Bq of Cs-137.

Table 2: Quantitative Hazard Screening Criteria

Criterion	Description (Note 1,2,3)	Direct Containment Bypass or Failure (Note 4)	Reference	Applicability of Screening Criteria to Reactor and/or Non-Reactor Sources
QN1	SCDF < 10^{-6} / yr.	No	EPRI 3002005287 [R-25]	QN-1 and QN-2 apply only to the reactor sources and not to the non-reactor sources
QN2	Design Basis Hazard Frequency < 10^{-5} / yr. and CCDP < 0.1 (Note 5)	No	EPRI 3002005287 [R-25]	
QN3	SCDF < 10^{-7} / yr.	Yes	EPRI 3002005287 [R-25]	This QN applies to the reactor sources only. An equivalent QN for non-reactor sources of LRF < 10^{-7}/yr will be considered
QN4	Design Basis Hazard Frequency < 10^{-6} / yr. and CCDP < 0.1 (Note 5)	Yes	EPRI 3002005287 [R-25]	This QN applies to the reactor sources only. An equivalent QN for non-reactor sources will be considered as follows: Design Basis Hazard Frequency, < 10^{-6}/yr and conditional large release probability (CLRP) < 0.1
QN5	IE or Hazard Frequency may be screened out if it can be shown that their frequency is < 10^{-7} / yr.	Not Applicable	CSA Standard N290.17 and IAEA NS-G-3.1 (Note 6)	This QN applies to both the reactor and the non-reactor sources.

Notes:

1) Similar to the ASME/ANS PRA standard, these criteria are based on a bounding or demonstrably conservative analysis.
2) The criteria in this table are nominally for plants with SCDF from all other hazards totaling ~10^{-5} / year or higher. If the SCDF from all other hazards total much less than 10^{-5}/year, then lower quantitative criteria should be considered.
3) With a cliff edge present, consider reducing the frequency of the screening criteria, such as by a factor of 10 (due to uncertainty in the hazard calculation and the absolute nature of the numeric criteria).
4) “Direct Containment Bypass or Failure” implies that the conditional large release probability is equal to or very close to 1.0, as a result of the hazard’s impact on the plant.

5) These criteria should not be used if potential design vulnerability is identified. The intent of the adjustments for potential design vulnerabilities is to address events whose magnitudes are less than the design basis hazard (i.e., the hazard frequency is greater) and the vulnerability may result in a CCDP that is significant, even though the event magnitude is reduced. If there is an identified design vulnerability, then only the two SCDF criteria (i.e., QN1 and QN3) are recommended for quantitative screening of the hazard.

6) IAEA NS-G-3.1[R-27] includes this criteria - In some States, a value for the probability of 10^{-7} per reactor-year is used in the design of new facilities as one acceptable limit on the probability value for interacting events having serious radiological consequences, and this is considered a conservative value for the SPL (Screening Probability Level) if applied to all events of the same type (such as all aircraft crashes, all explosions). Some initial events may have very low limits on their acceptable probability and should be considered in isolation.

Table 3: Summary of Criteria Applied for Screening for External Human-Induced Hazards

External Human-Induced Hazard	Screening Criterion
Small Aircraft Impact	[QN1]
Large Aircraft Impact	[QN5]
Rail Transportation – Cold Toxic Gas Release: Ammonia, Hydrogen Chloride, and Hydrogen Fluoride	[QL-3]
Rail Transportation – Cold Toxic Gas Release: Chlorine, Sulphuric Acid, and Sulphur Dioxide	[QN1]
Rail Transportation – Hot Toxic Gas Release	[QL-3]
Rail Transportation – Boiling Liquid Expanding Vapour Explosions (BLEVEs)	[QL-3]
Rail Transportation – Vapour Cloud Explosions	[QL-3]
Rail Transportation – Rail Line Blast	[QL-3]
Road Transportation – Cold Toxic Gas Release: Ammonia, Hydrogen Chloride, and Hydrogen Fluoride; Hot Toxic Gases, BLEVEs, Vapour Cloud Explosions (VCEs), and Explosions	[QL-3]
Road Transportation – Cold Toxic Gas Release: Chlorine, Sulphuric Acid, and Sulphur Dioxide	[QN5]
Ship Accidents – Small Vessels	[QL-6]
Ship Accidents – Large Vessels	[QL-3] and [QL-4]
Nearby Nuclear Event	[QL-5]
Fixed Sources – Toxic Gas Release: Ajax Water Treatment Plant	[QL-3]
Fixed Sources – Toxic Gas Release: Duffin's Creek Water Pollution Control Plant	[QN1]
Fixed Sources – BLEVEs	[QL-3]
External Fires – Including Forest Fire	[QL-3]
Thermal Radiation from Fire	[QL-3]
Orbital Debris	[QN3]

Table 4: Summary of Criteria Applied for Screening of Natural Hazards for Reactor Sources

External Natural Hazard	Screening Criterion
Earthquakes	Screened in
Slope Instability	No hazard
Subsidence	No hazard
Soil Frost	No hazard
Flooding Due to Runoff	[QN1]
Flooding Due to Rivers	[QL-6]
Flooding Due to Waves	[QL-6]
Flooding Due to Seiche	No hazard
Flooding Due to Tsunami	No hazard
Flooding Due to Sudden Releases of Water from Natural or Artificial Storage	No hazard
Flooding Due to Ice-Jamming	[QL-5]
Flooding Due to Other Causes	No hazard
Flooding Due to Combined Events	[QN1]
Extreme Low Temperature	Screened in
Extreme High Temperature	Screened in
Snowpack	[QL-5]
Freezing Rain	[QL-2]
Avalanches	No hazard
Hurricanes/Tornadoes	Screened in
Ice Storms	Screened in
Lightning	[QL-6]
Meteorites	[QN5]
Geomagnetic Storms	[QL-1]
Animals: Lake	Screened in
Animals: Land	[QL-3]
Animals: Airborne	[QL-6]

