ONTARIOPOWER GENERATION

Report

OPG Proprietary	
Document Number: NA44-REP-03611-00036	Usage Classification: N/A
Sheet Number: N/A	Revision: R001

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-R001

2018-09-28

OPG Proprietary

Prepared by: A. Sartipi 28 Sep, 2018
A. Sartipi — Date
Senior Technical Engineer
Nuclear Safety and Technology Department
Ontario Power Generation

Recommended by: A. Moisin 28 Sept 2018
A. Moisin — Date
Section Manager, Projects
Nuclear Safety and Technology Department
Ontario Power Generation

Reviewed by: Noemie Duvivier 28 SEP 2018
N. Duvivier — Date
Technical Engineer Officer
Nuclear Safety and Technology Department
Ontario Power Generation

Concurred by: 02OCT2018
S. Bedrossian — Date
Acting Manager
Nuclear Safety and Technology Department
Ontario Power Generation

Accepted by: 05 OCT 2018
H. Seid — Date
Acting Manager
Pickering Reactor Safety Department
Ontario Power Generation

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.

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 meet the intent of the Canadian Nuclear Safety Commission Regulatory (CNSC) Standard S-294 [1].

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. 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 was prepared following methodologies consistent with best industry practice. The OPG PSA Methodologies have been accepted by the CNSC under Regulatory Standard S-294.

The baseline PNGS-A safety assessments are documented in several reports:

- A hazard screening assessment identifies the hazards that require assessment in a PSA model. The assessment was performed based on an updated methodology which is consistent with the latest international guidelines and industry good practices.

- The Level-1 and Level-2 internal events at-power PSA assesses 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 and Beyond Design Basis Accidents including Severe Accidents while the reactor is at full power.

- The Level-1 internal events outage PSA assesses the risk of severe core damage from internal events occurring while the reactor is in the guaranteed shutdown state; 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.

- The internal fire PSA assesses the risk of severe core damage and large release from internal fires occurring while the reactor is at full power. The fire PSA development involved a number of significant enhancements, such as cable tracing and detailed fire modelling, which permitted to better characterize and demonstrate lower plant risk.

- The internal flooding PSA assesses the risk of severe core damage and large release from internal floods occurring while the reactor is at full power.

- The high wind PSA assesses the risk of severe core damage and large release from high winds occurring while the reactor is at full power.

The 2018 PNGS-A PSA update elements listed above incorporate plant design and operation improvements resulting from Fukushima Action Items (FAI), such as, implementation of Emergency Mitigating Equipment (EME) and a number of PSA modelling enhancements. The PNGS-A PSAs represent the most up-to-date risk estimates.

The PNGS-A PSA has demonstrated that for each hazard the safety goal is met for severe core damage frequency and large release frequency.

The scope of PNGS-A PSA was limited to assessing the impact of hazards affecting the reactors. Accidents affecting other sources of radioactivity such as the Irradiated Fuel Bay were outside of the scope of the PNGS-A PSA.

The PNGS-A PSA was prepared following a quality assurance plan consistent with Canadian Standards Association standard CSA N286.05, *Management System Requirements for Nuclear Power Plants* [2]. The PSA was prepared using computer programs consistent with Canadian Standards Association standard CSA N286.7-99 *Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants* [3]. The PNGS-A PSA was prepared following methodologies consistent with the current state of practice. All methodologies used in the preparation of the PNGS-A PSA were accepted by the CNSC.

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. OPG prepares PSAs for each of its nuclear generating stations to meet the intent of the Canadian Nuclear Safety Commission (CNSC) Regulatory Standard S-294 [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. 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 Regulatory Standard S-294. 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 S-294. 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 PARA was prepared following a quality assurance plan consistent with Canadian Standards Association standard CSA N286.05 Management System Requirements for Nuclear Power Plants [2]. The PSA was prepared using computer programs that were consistent with Canadian Standards Association standard CSA N286.7-99 Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants [3].

OPG has safety goals for severe core damage frequency (SCDF) and large release frequency (LRF) [4], 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 is low in comparison to risks to which the public is normally exposed. The safety goal represents the tolerability of risk exposure above which action shall be taken to reduce risk. The administrative safety goal represents the desired objective towards which the facility should strive.

This report summarizes the probabilistic safety assessments of PNGS-A and compares the results with OPG’s Safety Goals [4].

The baseline PARA studies show that the overall risk from the operation of PNGS-A is acceptable.

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, and

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.

1.2 Scope

The baseline PNGS-A PSAs and hazard screening are documented in separate reports listed below:

1. A hazard screening assessment for internal and external events, which identifies the hazards that require further analysis in a PSA.

2. A Level 1 at-power PSA for internal events. This PSA studies the risk of fuel damage resulting from events occurring within the station (i.e., loss of coolant accidents, steam line breaks) while the reactor is at full power; it considers the challenges to reactor core cooling from accident sequences covering Design Basis Accidents and Beyond Design Basis Accidents including Severe Accidents while the reactor is at full power. This report is commonly referred to as PARA-L1P.

3. A Level 2 at-power PSA for internal events. This PSA studies the frequency and composition of radioactive materials releases to the environment resulting from events occurring within the station (e.g., loss of coolant accidents, steam line breaks) while the reactor is at full power. This PSA is the extension of the Level-1 PSA (i.e., PARA-L1P) and is commonly referred to as PARA-L2P.

4. A Level 1 outage PSA for internal events. This PSA studies the risk of severe core damage due to failure to remove decay heat following internal events occurring at the station while the reactor is in the Guaranteed Shutdown State (GSS). This report is commonly referred to as PARA-L1O.

5. A limited assessment of the risk of a large release resulting from events occurring within the station while the reactor is in the GSS.

6. A PSA-Based Seismic Margin Assessment. This PSA studies the risk of severe core damage and large release from seismic events (i.e., earthquakes) while the reactor is at full power. This report is commonly referred to as PARA-SEISMIC.

7. A PSA for internal fires. This PSA studies the risk of severe core damage and large releases from fires originating in the station (e.g., fires caused by failures in station electrical equipment) while the reactor is at full power. This report is commonly referred to as PARA-FIRE.

8. A PSA for internal floods. This PSA studies the risk of severe core damage resulting from floods originating within the station while the reactor is at full power. This report is commonly referred to as PARA-FLOOD.

9. A limited assessment of the risk of a large airborne release of radioactive material to the environment resulting from floods originating within the station while the reactor is at full power.

10. A PSA for high winds. This PSA studies the risk of severe core damage and a large release resulting from high winds while the reactor is operating at full power. This report is commonly referred to as PARA-WIND.

11. Bounding assessments of the likelihood severe core damage and a large airborne release of radioactive material to the environment resulting from:

    - seismic events;
    - internal fires;
    - internal floods; and
    - high winds

    while the reactor is in the GSS.

The PARA reports do not cover the following potential sources of risk:

- Fuelling machine accidents while the fuelling machine is in transit between the reactor face and the Units 2 and 3 Irradiated Fuel Bay (IFB). Analysis demonstrated that fuelling machine accidents while in transit cannot result in a large airborne release of radioactive material to the environment;
- Hazards from chemical materials used and stored at the plant;
- Other external initiating events such as external floods, airplane crashes, train derailment, etc.; and
- Other internal initiating events such as turbine missiles.

These types of hazards were addressed separately through screening studies or deterministic hazard studies.

The PNGS-A PSA was limited to hazards affecting the reactors. Accidents affecting other sources of radioactivity such as the IFB were outside of the scope of the PNGS-A PSA.

The response of the two PNGS-A units to various initiating events 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.

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 method 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 nuclear reactors, four turbine generators 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 is shown in Figure 1.

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 associated Pressure Relief Duct (PRD) and Pressure Relief Valves (PRV);

(e) A service wing;

(f) An administration building;

(g) An auxiliary irradiated fuel bay;

(h) A heavy water upgrading building;

(i) A screenhouse;

(j) A water treatment building;

(k) Six standby generator enclosures;

(l) An auxiliary power supply building;

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

(n) An HPECI water storage tank;

(o) Two buildings housing unitized instrument rooms for Shutdown System Enhancement (SDSE); and

(p) An Emergency Mitigating Equipment (EME) building and outdoor portable generator area.

The administration and service buildings, the heavy water upgrading building, the vacuum building, the HPECI structures, the EME building and the auxiliary power supply 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.

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.

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.

2.3 Reactor

The reactor consists of a horizontal cylindrical structure, the calandria, filled with heavy water. The calandria is penetrated by 390 horizontal fuel channel assemblies, and reactivity monitroing and control units. Below the calandria is a large cylindrical tank, the dump tank, connected to the calandria by four goose neck pipes. These pipes provide for rapid draining of the heavy water from the calandria to the dump tank.

The calandria and dump tank are housed in an air-filled, concrete vault, the calandria vault. The ends of the calandria assembly, the end shields, are located in the walls of the calandria vault and form part of the calandria vault enclosure. The end shields and shield plugs in the fuel channels provide sufficient shielding against radiation to allow personnel to access the fuelling machine vault when the reactor is shutdown.

An arrangement of embedded pipes carrying natural water provides cooling for the calandria 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, sheathed and sealed in Zircaloy-4 tubes. Twenty-eight tubes are assembled between two end plates to form one fuel bundle. Each of the reactor's 390 fuel channels contains 12 fuel bundles.

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.

Irradiated fuel is transferred from the fuelling machines to the IFB. The irradiated fuel remains in the IFB, or an auxiliary IFB, until it can be transferred to dry storage containers in the Pickering Waste Management Facility.

2.5 Reactivity Control Mechanisms and Systems

In-core neutron flux detectors and ion chambers are used to measure neutron flux in specific areas of the reactor. Signals from these detectors are supplied to the Reactor Regulating System (RRS) and the Shutdown System (SDS).

Fast shutdown of the reactor following a plant upset is accomplished by the SDS. The SDS releases 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 absoption, thereby controlling local neutron flux. Varying the water level in all of the tubes provides control of overall reactor power.

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 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 loss of coolant accident 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. 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 to remove this heat.

After an accident, the calandria sprays can be used as an additional heat sink to remove decay heat from the reactor.

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 turbine generator 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

Overpressure protection of the main steam system is provided by 16 safety valves, four on each steam main. The safety valves have staggered setpoints between 5.38 and 5.54 MPa(g).

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 is used to mitigate harsh environments caused by high temperature or high humidity in the powerhouse due to steamline 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) Shutdown System (SDS);

(b) Emergency Coolant Injection System (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 SDSA or SDSE exceeds it setpoint. SDSA and SDSE each have channelized 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.

  Each reactor has 23 shutoff rods normally suspended above the reactor. When a trip signal is received, an 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.

2.14.2 Emergency Coolant Injection System

The ECIS provides cooling water to the HTS following a loss of coolant accident. 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.

2.15.1 Electrical Power Systems

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

1. Class IV power is the normal alternating current supply to service unit loads;

2. Class III power is the alternating current supply for safety related equipment and auxiliaries;

3. Class II power is primarily used to supply 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. 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. 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 (APS). This system is comprised of two 100% redundant combustion turbine units that can supply Class 4 power to the station through the Site Electrical System. 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) High and Low Pressure Service Water System.

The service water system provides cooling water from Lake Ontario for various loads. 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 high pressure service water. The low pressure service water pumps, powered from the Class IV electrical system, draw water from the intake channel. The high pressure service water pumps, also powered from the Class IV electrical system, draw water from the discharge of the low pressure service water 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 (RCWS).

The RCWS provides clean, demineralized cooling water to equipment that might become contaminated or plugged if supplied by lake water. The RCWS recirculates water via a set of pumps and cools the water via a set of heat exchangers. The low pressure service water system is used on the secondary side of the RCWS heat exchangers for cooling purposes.

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 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 Powerhouse Heating 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

In response to the accident at the Fukushima Daiichi Nucler Power Plant, the CNSC prepared an action plan [5]. The Integrated Action Plan applied to all nuclear facilities and addressed:

- Strengthening defence in depth;
- Enhancing emergency response;
- Improving the regulatory framework;
- Enhancing international collaboration; and
- Communications and public consultation.

The actions related to nuclear power plants were summarized in Annex A of the CNSC's Integrated Action Plan [5]. As a result, the EME was incorporated into all updated PNGS-A PSAs.

The EME is stored in a light frame structure located north of the Brock Road security building. The EME building is not seismically robust; however, collapse of the building is not expected to damage the EME. The EME building is not robust with respect to wind damage; however, the EME itself will be tied down to prevent wind induced toppling or sliding. Provision has been made to clear the damaged structure following an earthquake or wind storm, and allow access to the EME.

Following an Initiating Event (IE), the EME is deployed to pre-determined locations in the plant and connected to the designated tie-in points. Deployment of the EME is initiated by the Shift Manager in the Main Control Room and follows pre-approved procedures. EME deployment is routinely drilled.

Provision has been made to clear debris from the path between the EME building and the plant following an external event.

The EME is comprised of:

- Two portable uninteruptable power supplies per unit to provide short-term power to the instrumentation necessary to monitor key plant parameters.
- One portable diesel generator per unit to provide long-term power to the instrumentation necessary to monitor key plant parameters.
- One portable self powered diesel driven pump for each unit that can be deployed either in the Reactor Auxiliary Bay or the Turbine Auxiliary Bay. The pump draws lake water through hose routed from the suction channel of the Condenser Cooling Water pumps and provide make-up water to refill the calandria and HTS via Emergency Cooling Injection flowpath. Additional portable pump can be deployed in the Reactor Auxillary Bay to provide make-up water to the boilers at Unit 1 and Unit 4 via Emergency Boiler Water Supply.

3.0 OVERVIEW OF PSA METHODS

Risk is defined as the product of the frequency of a hazardous event and the consequences of the event. Risk is expressed in units of consequence per unit time.

Risk = Frequency x Consequences

Risk provides a means of quantifying the degree of safety associated with a potentially hazardous activity and provides a common basis for comparing the relative safety of different activities. One of the principles of risk assessment is that the larger the numerical value of risk for a particular event, the more important the event is to safety. Thus, measures taken to reduce risk improve the level of safety.

OPG uses PSA to quantify the risk associated with accidents at its nuclear generating stations. For a nuclear generating station, the events studied are those leading to fuel damage in the reactor core or airborne releases of radioisotopes into the environment.

Consistent with the requirements of S-294, OPG has completed hazard screening, Level 1 and Level 2 PSA to assess the risk from PNGS-A:

- A hazard screening assessment was performed to confirm which hazards can be screened out from a probabilistic safety assessment, and identify which hazards need to be assessed by a PSA;
- A Level 1 PSA to assess the frequency of varying degrees of fuel failures, which lead to release of radioactive material from the fuel into containment; and
- A Level 2 PSA to assess the frequency and magnitude of airborne releases of radioactive material from containment to the environment.

OPG has defined two risk parameters based upon the PSA approach: Severe Core Damage Frequency (SCDF) and Large Release Frequency (LRF). These parameters are estimated in the Level 1 PSA and the Level 2 PSA, respectively.

OPG has defined safety goals for both SCDF and LRF, these are shown in Table 1. The intent of these goals is to ensure that the radiological risks arising from nuclear accidents at OPG's nuclear power reactors is low in comparison to risks to which the public is normally exposed.

For PNGS-A, detailed Level 1 PSAs were prepared for:

- Internal events while both reactors are at full power;
- Internal events while one reactor is in the GSS;
- Seismic events while both reactors are at full power;
- Internal fires while both reactors are at full power;
- Internal floods while both reactors are at full power; and

- High winds while both reactors are at full power.

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

For PNGS-A, a detailed Level 2 PSA was prepared for internal events while both reactors are at full power. This study also analyzed events involving both PNGS-A and PNGS-B. The methodology for the detailed Level 2 PSA is summarised in Section 6.0 of this report.

Limited scope Level 2 PSAs were prepared for internal events while one reactor is in the GSS, and internal fires, internal floods, seismic events and high winds while both reactors are at full power. The methodologies for these limited assessments are summarised in Sections 6.2 to 6.6 of this report.

For PNGS-A, bounding assessments were prepared for seismic events, internal fires, internal floods and high winds while one reactor is in the GSS. The rationale for these bounding assessments is described below.