Table 5: Screening for External Human-Induced Hazards for Non-Reactor Sources - IFB

Human-Induced External Hazard	Screening
Small Aircraft Impact	Screened In
Large Aircraft Impact	Screened Out
Rail Transportation – Cold Toxic Gas Release: Chlorine, Sulphuric Acid and Sulphur Dioxide	Screened In
Rail Transportation – Cold Toxic Gas Release – Ammonia, Hydrogen Chloride and Hydrogen Fluoride, BLEVE Missile, VCE, and Rail Line Blast	Screened Out
Road Transportation – Cold / Hot Toxic Gas Release, BLEVE Missile, VCE, and Explosion	Screened Out
Ship Accident	Screened In
Nearby Nuclear Event	Screened Out
Fixed Sources – Toxic Gas Release	Screened Out
Fixed Sources – BLEVE Missile	Screened Out
External Fires – Including Forest Fire	Screened Out
Thermal Radiation from Fire	Screened Out
Orbital Debris	Screened Out

Table 6: Screening for Natural External Hazards for Non-Reactor Sources - IFB

External Natural Hazard	Screening Criterion
Earthquakes	Screened In
Flooding – Due to Run Off	Screened In
Flooding – Due to Combined Events	Screened In
Low Lake Levels	Screened Out
Meteorological Extremes – High and Low Temperature, Rainfall, Snow, Freezing Rain, Snowpack	Screened In
Meteorological – Hurricanes/Tornadoes, Ice Storms	Screened In
Mist	Screened In
White Frost	Screened In
Frazil Ice	Screened In
Geomagnetic Storm	Screened In
Bio-fouling	Screened In
Soil Failures (slope failure, subsidence, soil frost and erosion)	Screened Out
Combined Hazard Events	Screened In

Table 7: Screening of the Human Induced External Hazards for Non-Reactor Sources – UFDS

Human-Induced External Hazard	Screening
Large Aircraft Impact	Screened out
Small Aircraft Impact	Screened out
Rail Transportation (Cold/Hot Toxic Gas Release, BLEVE Missile, Vapour Cloud Explosion, Rail Line Blast)	Screened out
Road Transportation	Screened out
Ship Accident	Screened out
Stationary Sources of Hazards: • Nearby Nuclear Site Accident, Toxic Gas Release, BLEVE • Thermal Radiation (e.g., from BLEVE hazard with accompanying fireball, jet fire hazard from natural gas pipeline failure, fuel fire following an aircraft crash) • Other Stationary Non-Nuclear Hazards (e.g., Regional Water Treatment Plants)	Screened out
External Fires – including Forest Fire	Screened out
Orbital Debris Crashes	Screened out

Table 8: Screening of the Natural External Hazards for UFDS

External Natural Hazard	Screening Criterion
Earthquake	Screened Out
External Flooding: • Flooding due to Runoff • Flooding due to River • Flooding due to Waves • Flooding due to Tsunami • Flooding due to sudden release of water from natural or artificial storage • Flooding due to ice jamming, lake ice, seiche • Flooding due to underwater landslides • Flooding due to combination of events	Screened Out
Low Lake Levels	Screened Out
Extreme Temperatures	Screened Out
Snow/Snowpack	Screened Out
Freezing Rain	Screened Out
Mist White Frost	Screened Out
Soil Failures: • Slope Instability • Subsidence • Soil Frost • Erosion	Screened Out
Avalanches	Screened Out
Ice Storms	Screened Out
High Winds, Tornadoes, Hurricanes	Screened Out
Lightning	Screened Out
Meteorites	Screened Out
Geomagnetic Storm and Solar Flares	Screened Out
Biofouling	Screened Out
Animals	Screened Out

Table 9: Screening of the Internal Hazards for IFB

Internal Hazard		Screening Criterion
Loss of Heat Sink	Random IFB cooling system failures (e.g., pumps, flow path, valving, control logic, etc.);	Screened In
	Random IFB support systems failures (e.g., power, instrument air, water supply failure);	Screened In
	Human errors (e.g., due to maintenance and testing);	Screened In
	Internal IFB fires;	Screened In
	Internal IFB flooding;	Screened In
	Reactor hazards that may impact IFB cooling system equipment operation (e.g., main steam line breaks, turbine generator fire, etc.)	Screened In
Loss of IFB water Inventory		Screened In
Hydrogen Generation in the IFB Due to Radiolysis		Screened Out
Transfer Mechanism Room Accidents		Screened Out
Four Bundles in the Elevator Housing		Screened Out
Conveyor Unloader Accidents		Screened Out
Fuel Module Drop in the Auxiliary Irradiated Fuel Bay (AIFB)		Screened Out
DSC Loading Accidents at the Auxiliary Irradiated Fuel Bay (AIFB)		Screened Out
Fuel Module Drop in the Auxiliary Irradiated Fuel Bay During DSC Loading		Screened Out
Loaded DSC Drop in the Auxiliary Irradiated Fuel Bay Loading Area		Screened Out
Loaded Inter Bay Transfer Flasks (IBTFs) Drop in the Irradiated Fuel Bay		Screened Out

Table 10: Screening of the Internal Hazards for UFDS

External Natural Hazard	Screening Criterion
Turbine Missiles	Screened Out
HT Pump Missiles	Screened Out
Missiles from Valves and Pumps	Screened Out
Explosions in hazardous Materials Storage Building; includes Missiles from Acetylene Explosion	Screened Out
Release of Oxidizing, Toxic, Radioactive or Corrosive Gases and Liquids from On-Site Storage	Screened Out
Release of Stored Energy	Screened Out
Dropped or Impacting Loads, e.g.; Crane Failure, DSC collision during craning (loaded DSC colliding with another DSC, loaded or empty), Transporter collision with a loaded DSC or another transporter, Equipment collision with a loaded DSC during craning due to operator error	Screened Out
Vehicle Impacts – Onsite Vehicle Movement (Outdoor Within Protected Area)	Screened Out
Vehicle Impacts – Within Waste Management Facility	Screened Out
Toxic and/or Dangerous Good – Onsite Vehicle Movements (Cold Toxic Hazards)	Screened Out
Electromagnetic Interference	Screened Out
Static Electricity	Screened Out
Fires	Screened Out
Loss of Support Services to the UFDS (Electrical Power, Control Power, Instrument Air, HVAC, Service Air)	Screened Out
Mishandling of Fuel (e.g., newer than 10 years old fuel transfer to DSC)	Screened Out
Criticality	Screened Out

Table 11. PARA Fuel Damage Categories

FDC	Definition	Typical Events in FDC
FDC1	Rapid loss of core structural integrity.	Positive reactivity transient (from 0.3 to 2.0 mk/s) and failure to shutdown.
FDC2	Slow loss of core structural integrity.	LOCA with failure of ECIS and failure of moderator heat sink.

Table 12: Initiating Events in the PARA-L1P

Category	Label IE-44-	Description (PARA-L1P)
Forced Shutdown	FSD	All reactor shutdowns not included in other initiating events
LOCA	LOCA1	Small break within the capacity of two D_2O pressurizing pumps (initial discharge rate 1 - ~40 kg/s)
	LOCA2A	Small breaks which require ECIS for refilling and repressurization of the HTS (initial discharge rate ~40 - 100 kg/s)
	LOCA2B	Small breaks which require ECIS for refilling and repressurization of the HTS (initial discharge rate 100-1000 kg/s)
	LOCA3	Large breaks which require high and subsequently low pressure ECIS for refilling and do not result in flow stagnation into the core (initial discharge rate >1000 kg/s)
	LOCA4	Large breaks which require high and subsequently low pressure ECIS for refilling and lead to flow stagnation into the core (initial discharge rate >1000 kg/s)
	LOCA1-SF	Stagnation feeder break in LOCA1 range
	LOCA2-SF	Stagnation feeder break in LOCA2A range
Pressure Tube Rupture	PTL	Pressure tube failure resulting in an initial discharge rate of less than 1 kg/s
	PTF	Pressure tube failure resulting in an initial discharge rate in excess of 1 kg/s
End-fitting Failure	EFL2	End-fitting break of LOCA2-size outside annulus gas bellows in LOCA2 range (includes fuelling machine induced LOCAs)
Steam Generator Tube Rupture	SGTB1	Boiler tube break within the capacity of the D_2O feed system (initial discharge rate 1 - ~40 kg/s)
	SGTB2	Boiler tube break beyond the capacity of the D_2O feed system (initial discharge rate > ~40 kg/s)
Loss of HTS Pressure Control (Low)	LRVO	One or more liquid relief valves fail open spuriously
	LBVO	A liquid bleed valve opens spuriously
	2LBVO	Both liquid bleed valves open spuriously
	FVFC	Both D_2O feed valves fail closed
	FPFO	Failure of in-service D_2O pressurizing pump
	XSPR	Bleed condenser spray valve 3332-CV113 opens spuriously
Loss of HTS Pressure Control (High)	BVFC	Both HTS bleed valves fail closed
	FVFO	Any or both D_2O feed valves fail open
	FP2S	Inadvertent start-up of standby D_2O pressurizing pump
	BCLCVFC	Bleed condenser level control valves fail closed

Category	Label IE-44-	Description (PARA-L1P)
Loss of HTS Inventory Control	D2OFDL	Pipe break in D_2O feed system upstream of check valve 3331-NV1 or -NV2
HTS Pump Trip	HTPT	Any or up to four HTS pumps trip
Channel Flow Blockage	LFB	Channel flow reduced by 90 percent or more
	HTMV	Spurious closure of boiler isolating valve or HTS main pump discharge valve
Moderator Failure	LOMHS	Loss of moderator heat sink
	LOMF	Loss of moderator flow
	LOMI	Loss of moderator inventory
	DUMP	Spurious moderator dump
Loss of End Shield Cooling	LOESHS	Loss of end shield heat sink
	LOESF	Loss of end shield flow
	LOESI	Loss of end shield inventory
Steam Line Break	SRV	One or more atmospheric steam rejection valves open spuriously
	SSLB-IC	Small steam line break inside containment
	SSLB-OC	Small steam line break outside containment
	LSLB-IC	Large steam line break inside containment
	LSLB-OC	Large steam line break outside containment
	U1LSLB-OC	Unit 1 large steam line break outside containment
	IE-30-LSLB-OC [7]	Unit 5 large steam line break outside containment at Pickering NGS B.
	IE-30-U678LSLB-OC	Unit 6/7/8 large steam line break outside containment at Pickering NGS B
Loss of Feedwater to One or More Boilers	TLOFW	Total loss of feedwater to all quadrants
	PLOFW	Partial loss of feedwater to all quadrants
	ALOFW	Asymmetric loss of feedwater (no feedwater flow to boilers in one quadrant)
Feedwater Line Break	SFLB-IC	Small feedline break inside containment
	SFLB-OC	Small feedline break outside containment
	LFLB	Large feedline break resulting in total loss of feedwater
	FLBCOND	Break in condensate system resulting in total loss of condensate flow to deaerator
	FWLB-CL1ROOM	Feedwater line break above Class I room
	U1LFLB	Unit1 large feedwater line break

---

[7] Note that events IE-30-LSLB-OC and IE-30-U678-LSLB-OC do not have the IE-44- prefix, since they originate in Pickering B.