3.1 Bounding Assessments for Shutdown Units

OPG did not prepare Level 1 and Level 2 PSAs for internal floods, internal fires, seismic events and high winds while one PNGS-A unit was shutdown. The rationale for this approach is based upon five high level premises:

1. The level of detail in a PSA should reflect the level of risk.
2. The risk from each of these hazards while a unit is shutdown is low and bounded by the risk from the equivalent hazard for a high power unit. The key factors supporting this assertion are that:
    - An event and failure to remain shutdown is not a significant contributor to risk. This results from the provision of two reliable lines of defence to prevent criticality: the shutdown guarantee and the shutdown system.
    - Given the above, the risk from these hazards is dominated by sequences involving the failure of all heat sinks.
    - Initial reactor power is *at least* two orders of magnitude less for a shutdown unit than for a high power unit. Therefore, fuel temperatures will be lower, accident progression will be slower, and the amount of energy deposited into containment will be lower for a shutdown unit.
    - Analysis demonstrated that:
        - For single unit sequences, only those sequences in which Early Calandria Vessel Failure (ECVF) occurs progress from severe core damage to a large release. Only 13% of the sequences that progress to severe core damage will progress to a large release as a result of ECVF.

    - Single and two-unit sequences only progress to a large release if the transient is initiated in the earliest part of an outage.

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

3. Accident progression for a shutdown unit is well understood from the analysis prepared in support of the limited Level 2 PSA for internal events while the reactor is in the GSS. Therefore, additional analysis of accident progression is not warranted.
4. On average, a PNGS-A unit is shutdown for a planned outage for approximately 20% of the operating cycle. Therefore, the exposure to these low frequency hazards is much lower for a shutdown unit than for a high power unit.
5. Risk management programs at the station are adequate to control the risk from these hazards while a unit is shutdown.

4.0 HAZARD SCREENING METHODS

A hazard is an event or natural phenomenon that has the potential to pose some risk to the facility. 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 aircraft crashes. 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.

4.1 External Hazard Screening

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 crash, etc.).

4.1.1 Overview of External Hazards Screening Method

The external hazards screening method involves three main steps [6]:

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 likelihood of event occurring. Screen-out events quantitatively based on the likelihood of event occurring, severe core damage frequency or conditional core damage probability.

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 purpose a screening distance value (SDV) is defined by the OPG Hazard Screening Guide [6], 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.

[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.

The quantitative screening steps QN1 to QN5 discussed below, and shown in Table 2 are the criteria for quantitative screening.

[QN1] The SCDF is less than 1.0E-06/yr. with no direct containment bypass/failure.

[QN2] Design basis hazard frequency is less than 1.0E-05/yr. and the conditional core damage probability (CCDP) is less than1.0E-01, with no direct containment bypass/failure.

[QN3] The SCDF is less than 1.0E-07/yr., with a conditional large release probability equal to or very close to 1.0, as a result of the hazard's impact on the plant (i.e., containment bypass/failure).

[QN4] Design basis hazard frequency is less than 1.0E-06/yr. and the conditional core damage probability is less than1.0E-01, with a conditional large release probability equal to or very close to 1.0, as a result of the hazard's impact on the plant (i.e., containment bypass/failure).

[QN5] The initiating event or hazard may be screened out if it can be shown that their frequency is less than 1.0E-07/yr.

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 a PSA. 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, with the exception of hazards that are already addressed in the PSA for PNGS-A. Such hazards for which a PSA has already been initiated are seismic events, high winds/tornadoes. A list of the natural external hazards considered is presented in Table 4.

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 man-made 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 Internal Hazards Screening

4.2.1 Overview of Internal Hazards Screening Method

The internal hazards screening method is similar to the external hazards screening method and involves three main steps steps [7]:

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 PARA 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.

4.2.2 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. Internal hazards for which a PSA has already been initiated (e.g. internal fires, internal floods) were not considered. As a result of the screening assessment, no new internal hazard was identified to be included in the PARA.

5.0 LEVEL 1 PSA METHODS

The goal of the PNGS-A Level 1 PSA was to identify potential transients at the plant that would challenge fuel cooling, to identify what systems can be credited to mitigate the event, to determine what the impact of the transient may be on the mitigating systems, to determine whether the event can result in severe core damage should the mitigating systems fail, to quantify the total frequency of events that result in severe core damage, and to identify the major contributors to SCDF.

Typically, the first PSA study for a station is the Level 1 at-power PSA for internal events. Much of the effort of this study is in constructing models of what mitigating systems can be credited for a given transient, and how the mitigating systems can fail. In PSAs for other types of initiating events, e.g., internal fire, internal flood and seismic, much of the effort is associated with determining the impact these events have on the mitigating systems. The descriptions of the methodology for the various Level 1 studies in the following subsections reflect different requirements for the different studies.

The Level 1 at-power PSA for internal events was used to aid in the development and quantification of the outage, seismic, fire, high wind, and internal flood PSA.

5.1 Level 1 At-Power PSA for Internal Events

The PARA-L1P for internal events was prepared following the methodology described in [8]. This methodology was accepted by the CNSC.

The major activities of the PARA-L1P were:

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

(b) Development of a Fuel Damage Category (FDC) 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. Event trees are a tool that establishes what consequences can occur following a particular initiating event, given success or failure of the systems credited with mitigating the initiating event. Development of the PARA event trees is discussed in Section 5.1.3.

(d) Development of system-level fault trees needed to quantify the probability of failure of the mitigating systems credited in the event trees. This includes the support systems that interface with mitigating systems. The development of the fault trees 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 fault tree analysis mentioned above. The sources of the data in the component reliability database are also 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 event trees and system-level fault trees. Human error probabilities are systematically estimated and assigned. Human errors are referred to as “human interactions” in PARA. The HRA is discussed in Section 5.1.5.

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

Each of the above activities is summarised in the following sections of this report.

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.

5.1.1 Initiating Events Identification and Quantification

An Initiating Event (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 initiating events under consideration were those plant failures that could lead directly, or in combination with other failures, to severe core damage in a PNGS-A reactor. The list of initiating events in the PARA-L1P included:

- Events that only affect a single unit at PNGS-A.
- Events that can affect both units at PNGS-A. This includes, for example, events leading to a hostile environment in the powerhouse (e.g. steam line breaks), losses of off-site power and events leading to failure of the service water intake.
- Events occurring at PNGS-B that can also affect PNGS-A.

The objective of initiating event selection is to develop a comprehensive list of credible initiating events. For the PARA-L1P, the initiating event list was developed from past OPG PSAs, other published PSAs, safety reports for OPG’s nuclear generating stations, operating experience from CANDU nuclear generating stations, and insights gained from the system-level fault tree modelling. The complete set of initiating events used in the PARA-L1P is listed in Table 5.

The frequency of initiating events was quantified primarily using Bayes' Theorem. In a Bayesian approach, generic experience is updated with station-specific experience. This technique allows general experience and knowledge about a given event to be combined with actual operating experience 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 mitigating systems, may result in a different end state. The 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 frequency.

Each FDC represents a collection of event sequences judged to result in a similar degree of fuel damage. The FDCs are used as end-states in the Level 1 event trees, discussed in Section 5.1.3 of this report, and are used to transition from the Level 1 PSA to the Level 2 PSA, see Section 6.1 of this report.

The PARA-L1P used three FDCs:

1. Fuel Damage Category 1 (FDC1). This FDC represents the loss of core structural integrity due to the failure to shutdown the reactor following an initiating event.
2. Fuel Damage Category 2 (FDC2). This FDC represents the loss of core structural integrity due to the failure of post-accident heat sinks following a successful shutdown in response to an initiating event.
3. Core Structural Integrity Maintained (CSIM). This FDC represents all other end states for the event sequences.

SCDF is defined to be the sum of the frequencies of FDC1 and FDC2.

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, event trees are used to systematically review the possible ways that radioisotopes can be released from the fuel into containment.

The accident sequences are constructed using inductive logic. The graphical representation of this inductive logic is called an Event Tree (ET). The start of this inductive method is the IE, usually a plant malfunction. Following the identification of the IE, the next step is to identify the systems required to mitigate the IE and to show how the accident would progress if the mitigating systems were also to fail.

ET analysis requires the following to be predefined:

(a) The list of IEs to be considered (Section 5.1.1 of this report).

(b) The definition of sequence end states (Section 5.1.2 of this report) .

(c) The identification of mitigating systems.

A simplified ET for a large Loss Of Coolant Accident (LOCA) is presented in Figure 4. Following a large LOCA, three systems can mitigate fuel damage: the SDS, the ECIS and the heat sink function of the moderator system. The plant state must be assessed if one or more of these mitigating systems fail. These three systems form the branch points in the event tree.

The event tree is read from the left:

- Starting at the left is the initiating event “IE-LOCA”.

- Moving to the right, the first system credited with preventing fuel damage is the SDS. Failure of the shutdown system is represented by the ET branch point “SD”.

  The convention used to read an ET is that success of the mitigating system is the top branch of the event tree and failure is the lower.

  If the SDS fails, 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 are 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 5.

Once the Level 1 event trees have been created, the failure probability of the mitigating systems that have been identified in the ET must be assessed. This is achieved using fault tree analysis.

5.1.4 Fault Tree Analysis

A Fault Tree (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 the PARA-L1P, FT analysis was used to calculate the probability of ET branch points. FTs were used to quantify the probability of failure of the mitigating systems that appear in the ET. FTs were also used to calculate the probability of failure of the systems that support the mitigating systems that appear in the ETs.

Figure 5 depicts the relationship between the ETs and the FTs. Table 6 lists the systems modelled by FTs in the PARA-L1P.

For example, consider the moderator dump function of Shutdown System A. 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, a 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, the Abnormal Incidents Manuals, and other assessments and regulatory submissions.

Once a FT is constructed, it is linked with a database containing the information required to calculate the probability of each event in the FT. In the 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.

In the PARA-L1P, a Bayesian approach was adopted for estimating component failure rates. The Bayesian approach uses both generic data and plant-specific data in deriving failure rates. In the PARA-L1P, generic data was obtained from the U.S. Nuclear Regulatory Commission (NRC) [9], the T-Book and the Westinghouse Savannah River generic database [10]. The PNGS-A plant-specific data documented in the 2016 Annual Reliability Report [11] was used for the Bayesian update.

The reliability database also contains information on human errors modelled in the fault tree and event trees. 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 accident progression and the performance of mitigating systems, and in some cases can be significant contributors to risk. Thus, the potential for human errors must be systematically identified and incorporated into the event trees and the system level fault trees. Probabilities for the identified human errors must be estimated in a systematic fashion.

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 reflected in the components' failure rates and need not be identified in fault trees.

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

1. Where a system or component is inadvertently disabled by a human action prior to an IE. For example, a component may be left inadvertently disabled following a routine test or routine maintenance.
2. Where a system or component fails prior to an IE, and the failure is annunciated, but the operator fails to respond to the annunciation prior to an IE.
3. Where an operator action or a closely related series of actions simultaneously disables more than one piece of parallel / redundant equipment prior to an IE.
4. Where an operator fails to respond appropriately following an IE, either by not taking an action or by taking an inappropriate action.
5. Where an operator can plausibly interfere with the correct response of a mitigating system following an IE either by inhibiting the system or by activating the system.

Items 1 to 3, above may occur while performing normal operating, testing and maintenance procedures. Items 4 and 5, above may occur while following an emergency operating procedure.

Wilful or vengeful actions were not included in the PARA-L1P.

In order to systematically quantify the human interactions in the PARA, OPG used a human interaction taxonomy. This taxonomy classified human interactions in the PARA-L1P as one of: *simple* interactions, *complex* human interactions that occur prior to an IE; and *complex* interactions that occur after an IE.

Simple human interactions have the following characteristics:

(a) They occur while performing 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 main control room 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 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 main control room, and if any annunciations or inspections can detect the error.

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.

Post-initiating event complex human interactions 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 main control room 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 [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 [8] can be further refined using a detailed methodolgy such as Technique for Human Error Rate Prediction (THERP) [13].

5.1.6 Fault Tree 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.

In order to combine the FTs and ETs, the ET logic is first converted into FT logic with a top event for each FDC. These fault trees are referred to as the high level logic. The events in the high level logic are the IEs and the branch points from the event trees. 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 the PARA, CAFTA [14] was used to evaluate the integrated fault trees and FTREX [15] was used as the solution engine to quantify the results.

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 FDC. 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 fault tree 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 PSA guide for internal events [8] recommends that the solution of the integrated fault tree for each FDC be truncated at either four orders of magnitude below the most likely minimal cutset in that FDC or at 1×10^{-12} occ/yr, whichever is the highest. For FDC2 in the PARA-L1P, the frequency of the top minimal cutset was 6×10^{-7} occ/yr and a truncation of 6×10^{-11} 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.
- Sensitivity analysis to evaluate the impact on the results of a number of potentially critical assumptions made in the study.

5.2 Level 1 Outage PSA for Internal Events

The PARA-L1O was prepared following the methodology described in [16]. This methodology was accepted by the CNSC.

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 20% of the operating cycle.

A Level 1 outage PSA for internal events is developed following the same steps and general methodology as a Level 1 at-power PSA for internal events. However, an outage PSA must reflect the changing status of the plant through an outage, e.g. not all initiating events are possible during all phases of an outage and not all mitigating systems are available during all phases of an outage. This section of this report highlights the differences between an at-power PSA and an outage PSA.

5.2.1 Plant Operational State (POS) 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 grouping the various outage configurations into a manageable number of POSs during which the plant configuration and system failure criteria can be considered to be constant.

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. Pre-POS are developed based upon actual experience from planned outages and are the highest resolution of the outage states.

The Pre-POSs are then grouped into POSs. The POSs are bounding states based on the pre-POSs; the conditions in a POS are considered to be sufficiently stable for the purposes of an outage PSA. In the PARA-L1O, six pre-POSs were grouped into three POSs. Table 7 defines the three POSs used in the PARA-L1O.

5.2.2 Initiating Event Identification and Quantification

The development of a Level 1 outage PSA requires the identification, grouping and quantification of a set of outage IEs. IE identification and quantification for a Level 1 outage PSA for internal events follows the same steps and general methodology as for a Level 1 at-power PSA for internal events (Section 5.1.1 of this report). However, it is important to note that:

- There are system failures unique to an outage, e.g. failure of an ice plug on a HTS feeder.
- There are at-power IEs that cannot occur on a shutdown unit, e.g. a main steam line break.
- Not all IEs can occur in all POSs. For example, a large LOCA can only occur in a POS where the HTS is pressurized.
- IEs on the adjacent at-power units can affect the shutdown unit, e.g. a main steam line break on Unit 1 can induce a transient on U4.

Table 8 lists the outage IEs used in the PARA-L1O and lists the POSs in which each IE can occur.

5.2.3 Fuel Damage Category (FDC) Analysis

In the PARA-L1O, event tree sequences were assigned to either FDC2 or CSIM.

The PARA-L1O did not model loss of core structural intergrity 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 shutdown guarantee 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 Event Tree Analysis

The development of a Level 1 outage PSA requires the preparation of an ET for each outage IE.

ET analysis for a Level 1 outage PSA for internal events follows the same steps and general methodology as for a Level 1 at-power PSA for internal events (Section 5.1.3 of this report). However, a separate ET must be prepared for each IE/POS combination.

5.2.5 Outage System Fault Tree Analysis

The development of a Level 1 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 a Level 1 outage PSA for internal events follows the same steps and general methodology as for a Level 1 at-power PSA for internal events (Section 5.1.4 of this report). However, the outage FTs may be significantly different from the at-power FTs, these differences reflect the differences in system configuration and success criteria. 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 6 lists the systems modelled by fault trees in PARA-L1O.

5.2.6 Reliability Data Analysis

Reliability data analysis for a Level 1 outage PSA for internal events follows the same steps and general methodology as for a Level 1 at-power PSA for internal events (Section 5.1.4 of this report).

5.2.7 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.

Human reliability analysis for a Level 1 outage PSA for internal events follows the same steps and general methodology as for a Level 1 at-power PSA for internal events (Section 5.1.5 of this report). However, in an outage PSA, human error probabilities for the same action may vary between POSs and may be different from the values calculated in the at-power PSA. These differences reflect the different outage configurations.