Category	Label IE-44-	Description (PARA-L1P)
Turbine Trip	TT	All turbine trips not included in other initiating events (includes loss of condenser vacuum events)
Loss of Condensate Flow	LOCONDA	Total loss of condensate flow to deaerator (excluding condensate pipe breaks)
	LOCONDB	Loss of main condensate flow to deaerator (excluding condensate pipe breaks)
Reheater Drains Line Break	RDLB	Breaks in reheater drains line between the boilers and the second check valve
Unplanned Increase in Reactivity	FLOR	Fast rate of reactivity insertion
	SLOR	Slow rate of reactivity insertion
	LZCPMPFL	All liquid zone control system pumps fail
	URIR	Unplanned regional increase in reactivity
	SORD	Spurious shutoff rod drop resulting in a regional increase in reactivity
Loss of Computer Control	WDTOX	Controlling computer stall
	DCCF	Dual computer failure
	DCCUF	Unsafe failure of digital control computer leading to reactor power increase
	BPCF	Failure 'off' of boiler pressure control program on both computers
	FHCF	Failure 'off' of fuel handling system control program on digital control computer DCC2
	RRSF	Failure 'off' of reactor power control program on both computers
Loss of LPSW System	LOLPSW	Total loss of LPSW
Forebay event	FOREBAY	Adverse conditions in the forebay
Loss of HPSW System	LOHPSW	Total loss of HPSW
Loss of RCW System	LORCW	Total loss of recirculated cooling water system flow
Loss of Instrument Air	TLOIA	Total loss of instrument air
Loss of Bulk Electricity Supply	LOBES	Loss of bulk electricity supply
Loss of Switchyard	LOSWYD	Loss of switchyard
Loss of Power to Unit Class IV 4.16 kV Bus	LOCL4	Total loss of unit Class IV power
	LOSST	Loss of system service transformer or circuit breakers 5320-CB1A or -CB1C causing loss of power supply to Class IV 4.16 kV buses 5320-BUA or -BUC, respectively
	LO5320BUA	Loss of power to unit Class IV 4.16 kV bus BUA

Category	Label IE-44-	Description (PARA-L1P)
	LO5320BUB	Loss of power to unit Class IV 4.16 kV bus BUB
	LO5320BUC	Loss of power to unit Class IV 4.16 kV bus BUC
	LO5320BUD	Loss of power to unit Class IV 4.16 kV bus BUD
Loss of Unit Class IV 600 V Bus	LO5330BUA	Loss of power to unit Class IV 600 V bus BUA
	LO5330BUB	Loss of power to unit Class IV 600 V bus BUB
	LO5330BUC	Loss of power to unit Class IV 600 V bus BUC
	LO5330BUD	Loss of power to unit Class IV 600 V bus BUD
Loss of Power to Unit Class III 4.16 kV Bus	LO5412BUA	Loss of power to unit Class III 4.16 kV bus BUA
	LO5412BUB	Loss of power to unit Class III 4.16 kV bus BUB
Loss of Power to Unit Class III 600 V Bus	LO5413BUA	Loss of power to unit Class III 600 V bus BUA
	LO5413BUB	Loss of power to unit Class III 600 V bus BUB
	LO5413BUC	Loss of power to unit Class III 600 V bus BUC
	LO5413BUD	Loss of power to unit Class III 600 V bus BUD
Loss of Power to Unit Class II 600 V Bus	LO5423BUA	Loss of power to unit Class II 600 V bus BUA
	LO5423BUB	Loss of power to unit Class II 600 V bus BUB
Loss of Power to Unit Class II 120 V Bus	LO5440BUA	Loss of power to unit Class II 120 V ac bus BUA
	LO5440BUB	Loss of power to unit Class II 120 V ac bus BUB
	LO5450BUA	Loss of power to unit Class II 120 V ac bus BUA
	LO5450BUB	Loss of power to unit Class II 120 V ac bus BUB
	LO5450BUC	Loss of power to unit Class II 120 V ac bus BUC
	LO5450BUD	Loss of power to unit Class II 120 V ac bus BUD
	LO5450BUE	Loss of power to unit Class II 120 V ac bus BUE
	LO5450BUF	Loss of power to unit Class II 120 V ac bus BUF
	LO5440BUB1	Loss of power to unit Class II 120 V ac bus BUB1
Loss of Power to Unit Class II 48 V Bus	LO5520BU1 to LO5520BU22	Loss of power to unit Class II 48 V dc bus BU1 to BU22
	LO5520BU31 to LO5520BU52	Loss of power to unit Class II 48 V dc bus BU31 to BU52
Loss of Unit Class I 250 V Power	LO5510BUA1	Loss of unit Class I 250 V dc bus 55100-BUA1
	LO5510BUB1	Loss of unit Class I 250 V dc bus 55100-BUB1
Heat Transport Flow Diversion	SDCMV	Spurious opening of both shutdown cooling isolation valves in one or more quadrants