Human interactions that can only occur during an outage are also addressed in this task.

5.2.8 Fault Tree 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.

Fault tree integration and evaluation for a Level 1 outage PSA for internal events follows the same steps and general methodology as for a Level 1 at-power PSA for internal events (Section 5.1.6 of this report). However, it is important to note that:

1. Only the frequency of FDC2 was estimated in the PARA-L1O.

2. The integration was performed for FDC2 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.

5.3 Level 1 At-Power PSA for Internal Fires

The PNGS-A at-power fire PSA (PARA-FIRE) was prepared following the methodology described in [17]. The methodology described in [17] is based upon NUREG/CR-6850 [18] and was accepted by the CNSC.

The objectives of the PARA-FIRE were:

- To identify areas of the plant particularly vulnerable to fires while both units are at high power;

- To identify the fire scenarios that make the greatest contribution to risk while both units are at high power;

- To characterize differences between the units that may affect risk; and

- To estimate the SCDF and the LRF for both single-unit and multi-unit fire scenarios.

The methodology described in [17] is broken into 17 tasks; these tasks are briefly descibed in Sections 5.3.1 to 5.3.14 of this report. The relationship between the 17 tasks is shown in Figure 8.

Seismic-fire interaction (Task 13) was outside the scope of the PARA-FIRE and is not addressed in this report.

The PARA-FIRE was prepared following an iterative approach. That is, the initial estimate of risk was based upon conservative and simplifying assumptions. With each subsequent iteration, the methods used to estimate risk for the various scenarios were refined, with effort focused on the most important contributors to risk.

5.3.1 Plant Boundary Definition and Partitioning (Task 1)

In this task the global boundary of the analysis is identified, i.e. the areas within the site where a fire could affect risk, and then partitioned into smaller Physical Analysis Units (PAU).

In the PARA-FIRE, a PAU is an area of the plant within which all fire scenarios are subject to similar conditions. In general, the boundaries of PAUs are defined by either physical barriers or a change in the fire detection and suppression capability. In some cases, large areas with no physical boundaries or changes in detection and suppression capability were subdivided into multiple PAUs to make the analysis more manageable.

The PAUs used in the PARA-FIRE were based on those identified in the PNGS-A Fire Hazard Assessment (FHA) [19]. 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 are identified. The cables may be associated with power supply to or control of the affected components.

In the PARA-FIRE, components and cables were divided into three groups:

1. Group B is the set of systems and components credited in the Fire Safe Shutdown Analysis (FSSA) [20] for safe shutdown and decay heat removal. 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 fires. These systems were only credited for fires which could be shown not to affect cables.

   The explicit component and cable selection process was applied to the following Group A functions:

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

   ii) Calandria Spray System (Moderator).

   This allowed reducing the modelling conservatism in the Fire PSA.
3. Group A was augmented by two additional functions:

   i) Make-up from the Emergency Mitigating Equipment (EME) to the boilers and to the calandria; and

   ii) Make-up from the firewater system to the calandria.

The cables and cable routing required for operation of these additonal functions were identified using the online wiring database.

The above grouping of components and cables was for the purposes of the PARA-FIRE only; it does not reflect any design or operational consideration.

5.3.3 Qualitative Screening (Task 4)

This task involves the identification and screening of PAUs that can be shown qualitatively to have little or no risk signficance. This task was not performed in the PARA-FIRE; all PAUs were conservatively retained for later tasks.

5.3.4 Fire-Induced Risk Model (Task 5)

This task involves the development of a logic model that reflects plant response to a fire.

The fire-induced risk model was developed from the PARA-L1P event tree for a forced shutdown. The PARA-L1P event tree was augmented to include:

- The impact of fire upon operator response (Task 12).
- The EME supply to the boilers and the calandria.
- The firewater supply to the calandria.

In fire PSA quantification (Task 14), this model was used to calculate the Conditional Core Damage Probability (CCDP) for each postulated fire scenario.

In the PARA-FIRE, the fire 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 internal fires to adversely affect the fail safe shutdown system was judged to be minimal.

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.

The key steps in the development of FIFs are:

- Plant walkdowns to identify fixed ignition fire sources. In the PARA-FIRE, the walkdowns were completed for PAUs in Unit 4 and PAUs in common areas that may affect Unit 4, e.g. the Main Control Room.
- Where Pickering experience was available, a Bayesian update of the generic fire frequencies obtained from [21] with Pickering site specific experience was performed. Where Pickering experience was not available, the generic FIFs from [21] were used.

- Development of transient fire ignition frequencies. This was based upon walkdowns and engineering judgment from site personnel who were familiar with plant operation.

5.3.6 Quantitative Screening (Task 7)

In the PARA-FIRE, this task was perfomed 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).

5.3.7 Scoping Fire Modeling (Task 8)

This task is a conservative and simplified initial refinement to the bounding treatment in Task 7. Ignition sources that do not pose a threat to targets in a PAU are screened out of the PSA.

The scoping fire modelling is used to develop explicit fire scenarios for individual fixed ignition sources, transient ignition sources, and self-ignited cable fires within the risk significant PAUs. The development of these detailed fire scenarios was supported with plant walkdowns, during which information was collected on each ignition source, and distances measured from each ignition source to potential target equipment and cabling.

Only the target cables and equipment within the zone of influence of a particular ignition source were assumed to fail in the fire scenario and then carried forward into the PSA quantification (Task 14). The zone of influence for a particular fire was determined using generic fire models.

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

The purpose of these tasks is to:

- Screen out cables that do not affect a component's response to a fire;
- Determine the response of components to the different cable failure modes; and
- Estimate the probability of the cable failure modes that can affect the operation of components.

For Group B components and cables, the analysis completed in the PNGS-A FSSA [20] was used in the PARA-FIRE.

The only components included in the PARA-FIRE that were not in the PNGS-A FSSA were the Group A components, the EME supply to the boilers and the calandria, and the firewater make-up to the calandria:

- For Group A components, fires were either shown not to affect the control circuits and power cabling of Group A components or the whole of Group A was assumed to fail. Therefore, these tasks were not required for Group A components.

- The routing of the cables for the EME and firewater systems were identified from the online wiring database, and a simplified and bounding approach for these tasks was applied to these cables.

5.3.9 Detailed Fire Modeling (Task 11)

The purpose of this task is to develop more detailed fire models that more realistically assess the impact of fire scenarios upon equipment, cables and human response.

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 a 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. Main Control Room 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 latest PARA-FIRE, in addition to updating the fire ignition frequencies with the latest generic fire frequencies as described in Section 5.3.5, the modelling of the following fire scenarios were refined:

- Catastrophic turbine generator (TG) oil 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.

The methodology for assessing potential fire-induced failures of containment isolation was also updated as part of the refinement efforts.

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 new actions that may be specific to the fire PSA, e.g. the plant's fire response 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).

The fire risk model was developed from the forced shutdown event tree in the PARA-L1P. Therefore, the first step in this task was to identify the post-initiator operator actions modeled as human failure events in the fire risk model / forced shutdown event tree. Pre-fire operator actions and operator actions associated with non-fire induced events were not revised.

For each human failure event that represents a post-fire operator action, multipliers were developed to adjust the human error probability assumed in the forced shutdown event tree. The multipliers considered the following factors:

- Location (either inside the MCR actions or outside the MCR actions);
- Time available;
- Complexity of the action;
- Availability of instrumentation; and
- Availability of the path to equipment in field actions.

In addition, human error probabilites were calculated for the deployment and monitoring of the EME.

5.3.11 Level 1 Fire 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 impact of each fire scenario upon equipment and cables determined in Tasks 8 – 11 is reflected in the fire PSA model (Task 5), and the fire PSA model is solved to estimate the CCDP for each fire scenario.

The CCDP is multiplied by the appropriate FIF to estimate the fire induced SCDF for each of the fire scenarios. The total fire SCDF is the sum of the SCDFs from all of the fire scenarios.

The SCDF contribution from the PAUs that were screened out as part of quantitative screening analysis (Task 7) was added to estimate the total fire-induced SCDF.

5.3.12 Uncertainty and Sensitivity Analysis (Task 15)

Sources of uncertainty were identified and the sensitivity of the results of the PARA-FIRE to the sources of uncertainty was assessed. In general, uncertainties associated with each of the fire PSA tasks were minimized and those that remained lend a conservative bias to the results.

Sensitivity studies were performed for:

- Credit for Phase 2 EME;
- Credit for simultaneous EME deployment to Units 1 and 4 in a two unit event; and,
- Credit for installed Uninterrupitble Power Supply (UPS) to Emergency Coolant Injection (ECI) and Shutdown Cooling (SDC) Isolation valves.

5.3.13 Level 2 Analysis (Task 17)

Refer to Section 6.3 of this report.

5.3.14 Alternate Unit Analysis (Task 18)

The comparison of Unit 1 to Unit 4 from the fire risk perspective 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 Level 1 At-Power PSA for Internal Floods

The PARA-FLOOD was prepared following the methodology described in [22]. This methodology was accepted by the CNSC.

The major tasks of a Level 1 at-power PSA for internal floods are:

- 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 5.4.9 of this report. The relationship between these tasks is shown in Figure 9.

Seismic-flood interaction was outside the scope of the PARA-FLOOD and is not addressed in this report.

The PARA-FLOOD was prepared following an iterative approach. That is, the initial estimate of risk was based upon conservative and simplifying assumptions. With each subsequent iteration, the methods used to estimate risk for the various scenarios were refined, with effort focused on the most important contributors to risk.

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 [20].

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 HPECI; or
- Group A – all other systems credited in the forced shutdown event tree of the PARA-L1P.

The above grouping of components and cables was for the purposes of the PARA-FLOOD only; it does not reflect any design or operational considerations.

The potential for floods originating in PNGS-A and affecting Group B mitigating equipment located in PNGS-B was addressed in this task.

5.4.2 Identification of Flood Sources (Task 2)

This task identified the potential flood sources in the plant and the associated flooding mechanisms. This task included:

- Identifying or confirming the flood sources in each flood area. The potential flood sources included:
  - Normally operating systems that contain water;
  - Standby safety systems that contain water, e.g. the ECIS;
  - Tanks or pools located in the flood area;
  - External sources of water, e.g. Lake Ontario, that are connected to the flood area through a system or structure; and
  - In-leakage pathways from other flood areas, e.g. drains and doorways.
- 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 these mitigating functions.
- Identifying flood propagation paths.

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 supported the other tasks by identifying or confirming plant data by observing it at the plant during walkdowns.

5.4.4 Internal Flood Qualitative Screening (Task 4)

This task involved the identification and screening of flood scenarios that can be shown qualitatively to have little or no risk significance. The following rules were used when screening:

- Screening criteria for flood areas:
  - The area contains no credible flood source or no sources that could propagate from one area to another; and
  - Flooding of the area does not cause an initiating event or the need for an immediate plant shutdown.

- 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 PARA-L1P already addresses this type of failure; and
  - Mitigating human actions can be shown to be effective, i.e. all of the following can be shown:
    - i) Flood indication is available in the MCR;
    - ii) The flood source can be isolated; and
    - iii) The mitigation action can be performed with high reliability.
- The flood source is a high energy line already considered in the PARA-L1P.

5.4.5 Flood Scenario Characterization (Task 5) and Consequence Analysis (Task 7)

These tasks 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 flood failure mechanism, e.g. spray, jet or flood.
- The consequences of the flood, including:
  - Flood propagation;
  - SSCs damaged by the flood; and
  - Identification of the type of initiating event caused by the flood. As a minimum all floods were assumed to cause a forced shutdown.
- Operator and mitigation system responses to terminate the flood.
- The means to be used to define the interface with the PARA-L1P model for estimating SCDF.

5.4.6 Initiating Event Frequency Estimation (Task 6)

This task estimated the frequency of internal flood initiating events.

The frequency of internal flood initiating events was estimated by multiplying generic pipe rupture frequencies, 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 for sprays, floods and major floods.

5.4.7 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 is similar to that used in the PARA-L1P; however, flood scenario-specific Performance Shaping Factors were considered for all credited operator actions. The flood specific Performance Shaping Factors addressed:

- Additional workload and stress above that for similar sequences not caused by internal floods;
- Availability of indications;
- Time available;
- Complexity of the action;
- Availability of flooding-specific job aids and training; and
- Effect of the flood upon the mitigation actions, e.g. accessibility restrictions due to the flood.

5.4.8 PSA Modelling of Flood Scenarios (Task 9)

This task involved the development of a logic model that reflects plant response to a flood.

The flood-induced risk model was developed from the PARA-L1P event tree for a forced shutdown.

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 shutdown system was judged to be minimal.

5.4.9 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 event trees.

Qualitative sensitivity and uncertainly analyses were prepared as part of this task.

5.5 Level 1 At-Power Seismic

OPG prepared seismic assessment following the “phased approach” described in [23];

- **Phase 1 - PSA-Based Seismic Margin Assessment** - In Phase 1, a Probabilistic Safety Assessment-based Seismic Margin Assessment (PSA based SMA) is performed. This focused approach uses a plant model based on Level 1 At-Power PSA with the addition of 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 - Limited Seismic PSA** – In Phase 2, the Phase 1 results are used to identify the most effective approach to convert the Phase 1 risk-based seismic margin study into a limited seismic PSA. Uncertainty in the seismic hazard and seismic fragilities are included, propagated, and displayed in the final quantification of risk estimates of the plant for significant risk contributors.

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 primary steps in developing the PSA-based SMA are identifying the seismic hazard at the site, constructing an event tree and fault tree 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 was created based on the internal events At-Power PSA, PARA-L1P. 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 relationship between these tasks is shown in Figure 10.

In addition to the above tasks, the risk of seismically-induced internal fires and seismically-induced internal floods 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 develop the site-specific seismic hazard.

The seismic hazard is a representation of the 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). RLE is the ground motion defined as the 84th percentile Uniform Hazard Response Spectrum (UHRS) based upon the 10,000 year return period.

Within the PSA-based SMA, the RLE curve is used to obtain seismic fragilities of the credited equipment and structures, and the plant level seismic capacity is further determined. The mean 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 involves two related but separate sub-tasks: development of the seismic event tree logic and development of the Seismic Equipment List (SEL).

The seismic event tree displays and accounts for the impact of a seismic event upon SSCs required for safe shutdown and decay heat removal following an earthquake. The seismic event tree must address:

- The seismically induced failure of buildings and other structures, such as the powerhouse. 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 unqualified 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 rupture of the HTS and/or the main steam system. Failure of one or both of these systems can significantly affect seismic risk;

- The seismically induced failure of rugged equipment. This branch point represents the plant equipment screened in Task 4; and

- The failure, seismically induced and random, of equipment in the systems that mitigate the consequences of a seismic event.

The SEL is the list of all components that are required to safely shutdown the reactor and remove decay heat following an earthquake and credited in the PSA-based SMA. This task relies upon the internal events PSA and other safe shutdown analyses to define the functions, structures, systems and components required to mitigate seismic initiating events.

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 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 equipment in the SEL 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. The site structures responses developed in the PNGS-A SMA issued in 1998 [24] were used in the PARA-SEISMIC. This was considered to be reasonable and conservative as the UHRS developed in 1998 is bounding the latest UHRS developed for the PARA-SEISMIC in the range of spectral frequencies of concern for the site structures response. 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 reviews of the SEL items in one lead unit (Unit 4) and the items in the systems common to all four units.

The role of the plant walkdown is to:

- Observe as many of the SEL items as possible and record any deficiencies;
- Screen out SSCs from further evaluation on the basis of high demonstrable seismic capacity. In the PARA-SEISMIC, a peak ground acceleration of 0.5g was used as the screening threshold; this screening level was chosen to be high enough such that the contribution from screened-out SSCs is not significant to overall seismic risk;
- Define the failure modes of SEL items;Identify equipment and structures that are not included in the SEL, but whose structural failure may affect nearby SEL items (i.e., seismic interaction concerns);
- 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..

the results of the walkdowns were recorded on a Screening Evaluation Worksheet 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 seismic demand. The likelihood that equipment will fail increases as it is subject to greater seismic demands. 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 0.8.