Category	Label IE-44-	Description (PARA-L1P)
Powerhouse Freezing	PHFREEZE	Spurious opening of powerhouse venting during an extreme cold outside condition
ECI Blowback	3335MV156	33350-MV156 opens spuriously
	3335MV156TS	33350-MV156 on test
	3335MV157	33350-MV157 opens spuriously
	3335MV157TS	33350-MV157 on test
	3335NV158	33350-NV158 opens spuriously
	3335NV159	33350-NV159 opens spuriously
	3335NV33	33350-NV33 opens spuriously
	3335NV34	33350-NV34 opens spuriously
	3335NV358	33350-NV358 opens spuriously
	3335NV47	33350-NV47 opens spuriously
	3335NV48	33350-NV48 opens spuriously
	3341MV1	33410-MV1 open spuriously
	3341MV10	33410-MV10 open spuriously
	3341MV10TS	33410-MV10 on test
	3341MV11	33410-MV11 open spuriously
	3341MV11TS	33410-MV11 on test
	3341MV1TS	33410-MV1 on test
	3341MV2	33410-MV2 open spuriously
	3341MV2TS	33410-MV2 on test
	3341MV4	33410-MV4 open spuriously
	3341MV4TS	33410-MV4 on test
	3341MV5	33410-MV5 open spuriously
	3341MV5TS	33410-MV5 on test
	3341MV7	33410-MV7 open spuriously
	3341MV7TS	33410-MV7 on test
	3341MV8	33410-MV8 open spuriously
	3341MV8TS	33410-MV8 on test
	BM-CHDTEST	LOCA conditioning logic on Test E-5 (Channel D)
	BM-CHETEST	LOCA conditioning logic on Test E-5 (Channel E)
	BM-CHFTEST	LOCA conditioning logic on Test E-5 (Channel F)
	BM-CHSTEST	LOCA conditioning logic on Test E-5 (Channel S)

Category	Label IE-44-	Description (PARA-L1P)
ECI Blowback contd.	SPBM-CHD	Spurious signal from LOCA conditioning logic (Channel D)
	SPBM-CHE	Spurious signal from LOCA conditioning logic (Channel E)
	SPBM-CHF	Spurious signal from LOCA conditioning logic (Channel F)
	SPBM-CHS	Spurious signal from LOCA conditioning logic (Channel S)
	SPHTPL-CHD	Spurious signal from LOCA HTS pressure low logic (Channel D)
	SPHTPL-CHE	Spurious signal from LOCA HTS pressure low logic (Channel E)
	SPHTPL-CHF	Spurious signal from LOCA HTS pressure low logic (Channel F)
	SPHTPL-CHS	Spurious signal from LOCA HTS pressure low logic (Channel S)
	SPHTPVL-CHD	Spurious signal from LOCA HTS pressure low logic (Channel D)
	SPHTPVL-CHE	Spurious signal from LOCA HTS pressure low logic (Channel E)
	SPHTPVL-CHF	Spurious signal from LOCA HTS pressure low logic (Channel F)
	SPHTPVL-CHS	Spurious signal from LOCA HTS pressure low logic (Channel S)
	BLR-CHDTEST	LOCA high boiler room pressure logic on test E-2 or E-6 (Channel D)
	BLR-CHETEST	LOCA high boiler room pressure logic on test E-2 or E-6 (Channel E)
	BLR-CHFTEST	LOCA high boiler room pressure logic on test E-2 or E-6 (Channel F)
	BLR-CHSTEST	LOCA high boiler room pressure logic on test E-2 or E-6 (Channel S)
	HTPLVL-CHDTEST	LOCA HTS pressure low / very low logic on test E-1 or E-6 (Channel D)
	HTPLVL-CHETEST	LOCA HTS pressure low / very low logic on test E-1 or E-6 (Channel E)
	HTPLVL-CHFTEST	LOCA HTS pressure low / very low logic on test E-1 or E-6 (Channel F)
	HTPLVL-CHSTEST	LOCA HTS pressure low / very low logic on test E-1 or E-6 (Channel S)
	MOD-CHDTEST	LOCA high moderator inventory logic on test E-3 or E-7 (Channel D)
	MOD-CHETEST	LOCA high moderator inventory logic on test E-3 or E-7 (Channel E)
	MOD-CHFTEST	LOCA high moderator inventory logic on test E-3 or E-7 (Channel F)
	MOD-CHSTEST	LOCA high moderator inventory logic on test E-3 or E-7 (Channel S)

Table 13: List of Systems Modelled by Fault Trees in the Internal Events PSAs

System Name	Level 1 At-Power	Level 1 Outage	Level 2 At-Power
Heat Transport System Feed, Bleed, Relief and D_2O Storage and Transfer System	Y	Y	*
Heat Transport System D_2O Recovery System	Y	Y	*
Heat Transport Pump Gland Seal Supply and Gland Seal LOCA	Y	Y	*
Heat Transport Shutdown Cooling System	Y	Y	*
Moderator and ECI Recovery Systems	Y	Y	*
Boiler Feedwater System	Y	Y	*
Boiler Emergency Cooling System	Y	N	*
Steam Relief System	Y	Y	*
Class IV Power Supply System	Y	Y	*
Class III Power Supply System	Y	Y	*
Class II Power Supply System	Y	Y	*
Class I Power Supply System	Y	Y	*
Low Pressure Service Water System	Y	Y	*
Recirculated Cooling Water System	Y	Y	*
High Pressure Service Water System	Y	Y	*
Low Pressure Instrument Air System	Y	Y	*
High Pressure Instrument Air System	Y	Y	*
Emergency Coolant Injection System	Y	Y	*
Emergency Boiler Water Supply System	Y	Y	*
Standby Generator Fuel Oil System	Y	Y	*
Hostile Environment Events	Y	Y	*
Shutdown System A	Y	N	*