The fragility analysis conducted for a PSA-based SMA is limited to that of the Conservative Deterministic Failure Margin method, whereby the seismic capacity is calculated in terms of a High Confidence of Low Probability of Failiure (HCLPF) value using a generic representation of the variabiltiy accordning to the applicable standards and practices [23].

5.5.6 Seismic Risk Quantification (Task 6)

The process of evaluating seismic risk is similar to that used for the PARA-L1P (Section 5.1.6 of this report). That is:

- The branches of the seismic event tree that result in severe core damage are converted to high level logic in the form of a fault tree.
- The high level logic is then integrated with the fault trees for the mitigating systems and their support systems. It is important to note that the system fault

trees must be revised to include seismically induced failures of SSCs based upon tasks 4 and 5.

i) All seismically induced failures are assigned a failure probability of 1 and the high level logic is solved using FTREX.

- 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.

- The total SCDF is the sum of seismically induced SCDF and the SCDF from cutsets that include non-seismically induced failures.

The SCDF was estimated for the full range of earthquake recurrence intervals. However, for comparison of the SCDF to OPG's risk goals, the convolution was limited to earthquakes with a recurrence interval up to and including 10,000 years.

In the PARA-SEISMIC, the seismic 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 seismic events to adversely affect the fail safe shutdown system was judged to be minimal.

5.6 Level 1 At-Power PSA for High Winds

The PNGS-A Level 1 at-power high wind PSA (PARA-WIND) was prepared following the methodology described in [25]. This methodology was accepted by the CNSC.

The major tasks of a Level 1 at-power high wind PSA are:

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

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.

The PARA-WIND was prepared following an iterative approach. That is, the initial estimate of risk was based upon conservative and simplifying assumptions. With each subsequent iteration, the methods used to estimate risk for the various scenarios were refined, with effort focused on the most important contributors to risk.

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 wind and tornado wind hazards based on site-specific and region-specific data.

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 tornado point hazard curves were combined with the point hazard curves for other high winds to produce the combined high wind hazard curves. These wind hazards are considered to be independent stochastic events.

A combined wind hazard is developed and from that the high wind initiating event frequencies are derived for the PSA model (Task 4), based on the mean wind speeds corresponding to each of the Fujita scales (F1 through F5).

The all-winds hazard curve used in the PARA-WIND is shown in Figure 14.

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 peak gust wind speed. A list of high wind targets was generated in Task 4. The missile risk was derived based on missile sources, plant layout, and plant design information, supplemented by plant walkdowns.

The EPRI-developed TORMIS methodology was utilised to estimate the probability of tornado missile impact and damage to plant structures and components ([26] and [27]).

5.6.3 Task 3 - High Wind Fragility and Combined Fragility Analysis

The purpose of this task is to evaluate the fragility of high wind targets identified in Task 4 due to high wind loading effects.

The SSCs identified in task 4 include both safety related systems and their support systems. For each component in a safety related system, a chain of dependencies from the components through its support systems can be identified. The weakest link in the chain of dependencies with respect to high wind and water exposure was considered in the fragility analysis.

The median wind capacity and associated uncertainty was calculated for the weakest links. These calculations were based on data available from design documentation, National Building Codes and plant walkdowns. The median wind capacities and associated uncertainties were used to derive wind fragility curves.

A refined fragility analysis was prepared for the metal cladding on the Turbine Hall, Turbine Auxiliary Bay, and Class I and II structures inside the turbine building. This provided a more accurate assessment of the cladding fragility and an assessment of the portion of the cladding over the whole building that might fail.

5.6.4 Task 4 - Plant Logic Model Development

This task addresses two related but separate sub-tasks: development of the high wind event tree logic and development a list of components to be credited / analyzed in the high wind PSA.

The high wind event tree displays and accounts for the impact of a high wind event upon SSCs required for safe shutdown and decay heat removal following a storm. The high wind event tree must address:

- The wind induced failure of buildings. The collapse of a building was assumed to result in the failure of all equipment in that building; and
- The failure of SSCs that are required to safely shutdown the reactor and remove decay heat following a storm. This includes both wind-induced failures and random, independent failures.

In the PARA-WIND, the EME supply to the boilers, the EME supply to the moderator and the firewater system to the moderator were incorporated into the high wind event tree.

The list of SSCs that are required to safely shutdown the plant and remove decay heat was developed from the high wind event tree and its associated fault trees. This list formed the basis for the list of targets to be considered in the analysis of wind borne missile risk (Task 2) and high wind fragility analysis (Task 3).

5.6.5 Task 5 - Plant Response Model Quantification

The purpose of this task is to integrate the risk model and estimate the SCDF due to high winds.

The branches of the high wind event tree that result in severe core damage were converted to high level logic in the form of a fault tree. The high level logic was then integrated with the mitigating system fault trees that had been updated to include both high wind failures and random component failures. The high level logic was then integrated with the wind hazard curve. That is, the model was solved for each of the wind speed sub-intervals (Table 9) using the mean hazard curve and the appropriate component wind fragilities for that sub-interval.

In addition to providing the frequency for each sequence, quantification identifies the dominant accident sequences, component failures, and human actions with respect to high wind risk.

The SCDF was estimated for the full range of high wind recurrence intervals. However, for comparison of the SCDF to OPG's risk goals, the convolution was limited to high winds with a recurrence interval up to and including 10,000 years.

In the PARA-WIND, the wind 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 high winds to adversely affect the fail safe shutdown system was judged to be minimal.

6.0 LEVEL 2 PSA METHODS

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 Level 1 PSA to quantify the frequency of releases.

The Level 2 at-power PSA for internal events is used as an aid in the development of the Level 2 at-power PSAs for the other hazards; therefore, the methodology for the Level 2 at-power PSA for internal events will be described in the most detail.

6.1 Level 2 At-Power PSA for Internal Events

The PNGS-A Level 2 at-power PSA for internal events was prepared following the methodology described in [28]. This methodology was accepted by the CNSC.

6.1.1 Interface with Level 1 PSA

The PARA-L1P identified sequences resulting in severe core damage and estimated their frequency. These sequences form the starting point of the PARA-L2P.

The PARA-L1P categorized the severe core damage states into FDCs. The first step of a Level 2 PSA is to assign the sequences in these FDCs to Plant Damage States (PDS). The PDSs are the interface to the Level 2 PSA and are used as a means of managing the many different scenarios that can result in severe core damage.

Four PDSs were assigned in the PARA-L2P:

1. PDS1 represents sequences resulting in severe core damage as the result of failure to shutdown. That is, all sequences in FDC1 were assigned to PDS1.

2. 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.

3. 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 both PNGS-A units.

    ii) PDS3-6U which represents severe core damage at one or more PNGS-A units *and* severe core damage at one or more PNGS-B units.

4. 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 was further sub-divided into eight, labeled PDS2B to PDS2K, to reflect various random containment failures. The random containment system failures were identified by means 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 Filtered Air Discharge System (FADS) were subsequently eliminated from the PARA-L2P. It was determined that FADS may be initiated many hours into a transient when command and control of the plant has been transferred to the Emergency Response Organization (ERO). OPG's current methodology for human reliability analysis does not include actions initiated by the ERO.

Accident sequences assigned to a particular PDS are expected to result in a similar fission product release to containment and a similar containment response. Therefore, the characteristics of each PDS can be represented and modelled by a single representative accident sequence.

The representative accident sequence for each PDS was chosen by:

- Identifying the initiating events from the PARA-L1P that were the largest contributors to the frequency of the PDS; and

- Reviewing the sequences identified above to select a representative sequence that bounds the consequence.

The above approach follows the guidance of the International Atomic Energy Agency. The representative sequences chosen for each PDS are summarized in Table 10.

6.1.2 Containment Event Tree Analysis

A Containment Event Tree (CET) serves two main purposes:

1. It is a logic model that describes the progression of a severe accident, in particular, how severe accident phenomena can challenge the containment boundary.

2. It is a means to estimate the frequency of the various sequences that challenge the containment boundary. This, coupled with an estimate of releases for each sequence (Section 6.1.5), is an input to the estimate of LRF (Section 6.1.6).

Figure 16 shows a generic CET.

CET branch points 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.

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 fault trees are required to quantify the frequencies of the end-states of the Bridging Event Tree (Figure 15). FTs are required for the following containment sub-systems:

- Large breach of containment (LCEI). This is defined as a breach greater than 0.1 m^2 and may result from breaches through:
    - Failure of containment isolation (box-up);
    - Breach of containment via an airlock; or
    - Breach of containment via other containment penetrations/components.
- Small breach of containment (SCEI). This is defined as a breach less than 0.1 m^2 and may result from the same sub-systems as a large breach.
- Failure of the PRVs to open and limit containment pressure (PRV).
- Failure of the air cooling units to condense steam and reduce containment pressure (ACU). This includes:
    - the east fuelling machine vault ACUs;
    - the west fuelling machine vault ACUs; and
    - the boiler room ACUs.
- Failure of the hydrogen ignition system to control hydrogen concentration inside containment (IGN). This includes:
    - the igniters in the west fuelling machine vault;
    - the fans in the west fuelling machine vault ACUs;
    - the igniters in the east fuelling machine vault; and
    - the fans in the east fuelling machine vault ACUs

The FTs were prepared following the same general methodology as the FTs for the PARA-L1P (Section 5.1.4). Where systems are shared between PNGS-A and PNGS-B, the FTs from the PNGS-B Level 2 at-power PSA for internal events were used.

6.1.4 Release Categorization

The release categories in the PARA-L2P were limited to those that result in a large release of radioactive material to the environment. The Release Categories (RC) are listed in Table 11.

6.1.5 MAAP-CANDU Analysis

MAAP-CANDU (Modular Accident Analysis Program – CANDU) is a severe accident simulation code for CANDU nuclear stations. It is used to simulate the evolution of a severe accident through events such as core melt, primary heat transport system failure, calandria vessel failure, calandria vault failure, and containment failure. It is also used to estimate the magnitude of airborne releases of radioactive material from containment to the environment.

MAAP-CANDU is an Industry Standard Toolset code. MAAP-CANDU version 4.0.7D was accepted by the CNSC for use in the PNGS-A PSAs.

There are five distinct roles for the code:

1. To establish accident progression for each plant damage state;
2. To support CET branch point quantification;
3. To estimate releases to the environment for those sequences in which containment fails;
4. To support systematic sensitivity and uncertainty analysis; and
5. To provide information related to plant environmental conditions.

6.1.6 Integration of the Level 1 and 2 PSA

The purpose of integration is to link the Level 1 event trees with the PDSs via the Level 1/Level 2 bridging event tree and containment fault trees, 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 for Internal Events

The PNGS-A Level 2 outage assessment for internal events was prepared following the OPG methodology. This methodology was accepted by the CNSC.

Given the low SCDF for internal events occurring while a unit is in GSS (see Section 7.0 of this report), and given that less energy is available to challenge the containment envelope, a detailed Level 2 outage PSA for internal events was not prepared. Instead, a bounding assessment of the LRF was prepared for a unit in the GSS.

The bounding assessment was based on the following principles:

1. A large release can only occur if severe core damage has occurred. Therefore, the LRF for a unit in the GSS is bounded by the SCDF for a unit in the GSS.

2. Analysis using MAAP-CANDU demonstrated that accidents initiated in POS C do not progress to severe core damage within a 7-day analysis period. Therefore, transients initiated in POS C do not result in a large release. This outcome reflects the very low decay heat available approximately 70 days after shutdown.

3. Analysis using MAAP-CANDU demonstrated that accidents initiated in POSs A and B where Early Calandria Vessel Failure (ECVF) is postulated can progress to a large release. Based on the results of the PARA-L2P, only 13% of accidents that progress to severe core damage will progress to a large release as a result of ECVF. Therefore, the LRF due to early calandria failure is bounded by 13% of the SCDF. This is a conservative assessment as the MAAP-CANDU analysis only investigated sequences initiated early in an outage. It is likely that additional analysis could demonstrate that accidents with ECVF initiated later in an outage do not progress to a large release.

4. Analysis using MAAP-CANDU demonstrated that single or dual unit accidents without ECVF only progress from severe core damage to a large release in the first six days of an outage. That is, the LRF due to these sequences will be less than 10% of the SCDF.

5. The earliest time for calandria failure was estimated to be 12.5 hours after accident initiation. This provides more than sufficient time to deploy the EME, add water to the calandria and prevent calandria failure. Preventing calandria failure also prevents a large release.

6. The analysis assumed that the accident was initiated at the earliest possible time in each particular POS. As the time after shutdown increases, so the decay heat level falls, the likelihood of a large release falls, and the time at which a large release occurs, if at all, increases. For example, the time at which a large release occurs due to a total loss of heat sink at the earliest possible entry into POS B is greater than 72 hours, the mission time in OPG's PSAs.

7. Accidents that result in severe core damage and progress to a large release as a result of random failures of the containment envelope are a small contributor to LRF. This results from the high reliability of the containment envelope.

6.3 Level 2 Fire Assessment

The PNGS-A Level 2 fire assessment for internal events was prepared following the methodology described in [17]. This methodology was accepted by the CNSC.

The Level 2 assessment of internal fire risk was built on the Level 1 internal fire model. The approach for Level 2 fire risk consisted of five steps:

1. Evaluating each of the 3190 fire scenarios against the potential mechanisms by which a Severe Core Damage event could progress to a large release in the scenario.

2. Fire scenarios that affect both units at PNGS-A, e.g. fires affecting the MCR, were identified. Scenarios that result in severe core damage at both units were assumed to progress directly to a large release.

3. The probability of consequential containment failure due to phenomenological events or random failures following a single-unit event was estimated as 13% in PARA-L2P.

4. Single unit fire scenarios that result in severe core damage where the fire also affects containment components were identified. These scenarios were assumed to progress to a large release. The PARA-L2P was used to identify the containment components of interest and the FSSA was used to identify and characterize the impact of fires upon the containment components.

5. Single unit fire scenarios that result in severe core damage and progress to a large release as a result of random failures of the containment envelope were identified. These scenarios were assumed to progress to a large release. The probability of random failure of containment components was taken from the PARA-L2P.

6.4 Level 2 Seismic Assessment

The PNGS-A Level 2 seismic assessment was prepared following the methodology described in [23]. This methodology was accepted by the CNSC. Consistent with the approach described in OPG PNGS-A PSA Guide for Seismic Events for Phase 1 PSA-based SMA, Level 2 assessment is limited to the estimate of the seismically induced frequency of containment failure (SCFF). The estimation of SCFF involves a convolution of the most vulnerable seismically induced containment boundary failure mode with the seismic hazard curve for the station.

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.

The plant level HCLPF for the containment boundary was determined by inspection of HCLPFs for the containment boundary components.

The Seismically-induced Containment Failure Frequency (SCFF) was calculated by convolving the plant level HCLPH for containment boundary with the mean seismic hazard curve over the range of events up to the 10,000 year return period.

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 postulated 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 considered that the LRF estimate is equal to the SCDF estimate.

6.5 Level 2 Flood Assessment

The Level 2 at-power PSA for internal floods followed the OPG methodology. This methodology was accepted by the CNSC.

The approach for Level 2 flood risk consisted of five steps:

1. Flood scenarios that affect both units at PNGS-A, e.g. floods affecting the MCR, were identified. Scenarios that result in severe core damage at both units were assumed to progress directly to a large release.

2. The probability of consequential containment failure due to phenomenological events or random failures following a single-unit event was estimated as 13% in PARA-L2P.

3. Single unit flood scenarios that result in severe core damage where the flood also affects containment components were identified. These scenarios were assumed to progress to a large release.

4. Single unit flood scenarios that result in severe core damage coupled with random failures of the containment envelope were assumed to progress to a large release. The probability of the random failure of containment components was taken from the PARA-L2P.

5. Sequences where the flood induces a forced shutdown in both units and there are random, independent failures of mitigating equipment on both units leading to severe core damage in both units were idetified and assumed to progress to a large release.

6.6 Level 2 High Wind Assessment

The Level 2 at-power PSA for high winds followed the OPG methodology. This methodology was accepted by the CNSC.

The approach for Level 2 high wind risk consisted of four steps:

1. High wind scenarios that affect both units at PNGS-A were identified. Scenarios that result in severe core damage at both units were assumed to progress directly to a large release.

2. The probability of consequential containment failure due to phenomenological events or random failures following a single-unit event was estimated as 13% in PARA-L2P.