System Name	Level 1 At-Power	Level 1 Outage	Level 2 At-Power
Shutdown System E	Y	N	*
Annulus Gas System	Y	Y	*
Digital Control Computer	Y	Y	*
Cooling and Ventilation (Electrical Rooms, MCR, Control Equipment Room (CER))	Y	Y	*
Reactivity Control System	Y	N	*
Condensate System	Y	Y	*
Emergency Coolant Injection System Blowback	Y	Y	*
Shutdown Heat Sinks	N	Y	N/A
Pressure Relief Valves	N	N	Y
Containment Isolation, Airlocks and Hydrogen Ignition System	N	N	Y
Containment In-Leakage	N	N	Y
Boiler Room and Fuelling Machine Vault Air Cooling Units	N	Y	Y
Pressure Relief Panel System	N	N	Y
Hydrogen Igniters	N	N	Y
Emergency Mitigating Equipment (EME)	Y	Y	*

* Included in Level 2 At-Power Model through integration with Level 1 At-Power Model.

Table 14: PARA-L1O Plant Operational State Definition

Input Parameter	Plant Operational State (POS)		
	A	B	C
GSS Configuration	GSS	GSS	GSS
HTS Boundary	Closed	Closed	Closed
Primary HTS Inventory and Pressure	All Boilers Primary Side Full, HTS Depressurized	Some Boilers Primary Side Drained & Isolated, HTS Depressurized	All Boilers Primary Side Full, HTS Pressurized
Primary Heat Sink (HS)	HS5	HS5 (normally), HS8[Note 1]	HS 7/8
Decay heat load - notes	Start of Outage	Early into Outage	Well into Outage
Time After Shutdown at Start of POS (days, for decay heat load)	0.7	5.3	81.5
Relative Outage Time in This POS	28.5%	62.8%	8.7%
POS Time Fraction per Reactor-Year (based on actual planned and forced outages)	0.0627	0.1382	0.0190

Note 1: Heat sink HS8 would only be used as the primary heat sink later in the outage when decay heat is lower, in order to permit specific outage maintenance activities (e.g., use of HS8 as the primary heat sink during a HPSW outage).

Table 15: Initiating Events for PARA-L1O

IE-LABEL	DEFINITION	APPLICABLE POS		
		POS A	POS B	POS C
SDC-HX	Loss of SDCS heat removal	Y	Y	-
SDC-FLOW	Loss of SDCS flow	Y	Y	Y
BLDCLR	Loss of bleed cooling	-	-	Y
TLOFW	Total loss of feedwater	-	Y	Y
BLOWDOWN	Loss of boiler blowdown	-	Y	Y
LEAK1	Small non-isolatable leak inside containment from a depressurized HTS, within the capacity of the D2O make-up function	Y	Y	-
LLEAK	Non-isolatable breaks inside containment from a depressurized HTS, beyond the capacity of the D2O makeup function	Y	Y	-
LOCA1	Non-isolatable rupture of pressurized HTS beyond the capacity of D_2O make-up	-	-	Y
LLOCA	Non-isolatable rupture of pressurized HTS beyond the capacity of D_2O make-up	-	-	Y
LEAK-SDC	Rupture of SDCS piping	Y	Y	Y
SDCHXTB	Break of SDCS HX tube	Y	Y	Y
PTF	Pressure tube failure	-	-	Y
PTL	Pressure tube leak	Y	Y	Y
SGTB	Boiler tube leak	-	-	Y
BLOWBACK	Blowback of HT system D_2O at high pressure outside containment through ECIS piping	-	-	Y
U1LSLB-OC	U1 large steamline break outside containment	Y	Y	Y
U5678-LSLB-OC	Large steamline break at Pickering NGS B unit	Y	Y	Y
U1LFLB	U1 large feedline break	Y	Y	Y
PHFREEZE	Spurious opening of powerhouse venting during extreme cold weather	Y	Y	Y
U15678-BREAK-IC	High energy line break inside containment originating from at-power unit	Y	Y	Y

IE-LABEL	DEFINITION	APPLICABLE POS		
		POS A	POS B	POS C
LOPIC-HIGH	Loss of HTS pressure & inventory control leading to high HTS pressure	-	-	Y
LOPIC-LOW	Loss of HTS pressure & inventory control leading to low HTS pressure	-	-	Y
SDC-INV	Loss of HTS inventory (without rupture) leads to failure of forced circulation using SDCS pumps	Y	Y	Y
LOBES	Loss of bulk electricity supply	Y	Y	Y
LOSWYD	Loss of switchyard	Y	Y	Y
LOSST	Loss of System Service Transformers or circuit breakers 5320-CB1A or -CB1C causing loss of power supply to Class IV 4.16 kV buses 5320-BUA or -BUC, respectively	Y	Y	Y
LOCL4	Total loss of Class IV power	Y	Y	Y
LOCL4BU	Loss of one or several Class IV busses	Y	Y	Y
LOCL3BU	Loss of one or several Class III busses	Y	Y	Y
LOCL2BU	Loss of one or several Class II busses	Y	Y	Y
LOCL1BU	Loss of one or several Class I busses	Y	Y	Y
LOLPSW	Total loss of LPSW	Y	Y	Y
FOREBAY	Adverse conditions in the forebay affecting station service water supply	Y	Y	Y
LOHPSW	Total loss of HPSW	Y	Y	Y
LORCW	Total loss of recirculated cooling water system flow	Y	Y	Y
TLOIA	Total loss of instrument air	Y	Y	Y

Table 16. Summary of Fuel Damage Categories for Outage PSA

FDC	Definition	Typical Shutdown Events in FDC
FDC1 – SD	Rapid loss of core structural integrity.	Positive reactivity transient during shutdown and failure to terminate the event.
FDC2 - SD	Slow loss of core structural integrity.	LOCA and failure of HTS make-up and failure of the moderator heat sink. Total and unrecovered loss of heat sinks.

Table 17: Seismic Hazard Bins

BIN	Bin Seismic Range (g)	Bin Average Acceleration (g)	Seismic Bin Frequency
1	0.01 – 0.05	0.02	3.4E-03
2	0.05 – 0.10	0.07	3.3E-04
3	0.10 – 0.20	0.14	1.4E-04
4	0.20 – 0.30	0.24	3.9E-05
5	0.30 – 0.50	0.39	2.7E-05
6	0.50 – 0.70	0.59	9.4E-06
7	0.70 – 1.00	0.84	5.9E-06
8	1.00 – 2.00	1.41	5.0E-06
9	> 2.00	2.00	1.6E-06

Table 18: PARA-L2P Plant Damage States

PDS	Representative Accident Sequence
PDS1	No representative sequence is defined.
PDS2A	Out-of-core LOCA, with loss of moderator cooling and Emergency Coolant Injection (ECI) and recovery.
PDS2B	Out-of-core LOCA with failure of moderator cooling and, ECI and recovery, and FADS.
PDS2C	Out-of-core LOCA, with loss of moderator cooling and ECI and recovery, combined with air cooling units (ACUs) unavailable in the accident unit.
PDS2D	Out-of-core LOCA, with loss of moderator cooling and ECI and recovery, combined with unavailability of ACUs in the accident unit, igniters.
PDS2E	Out-of-core LOCA, with loss of moderator cooling and ECI and recovery, combined with unavailability of containment pressure relief valves (PRV).
PDS2F	Out-of-core LOCA, with loss of moderator cooling and ECI and recovery, combined with unavailability of containment PRVs and unavailability of ACUs in the accident unit.
PDS2G	Out-of-core LOCA, with loss of moderator cooling and ECI and recovery, combined with a containment envelope impairment (CEI).
PDS2H	Out-of-core LOCA, with loss of moderator cooling and ECI and recovery, combined with a CEI and unavailability of ACUs in the accident unit.
PDS3-2U	Secondary side line break with PEVS success and no P&IC LOCA, but with failure of EBWS, hard-piped firewater, and EME in Unit 1 and Unit 4.
PDS3-6U	Secondary side line break with PEVS failure and loss of heat sinks at all six Pickering units.
PDS4	No representative sequence required.

Table 19: Pickering NGS A Release Categorization Scheme

Release Category #	Description
PA-RC1	Very large release with potential for acute offsite radiation effects and/or widespread contamination: > ~3% core inventory of I-131 occurring mainly within 24 hours
PA-RC2	Early release in excess of “Large Release” definition: Mixture of fission products containing > 10^{14} Bq of Cs-137 but <~3% core inventory of I-131 occurring mainly within 24 hours
PA-RC3	Late release in excess of “Large Release” definition: Mixture of fission products containing > 10^{14} Bq of Cs-137 but < ~3% core inventory of I-131 occurring mainly after 24 hours
PA-RC4	Early release in excess of “Small Release” definition: Mixture of fission products containing > 10^{15} Bq of I-131 but < 10^{14} Bq of Cs-137 occurring mainly within 24 hours
PA-RC5	Late release in excess of “Small Release” definition: Mixture of fission products containing >10^{15} Bq of I-131 but < 10^{14} Bq of Cs-137 occurring mainly after 24 hours

Notes:

‘PA’ is the plant identifier for PNGS-A.

‘NRC’ or no release category is used to define a fission product release that is less than the defined small release.

Table 20: Summary of PARA Severe Core Damage and Large Release Frequency Results for Internal Events

Model	Severe Core Damage Frequency (occurrences per reactor year)	Large Release Frequency (occurrences per reactor year)
Internal Events At-Power	8.3E-06	2.7E-06
Internal Events Outage	3.1E-06	8.7E-07
OPG Safety Goal	1.0E-04	1.0E-05

Table 21: Frequencies of PARA-L1P Fuel Damage Categories

Fuel Damage Category	Frequency (per reactor-year)
FDC1	2.6E-07
FDC2	8.0E-06
Severe Core Damage (FDC1 + FDC2)	8.3E-06

Table 22: Plant Damage State Frequency Results

Plant Damage State	Predicted Frequency (/year)
PDS1	2.6E-07
PDS2	5.8E-06
PDS3-2U	2.5E-07
PDS3-6U	2.1E-06
PDS4	1.5E-07

Table 23: PARA-L2P Release Category Frequency

Release Category	Frequency (per reactor-year)
RC1	2.7E-06
RC2	2.6E-08
RC3*	0
RC4*	0
RC5*	0

* The RC results with a zero value occur because only CET sequences with zero probability go to those end states regardless of the truncation level.

Table 24: Summary of PARA Severe Core Damage and Large Release Frequency Results for Fire, Seismic, Flooding and High Wind Events

Model	Severe Core Damage Frequency (occurrences per reactor year)	Large Release Frequency (occurrences per reactor year)
Internal Fire At-Power	4.7E-06	9.3E-07
Internal Flooding At-Power	2.0E-06	9.2E-07
Seismic At-Power	1.2E-06[1]	1.2E-06[1&2]
High-Wind At-Power	2.3E-05[1]	9.0E-06[1]
OPG Safety Goal	1.0E-04	1.0E-05

[1] The risk was estimated for seismic events / high winds with a return period up to and including 10,000 years.

[2] The Seismically-Induced Containment Failure Frequency (SCFF) is estimated to be 4.6E-08/year; however, a Level 2 model has not been developed and, therefore, the LRF is reported as equivalent to SCDF.