3. Single unit high wind scenarios that result in severe core damage coupled with random failures of the containment envelope were assumed to progress to a large release. The probability of the random failure of containment components was taken from the PARA-L2P.

4. Sequences where the high wind induces a forced shutdown in both units and there are random, independent failures of mitigating equipment on both units leading to severe core damage in both units were identified and assumed to progress to a large release.

6.7 Level 2 Outage Assessment for Seismic, Internal Flood, Internal Fire and High Wind Events

Given the low risk of fuel damage from internal events occurring while the unit is in GSS, a Level 2 study of the outage risks was not performed. Instead, it was shown that the risk from a single shutdown unit is low and it is bounded by the risk for the other high power unit. For more details refere to Section 3.1.

7.0 SUMMARY OF RESULTS

This section presents the results of the following most recent PSA studies that were completed as part of the PARA:

- Level 1 at-power PSA for internal events.
- Level 1 outage PSA for internal events.
- Level 2 at-power PSA for internal events.
- Level 2 outage for internal events.
- At-power PSA for internal fires.
- At-power PSA for internal floods.
- At-power PSA-based Seismic Margin Assessment.
- At-power PSA for high winds.

The PARA study uses SCDF and LRF measures to assess the acceptability of risk.

Table 12 and Table 13 present the SCDF and LRF for each of the above studies.

Table 12 compares the results of the internal events PSA studies described in Sections 5.0, and 6.0, with the OPG safety goals.

OPG did not prepare PSAs for internal floods, internal fires, seismic events and high winds for a single shutdown unit. The risk from each of these hazards while a unit is shutdown was shown to be bounded by the risk from an operating unit.

7.1 Results for At-Power PSAs

Results for PARA-L1P

The 2018 Level 1 at-power PSA for internal events (PARA-L1P) estimated the frequency of two Fuel Damage Categories, FDC1 and FDC2. These FDCs represent severe core damage due to the failure to shutdown and due to the failure of all heat sinks, respectively. The 2018 PARA-L1P includes items from the Fukushima Action Plan such as the EME credit in accident sequences with sufficient time for deployment. The frequencies of these FDCs are presented in Table 14.

The results in Table 12 and Table 14 show that:

1. The overall SCDF is more than one order of magnitude below OPG's safety goal; and
2. Sequences involving the failure to shutdown are a very small contributor to SCDF.

The PARA-L1P assumed that the reactor was at full power for 100% of the operating cycle.

Results for PARA-L2P

The Level 2 at-power PSA for internal events (PARA-L2P) included anlysis of five Plant Damage States (PDS).

The PDS analysis was used as an input to estimate the frequency of three Release Categories (RC). The frequencies of the three RCs are presented in Table 15.

The results presented in Table 12 and Table 15 show that the LRF is well below OPG's safety goal.

Results for the PARA-FIRE

The at-power fire PSA (PARA-FIRE) estimated the SCDF and LRF resulting from internal fires. The SCDF and LRF presented in Table 13 reflect the latest updates and modelling refinements described in Section 5.3.9.

The results in Table 13 show that:

1. The SCDF due to internal fires is well below OPG's safety goal; and

2. The LRF due to internal fires is below OPG's safety goal.

Results for the PARA-FLOOD

The at-power flood PSA (PARA-FLOOD) estimated the SCDF and LRF resulting from internal floods. The SCDF and LRF are presented in Table 13.

The results in Table 13 show that:

1. The SCDF due to internal floods is more than one order of magnitude below OPG's safety goal; and

2. The LRF due to internal floods is well below OPG's safety goal.

Results of the PARA-SEISMIC

The at-power PSA-based seismic margin assessment (PARA-SEISMIC) estimated the plant level HCLPF for the heat sinks to be 0.16g.

The PARA-SEISMIC estimated the seismically induced SCDF by convolving the plant level HCLPF with the mean seismic hazard curve.

The total seismic SCDF was estimated by adding the seismically induced SCDF to the SCDF from non-seismically induced failures. The non-seismically induced failures represent random failures of equipment in response to the unit shutdown forced by the seismic event. Random, non-seismically induced failures of SSCs contributed approximately 89% of the SCDF.

The results in Table 13 show that:

1. The total seismic SCDF is more than one order of magnitude below OPG's safety goal; and

2. The total seismic LRF is well below OPG's safety goal.

Results for the PARA-WIND

The at-power PSA for high winds (PARA-WIND) estimated the SCDF and LRF resulting from high winds. The SCDF and LRF are presented in Table 13.

The results in Table 13 show that the SCDF and LRF due to high winds are well below OPG's safety goal.

7.2 Results for Shutdown PSAs

Results for PARA-L1O

The Level 1 outage PSA for internal events (PARA-L1O) estimated the frequency of Fuel Damage Category FDC2 only as discussed in Section 5.2.3. This FDC represents severe core damage due to failure of all heat sinks. The frequency of FDC2 for each POS is presented in Table 16.

The results in Table 12 and Table 16 shows that the overall SCDF is more than one order of magnitude below OPG's safety goal.

Results for Level 2 Outage for Internal Events

Section 6.2 provides the methodology of the bounding assessment of Level 2 outage for internal events.

Given the time available for EME deployment and the low likelihood of a large release at any time other than the earliest part of an outage, the LRF from outage unit events occurring at Pickering 'A' was estimated to be less than the OPG safety goal for LRF as detailed in Table 1. The outage LRF estimate is presented in Table 12.

Results for Seismic, Internal Flood, Internal Fire and High Wind Events Level 1 and Level 2 Outage PSAs

As per the methodology described in Section 6.7 and based on the analysis results described for Level 2 Outage for Internal Events, the outage LRF for seismic, internal flood, internal fire and high wind events effectively becomes negligible as presented in Table 13.

8.0 REFERENCES

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

[2] Canadian Standards Association, "Management System Requirements for Nuclear Power Plants," CSA N286-05.

[3] Canadian Standards Association, "Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants," CSA N286.7-99.

[4] Ontario Power Generation, "Nuclear Program, Risk and Reliability Program," N-PROG-RA-0016, Revision 009, June 2016.

[5] Canadian Nuclear Safety Commission, "CNSC Integrated Action Plan on the Lessons Learned From the Fukushima Daiichi Nuclear Accident," August 2013.

[6] Ontario Power Generation, "OPG Probabilistic Safety Assessment (PSA) Guide - External Hazards Screening," N-GUID-03611-10001 Volume 8, Revision 004, November 2016.

[7] Ontario Power Generation, "OPG Probabilistic Safety Assessment (PSA) Guide - Internal Hazard Screening," N-GUID-03611-10001 Volume 9, Revision 002, May 2017.

[8] Ontario Power Generation, "Pickering NGS ‘A’ Probabilistic Risk Assessment (PRA) Guide – Level 1 (At-Power)," NA44-GUID-03611-00010, Revision 000, October 2012.

[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.

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

[11] Ontario Power Generation, "Pickering NGS – 2016 Annual Risk and Reliability Report," P-REP-09051.1-00016, Revision 000, April 2017.

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

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

[14] Electric Power Research Institute, "CAFTA, Software Manual Version 5.4," Software Product ID #1018460, 2009.

[15] Electric Power Research Institute and KAERI, "FTREX User Manual Version 1.7," Software Product ID #1016858, 2013.

[16] Ontario Power Generation, "Pickering 014 Probabilistic Risk Assessment Guide – Level 1 (Outage)," NA44-GUID-03611-00012, Revision 000, October 2013.

[17] Ontario Power Generation, Guide, "Pickering NGS A Probabilistic Risk Assessment (PRA) Guide - Fire," NA44-GUID-03611-00013, Revision 000, November 2012.

[18] Electric Power Research Institute (EPRI) and United States Nuclear Regulatory Commission, "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities: Volume 2: Detailed Methodology," EPRI TR-1011989 and NUREG/CR-6850, 2005.

[19] Ontario Power Generation, "Fire Hazard Assessment – Pickering A Nuclear Generating Station," NA44-REP-71400-10003, Revision 002, May 2017.

[20] Ontario Power Generation, "Fire Safe Shutdown Analysis – Pickering A Nuclear Generating Station," NA44-REP-71400-00023, Revision 001, May 2017.

[21] Electric Power Research Institute, "The Updated Fire Events Database: Description of Content and Fire Event Classification Guidance," EPRI Report 1025284, Palo Alto, CA, 2013.

[22] Ontario Power Generation, "Pickering NGS A Probabilistic Risk Assessment (PRA) Guide – Internal Flood," NA44-GUID-03611-00014, Revision 001, October 2013.

[23] Ontario Power Generation, "Pickering NGS A Probabilistic Risk Assessment Guide – Seismic," NA44-GUID-03611-00015, Revision 001, November 2013.

[24] Ontario Power Generation, "Seismic Assessment of Pickering A Nuclear Generating Station, Volumes 1 – 7," NA44-REP-02004-0073, February 25, 1998.

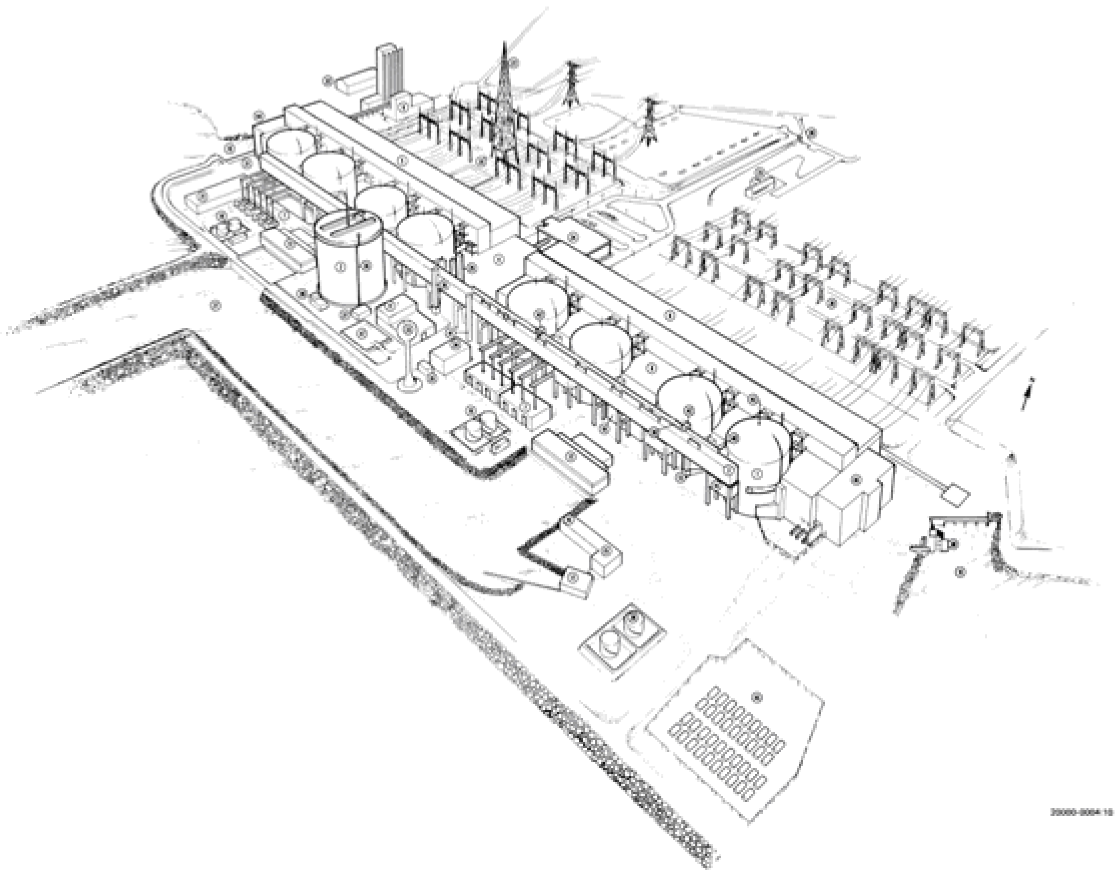
[25] Ontario Power Generation, "OPG Probabilistic Risk Assessment Guide – High Wind Hazard," N-GUID-03611-10001 Volume 10, Revision 000, September 2012.

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

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

[28] Ontario Power Generation, "Pickering A Probabilistic Risk Assessment (PRA) Guide – Level 2 (At-Power)," NA44-GUID-03611-00011, Revision 00, October 2012.

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



1. Reactor Building
2. Vacuum Building
3. Pressure Relief Duct
4. Service Wing
5. Turbine Hall (Units 1 to 4)
6. Turbine Hall (Units 5 to 8)
7. Standby Generators
8. Reactor Auxiliary Bay
9. Heavy Water Upgrading Plant
10. Cooling Water Outfall
11. Water Treatment Building
12. Screenhouses
13. Emergency Water Supply Valve Station (One Each for Units 5 to 8)
14. Unit Emergency Control Centre (One Each for Units 5 to 8)
15. Emergency Power Supply Generators
16. Emergency Water Supply Pumphouse
17. Tempering Water Pumphouse
18. Irradiated Fuel Bay (Units 5 to 8)
19. Oil Tanks for Standby Generators
20. Off-Gas Management Building
21. Auxiliary Irradiated Fuel Bay
22. Microwave Tower
23. Information Centre
24. Administration Building
25. Heavy Water Upgrading Towers
26. 230 kV Switchyard
27. Cooling Water Intake Channel
28. Emergency Power Generator Oil Tanks
29. Security Gatehouse
30. Small Craft Floating Dock
31. Component Dock
32. Warehouse
33. ECI Storage Tank
34. HPECI Pumphouse
35. ECIS Auxiliary Services Building
36. FAD Tower
37. FAD Stack Monitoring Buildings
38. FAD Stack
39. Emergency Cooling Injection System Piping
40. Emergency Cooling Injection System Valve Station (One Each for Units 5 to 8)
41. ECIS Concrete Tower
42. ECIS Steel Tower
43. Emergency Communications Antenna (Unit 8 Only)
44. West Annex Building
45. Dry Storage Module Yard
46. East Annex Building
47. Settling Basin