Table 25: Summary of PARA LRF for Non-Reactor Sources Events

Hazard[1]	LRF (occurrences per year)
Internal events	1.4E-07
Seismic events	9.7E-09

[1] The results listed in the table above are due to hazards directly affecting the IFB. The hazards associated with the UFDS facility have been screened out.

Appendix A Abbreviations and Acronyms

Acronym	Definition
ACU	Air Cooling Unit
AIFB	Auxiliary Irradiated Fuel Bay
AIM	Abnormal Incidents Manual
APC	Atmospheric Pressure Change
APS	Auxiliary Power System
BECS	Boiler Emergency Cooling System
BLEVE	Boiling Liquid Expanding Vapour Explosion
Bq	Bequerels
CAFTA	Computer Aided Fault Tree Analysis System
CANDU	CANadian Deuterium Uranium
CCDP	Conditional Core Damage Probability
CDFM	Conservative Deterministic Failure Margin
CER	Control Equipment Room
CET	Containment Event Tree
CNSC	Canadian Nuclear Safety Commission
Cs-137	Cesium-137
CSIM	Core Structural Integrity Maintained
CTU	Combustion Turbine Unit
D_2O	Deuterium Oxide (Heavy Water)
DBE	Design Basis Earthquake
DCC	Digital Control Computer
DSC	Dry Storage Container
EBWS	Emergency Boiler Water Supply System
ECIS	Emergency Coolant Injection System
ECVF	Early Calandria Vessel Failure
EME	Emergency Mitigating Equipment
ERO	Emergency Response Organization
ET	Event Tree
FADS	Filtered Air Discharge System
FAI	Fukushima Action Items
FDC	Fuel Damage Category
FHA	Fire Hazard Assessment
FIF	Fire Ignition Frequency
FSSA	Fire Safe Shutdown Assessment
FT	Fault Tree
FTREX	Fault Tree Reliability Evaluation eXpert

Acronym	Definition
GSS	Guaranteed Shutdown State
HCLPF	High Confidence of Low Probability of Failure.
HEP	Human Error Probability
HGL	Hot Gas Layer
HPECI	High Pressure Emergency Coolant Injection
HPSW	High Pressure Service Water
HRA	Human Reliability Analysis
HS	Heat Sink
HTS	Heat Transport System
HWEL	High Wind Equipment List
HX	Heat Exchanger
Hz	Hertz (1 Hz = 1 cycle per second)
I-131	Iodine-131
IBTF	Inter Bay Transfer Flasks
IE	Initiating Event
IFB	Irradiated Fuel Bay
IGN	Hydrogen Igniters
IST	Industry Standard Toolset
ISTB	Inter-Station Transfer Bus
kg/s	Kilograms per second
km/hr	Kilometres per hour
kV	Kilo-Volts
LCEI	Large Containment Envelope Impairment
LOBES	Loss of Bulk Electrical Supply
LOCA	Loss-of-Coolant Accident
LPSW	Low Pressure Service Water
LRF	Large Release Frequency
LRV	Liquid Relief Valve
m	Metres
m^2	Metres squared
MAAP	Modular Accident Analysis Program
MCA	Multi-Compartment Analysis
MCR	Main Control Room
MPa	Mega Pascals (10^6 Pascals)
MPa(g)	Mega Pascals gauge
MWe	Megawatt electrical
NGS	Nuclear Generating Station
NPCS	Negative Pressure Containment System
NRC	U.S. Nuclear Regulatory Commission

Acronym	**Definition**
NSQ	Non-Seismically Qualified
occ/yr	Occurrences per year
OPEX	Operating Experience
OPG	Ontario Power Generation
OSR	Operational Safety Requirement
PARA	Pickering NGS A Probabilistic Safety Assessment
PARA-Fire	Pickering NGS A At-Power Internal Fire PSA
PARA-Flood	Pickering NGS A At-Power Internal Flooding PSA
PARA-L1O	Pickering NGS A Level 1 Outage PSA for Internal Events
PARA-L1P	Pickering NGS A Level 1 At-Power PSA for Internal Events
PARA-L2P	Pickering NGS A Level 2 At-Power PSA for Internal Events
PARA-Seismic	Pickering NGS A At-Power PSA-Based Seismic Margin Assessment
PARA-Wind	Pickering NGS A At-Power High Wind PSA
PAU	Physical Analysis Unit
PDS	Plant Damage State
PEVS	Powerhouse Emergency Venting System
PNGS	Pickering Nuclear Generation Station
POS	Plant Operational State
PRD	Pressure Relief Duct
PRV	Pressure Relief Valve
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor
PWMF	Pickering Waste Management Facility
RC	Release Category
RCW	Recirculating Cooling Water
RE	Reference Earthquake
RLC	Review Level Condition
RLE	Review Level Earthquake
RRS	Reactor Regulating System
SCDF	Severe Core Damage Frequency
SCEI	Small Containment Envelope Impairment
SCFF	Seismically-Induced Containment Failure Frequency
SDCS	Shutdown Cooling System
SDS	Shutdown System
SDSE	Shutdown System Enhancement
SEL	Seismic Equipment List
SES	Site Electrical System
SEWS	Screening Evaluation Worksheets
SG	Standby Generator

Acronym	Definition
SMA	Seismic Margin Assessment
SQ	Seismically Qualified
SRF	Small Release Frequency
SRV	Steam Reject Valve
SSC	Systems Structures and Components
TG	Turbine Generator
TGO	Turbine Generator Oil
THERP	Technique for Human Error Rate Prediction
UHRS	Uniform Hazard Response Spectrum
VCE	Vapour Cloud Explosion