Figure 1: Pickering Site Layout

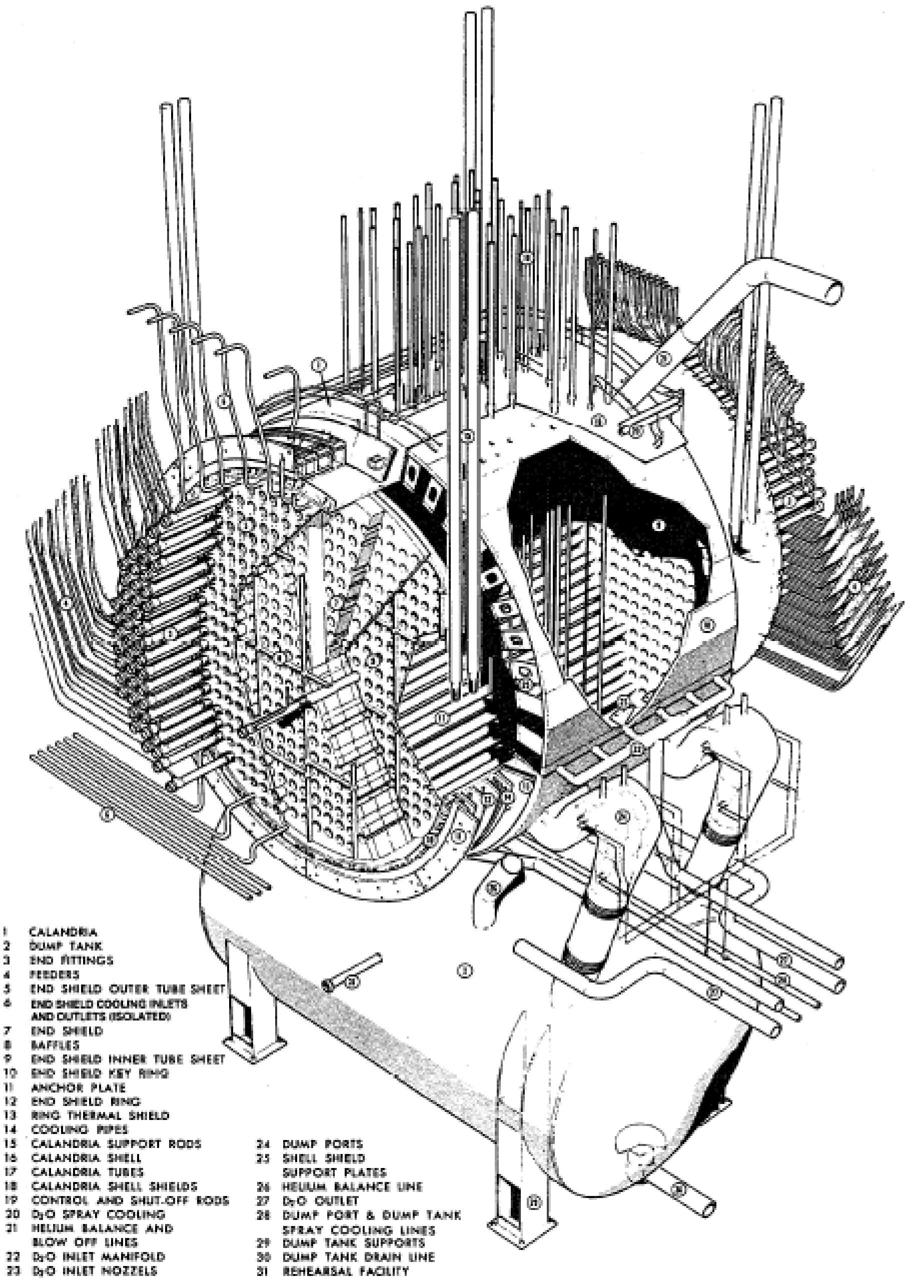


Figure 2: Typical Pickering NGS 'A' Reactor

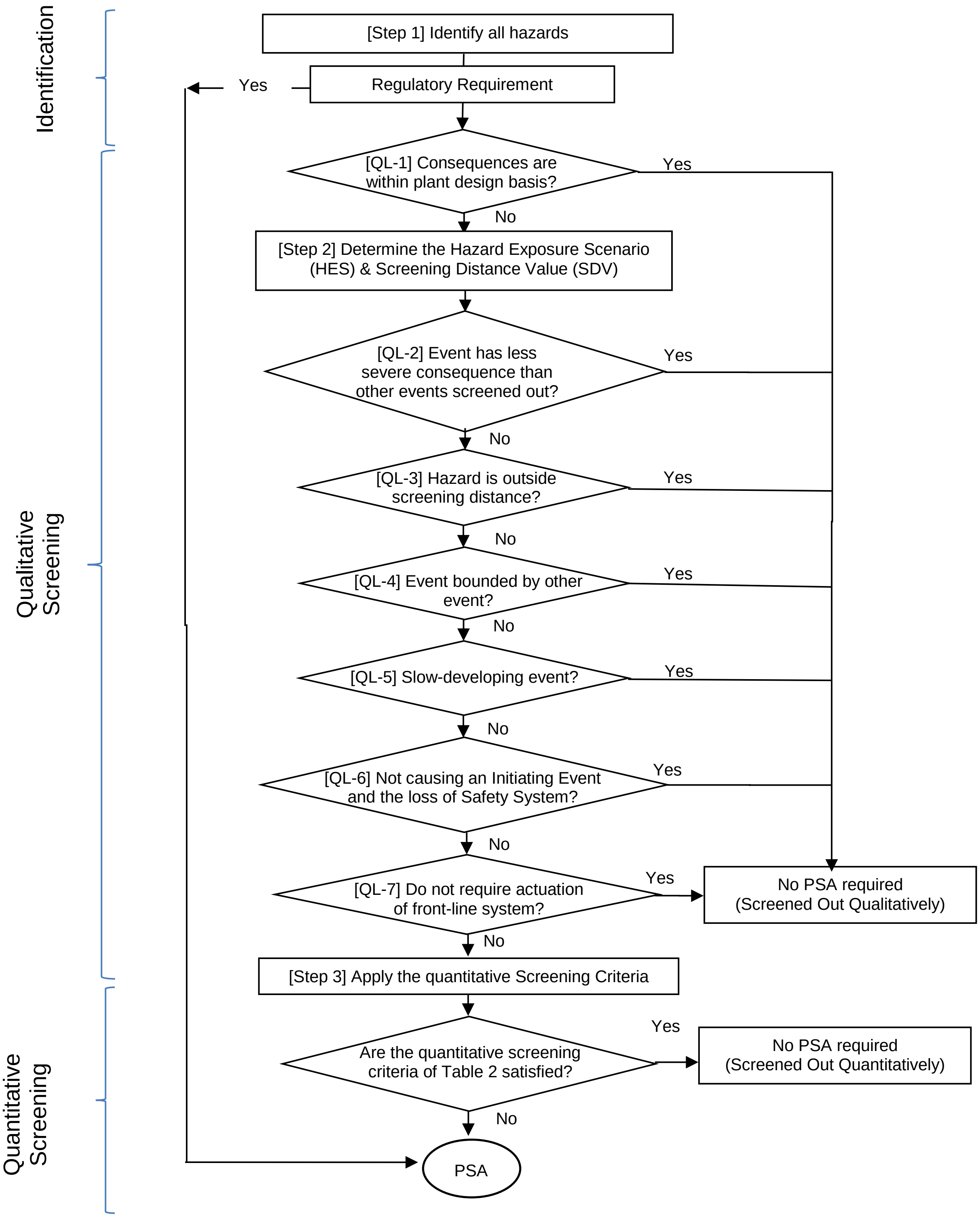


Figure 3: Hazards Analysis Steps

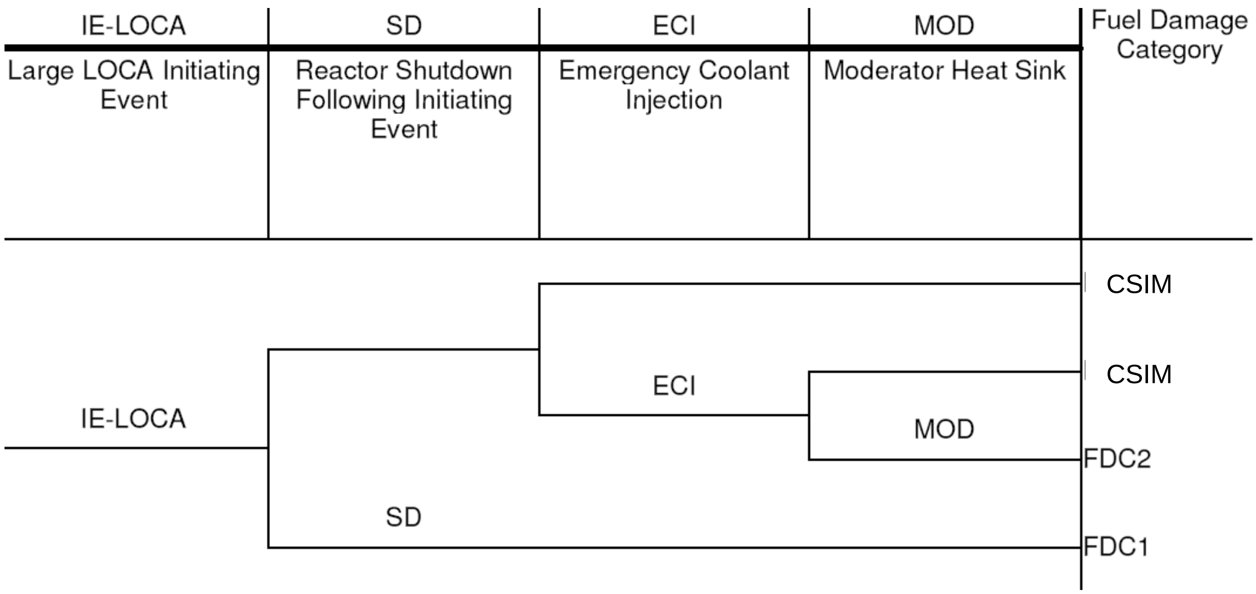


Figure 4: Example LOCA Event Tree

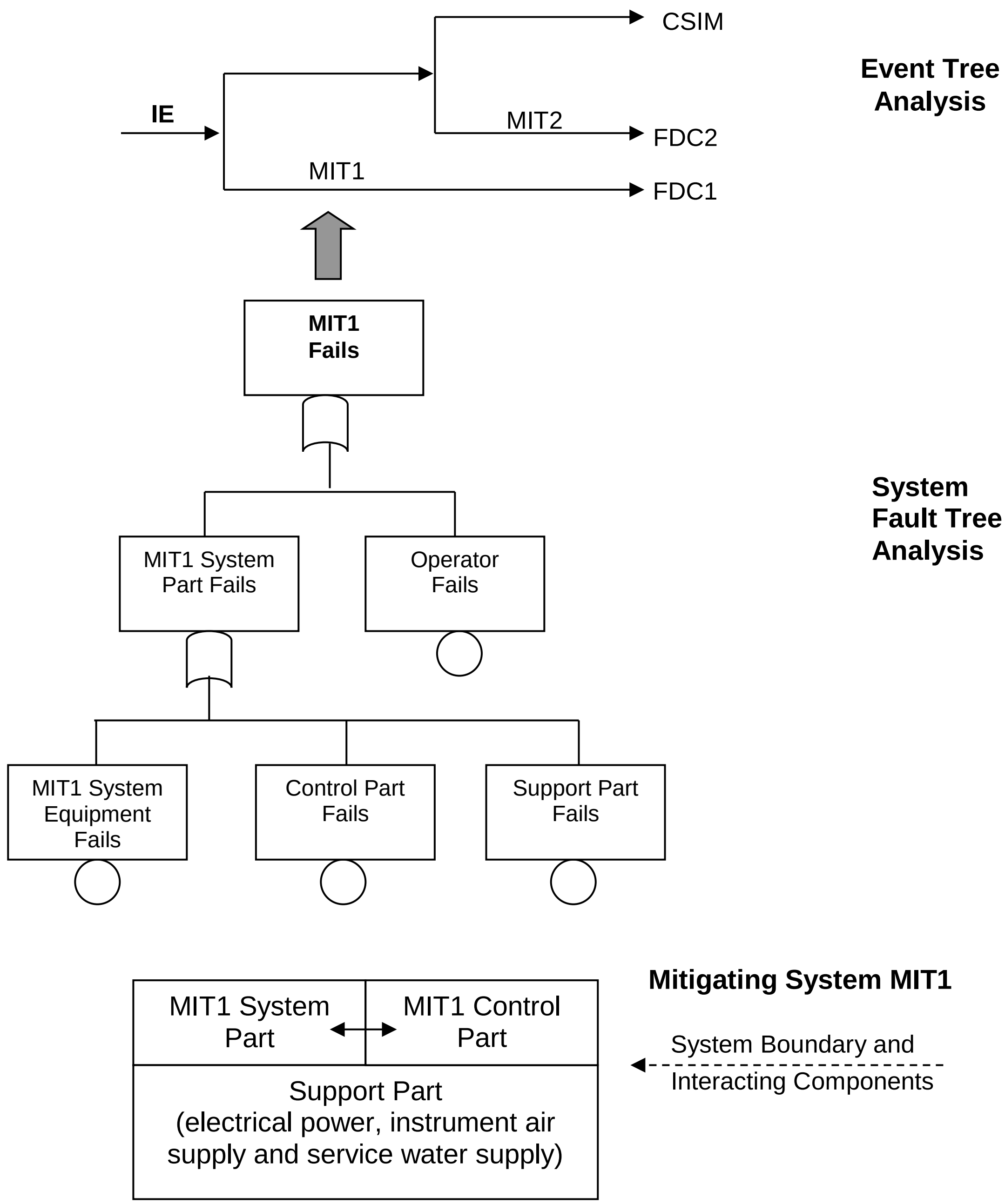


Figure 5: Fault Tree and Event Tree Integration

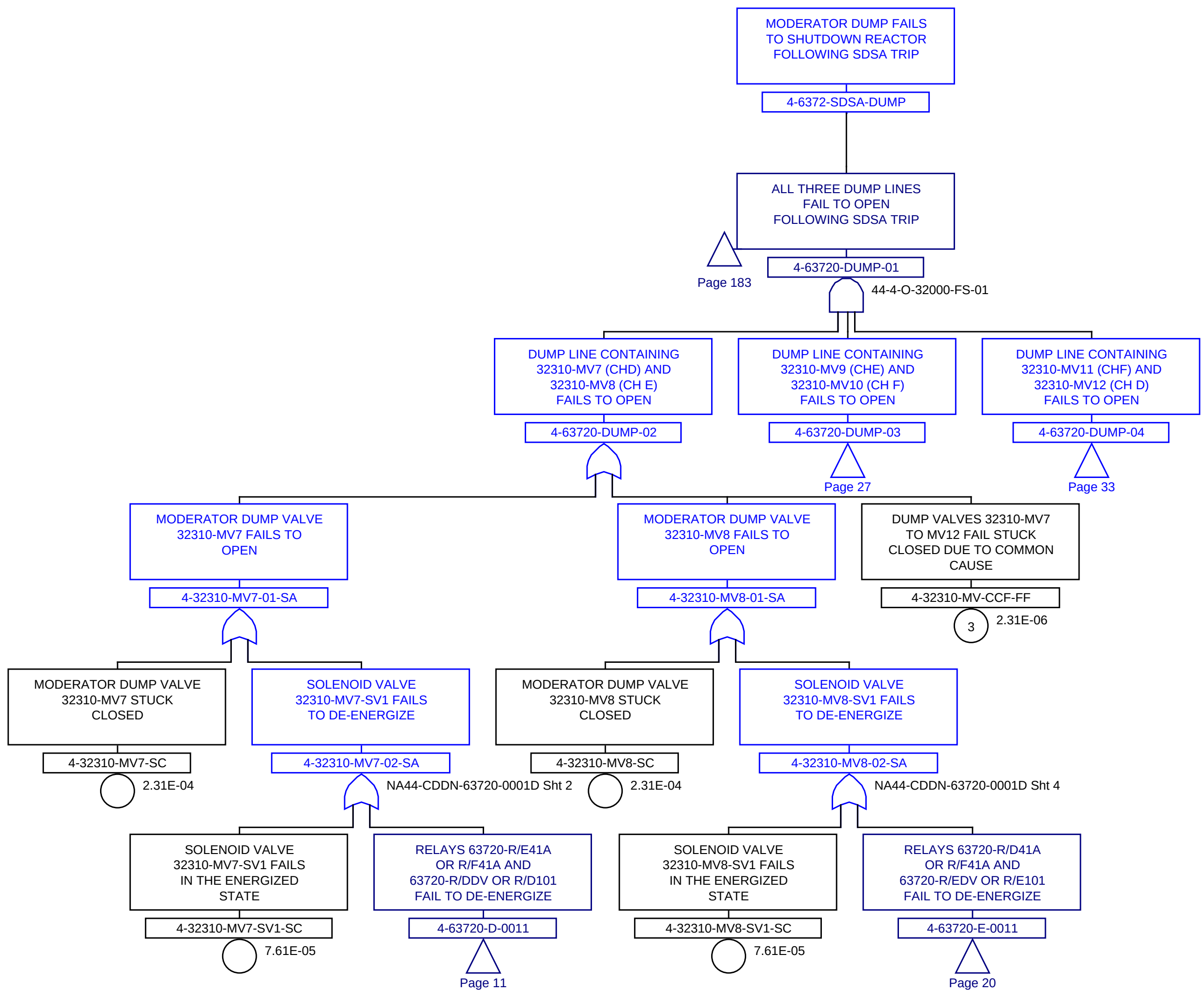


Figure 6: Example Fault Tree

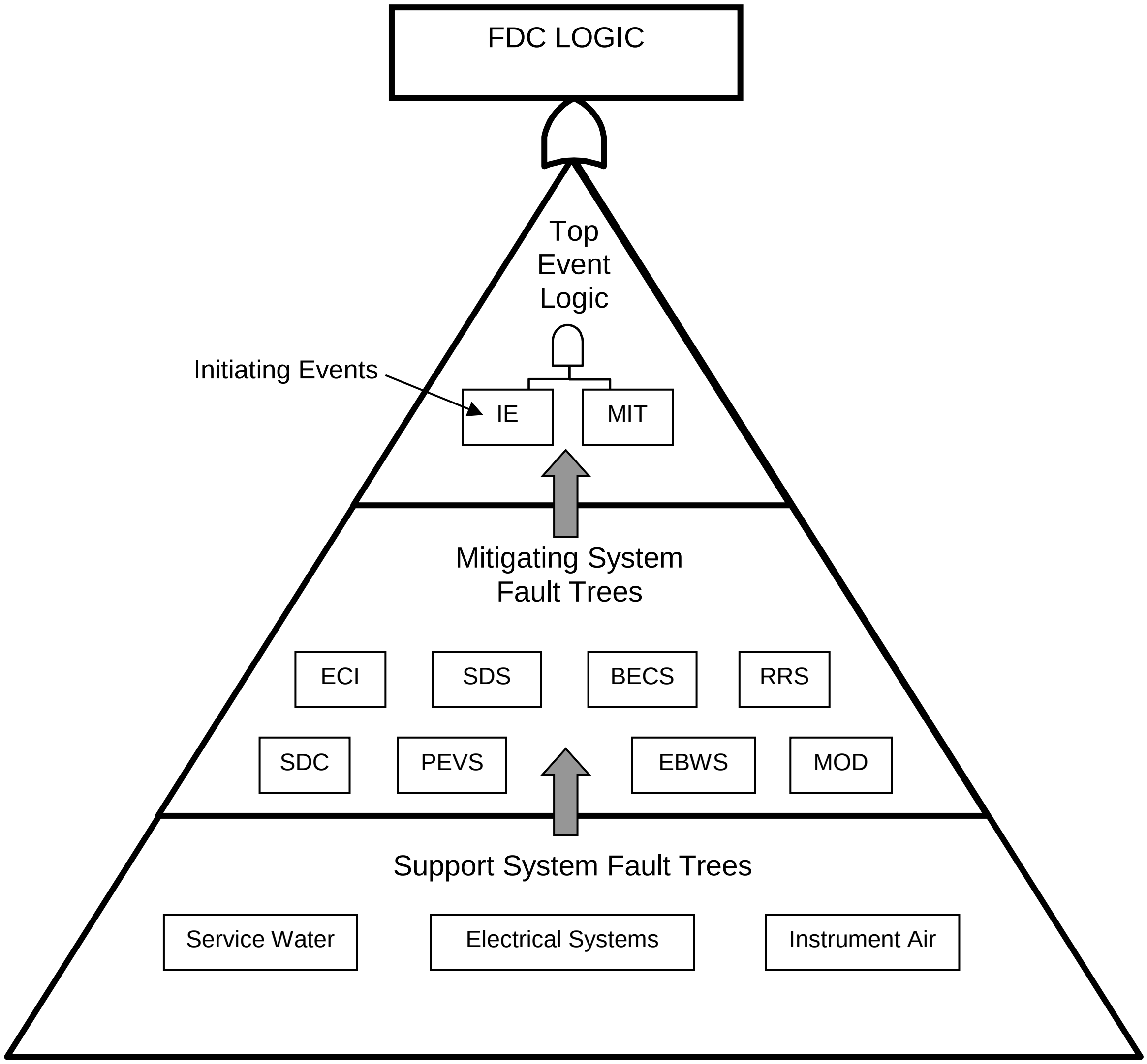


Figure 7: Fault Tree Integration

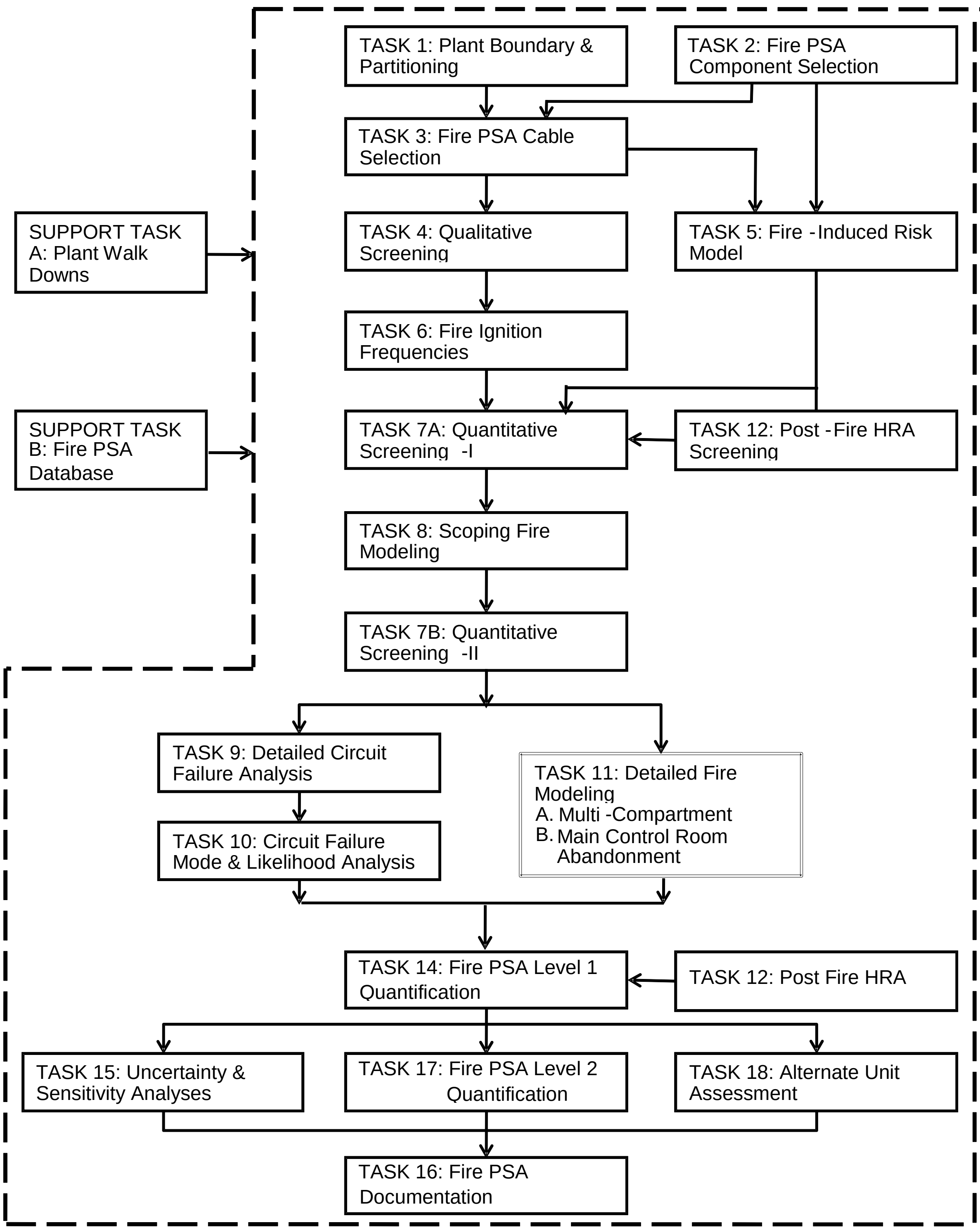


Figure 8: Fire PSA Tasks

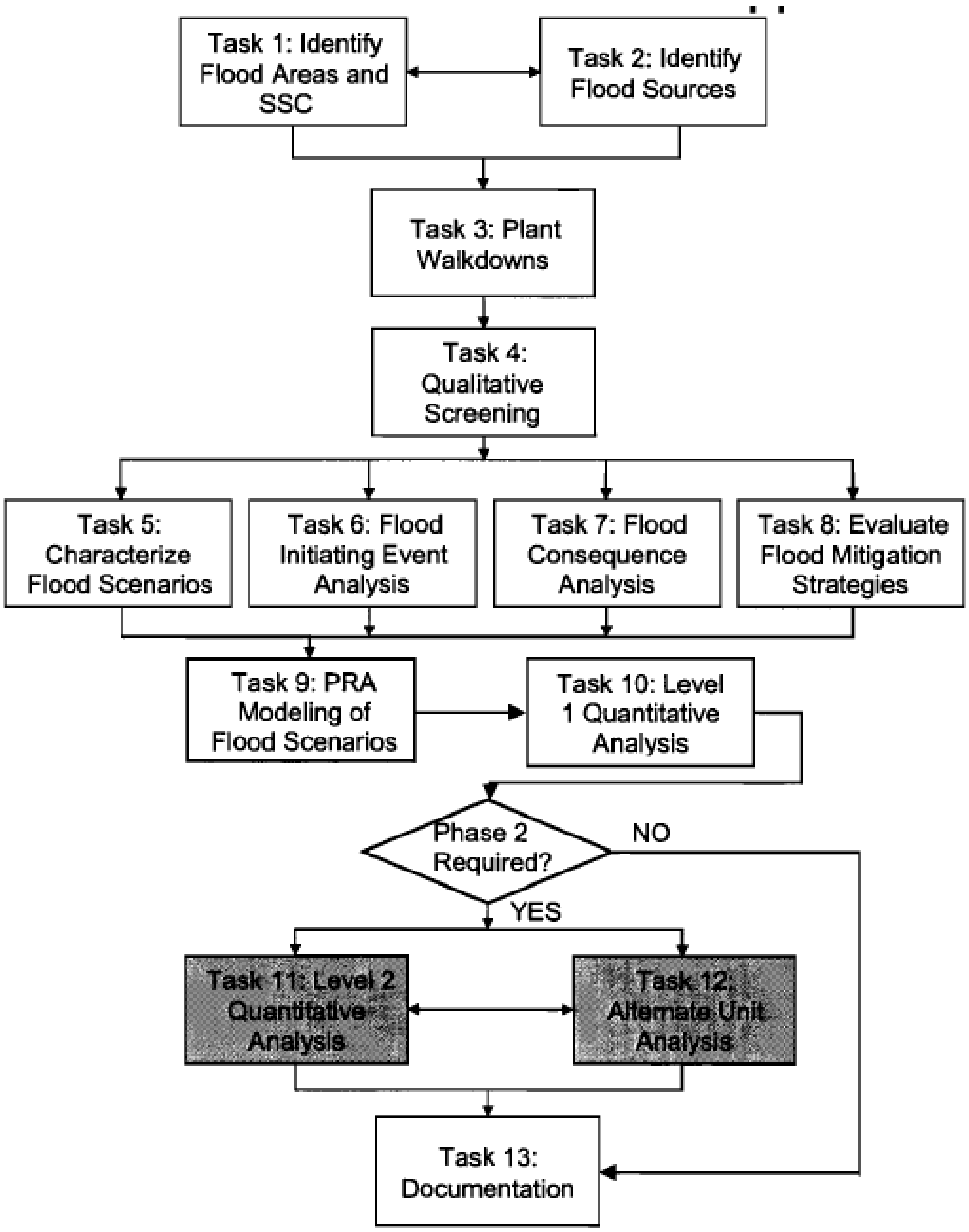


Figure 9: Internal Flood PSA Tasks

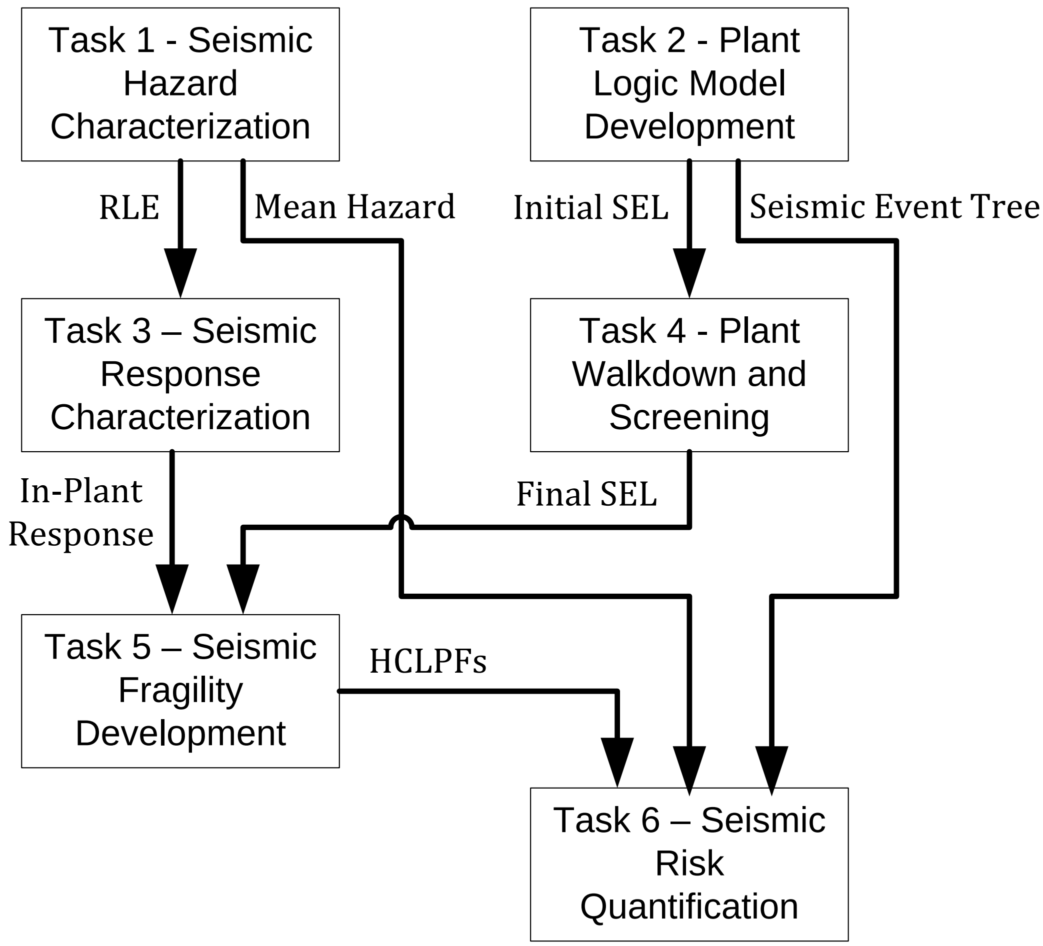


Figure 10: PSA-based SMA Tasks

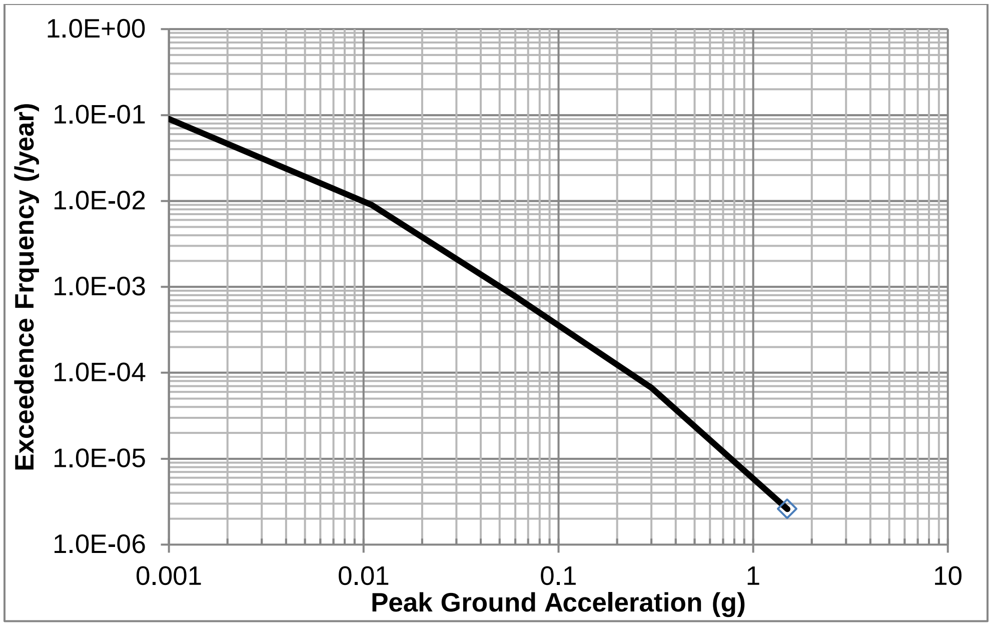


Figure 11: Example Seismic Hazard Curve

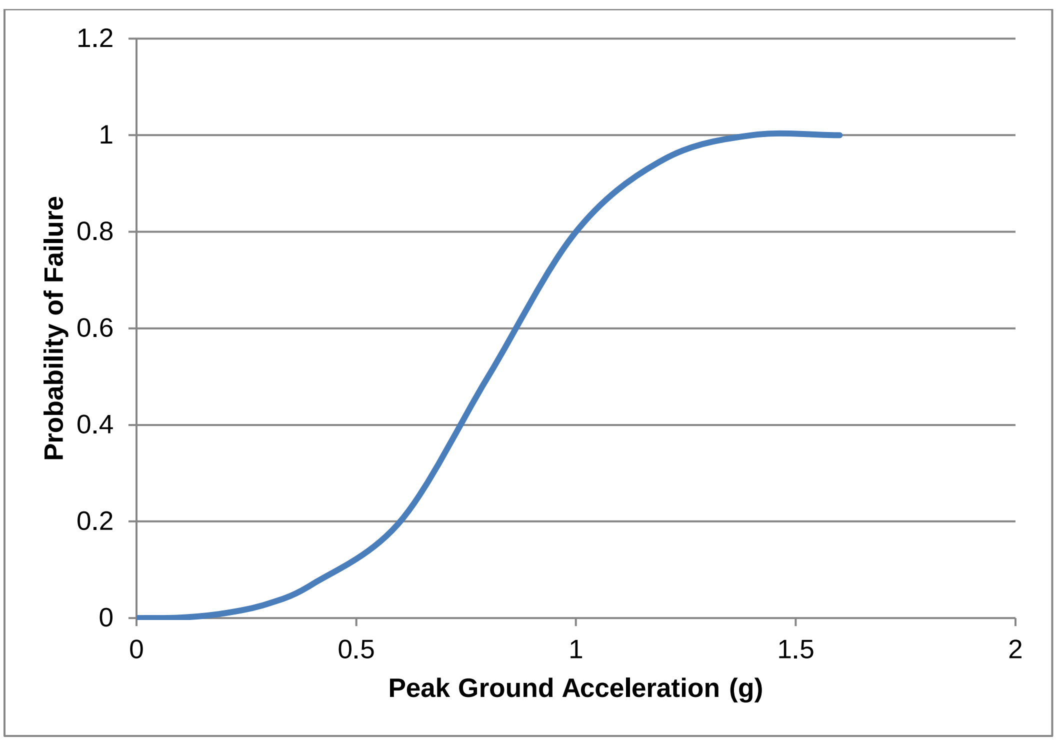


Figure 12: Example Fragility Curve

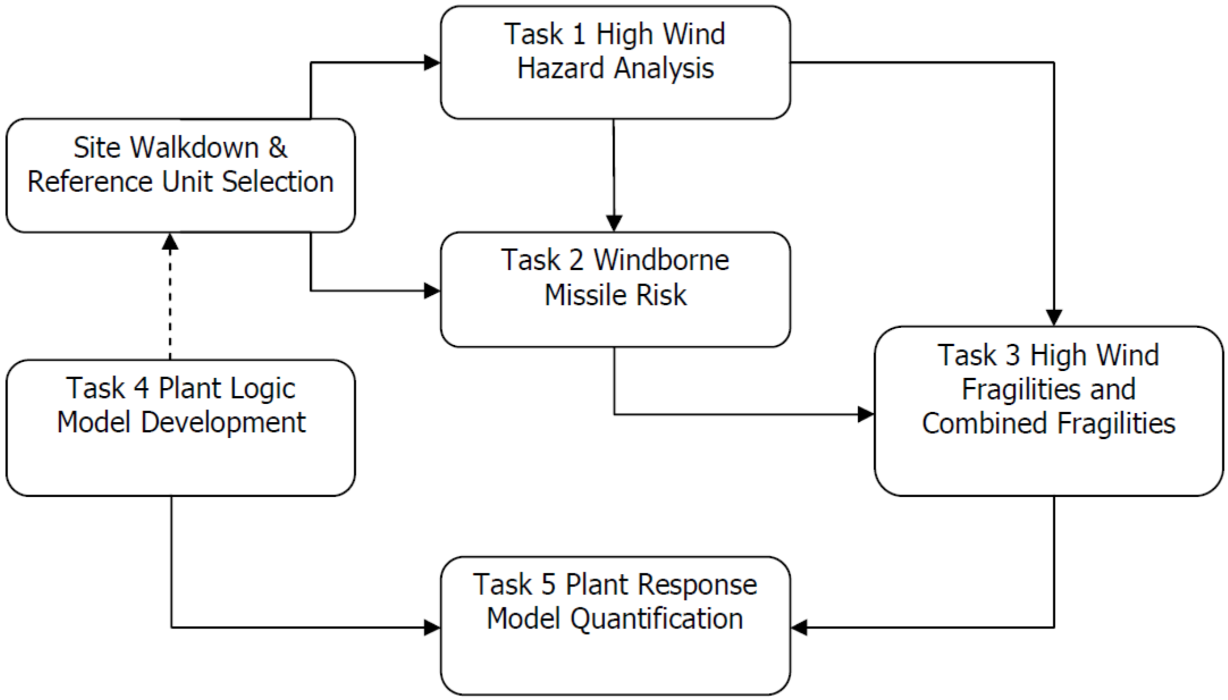


Figure 13: High Wind Hazard PSA Tasks

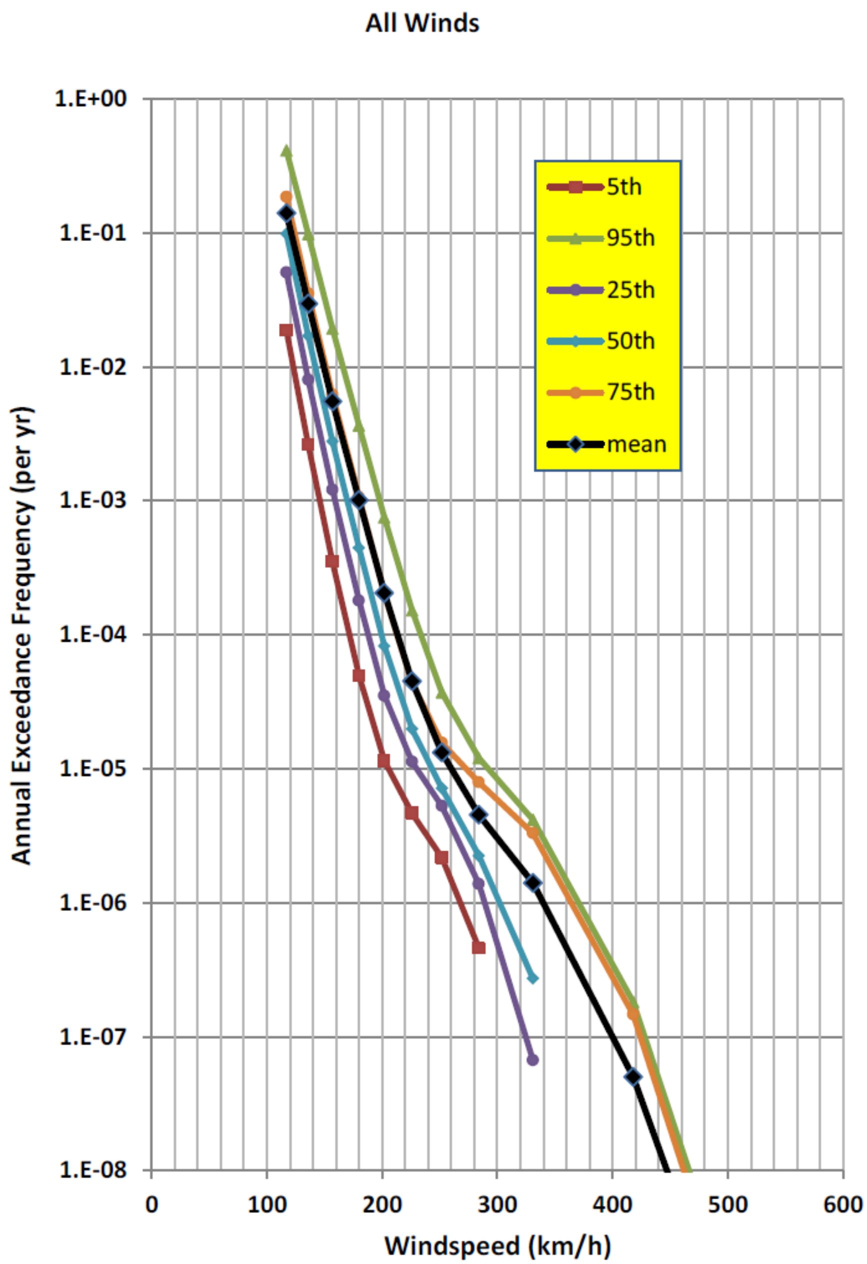


Figure 14: Pickering NGS A High Wind Hazard Curve

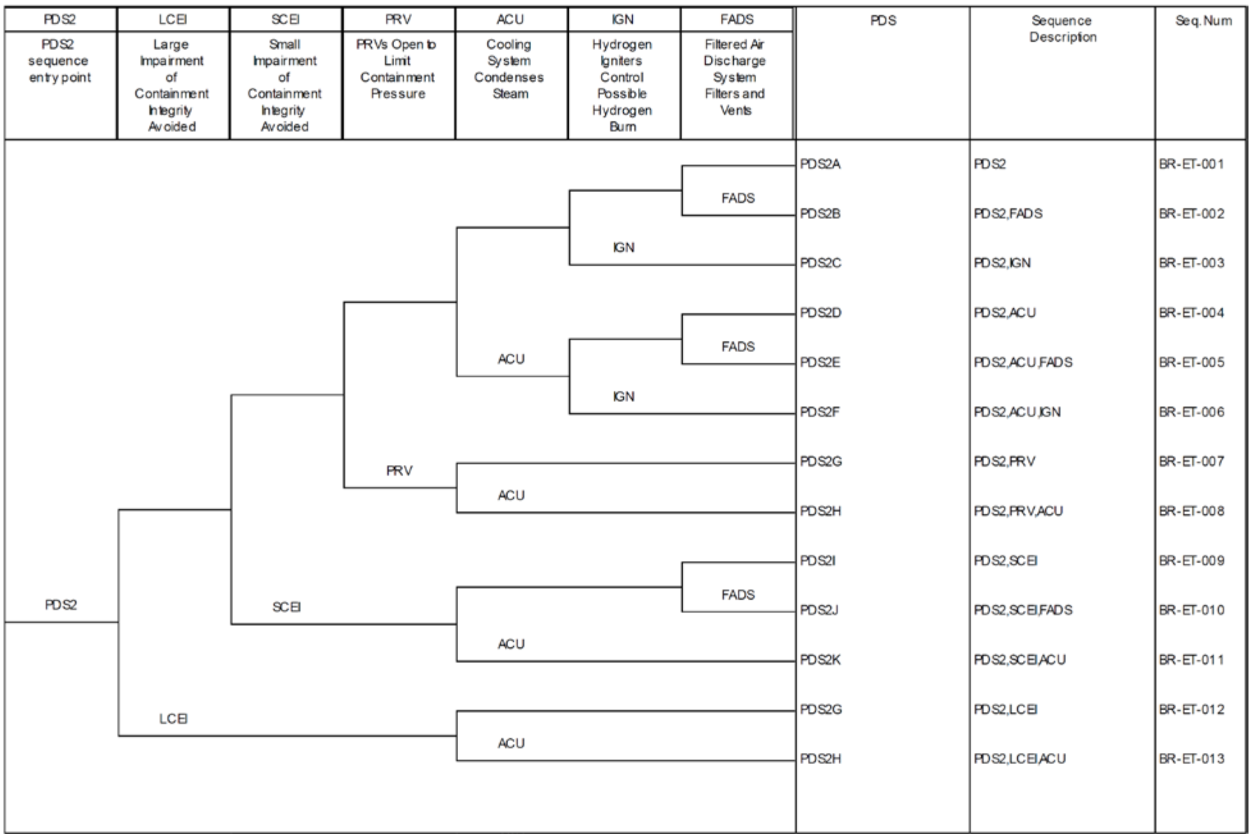


Figure 15: Pickering NGS A Bridging Event Tree

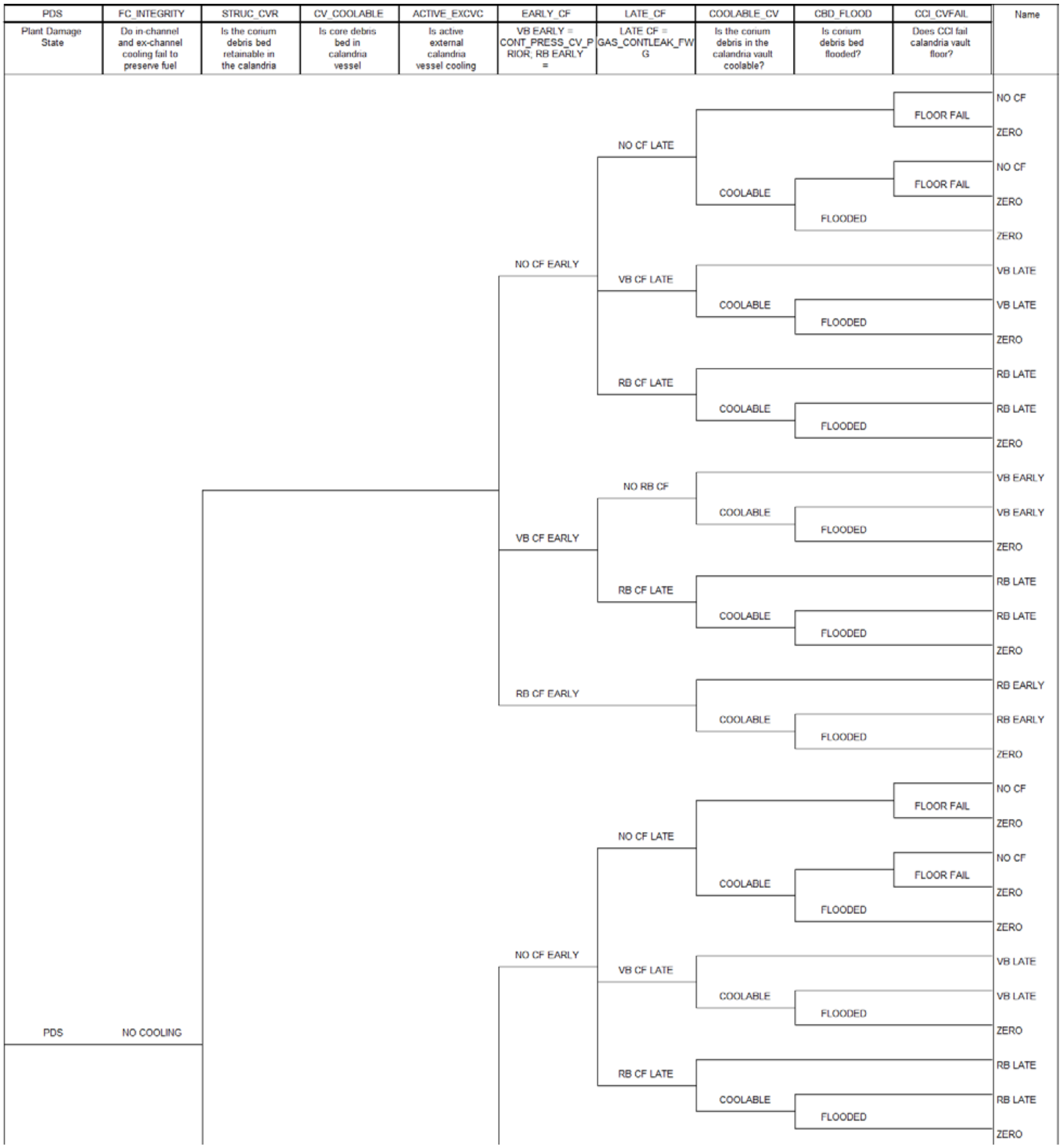


Figure 16: Generic Containment Event Tree

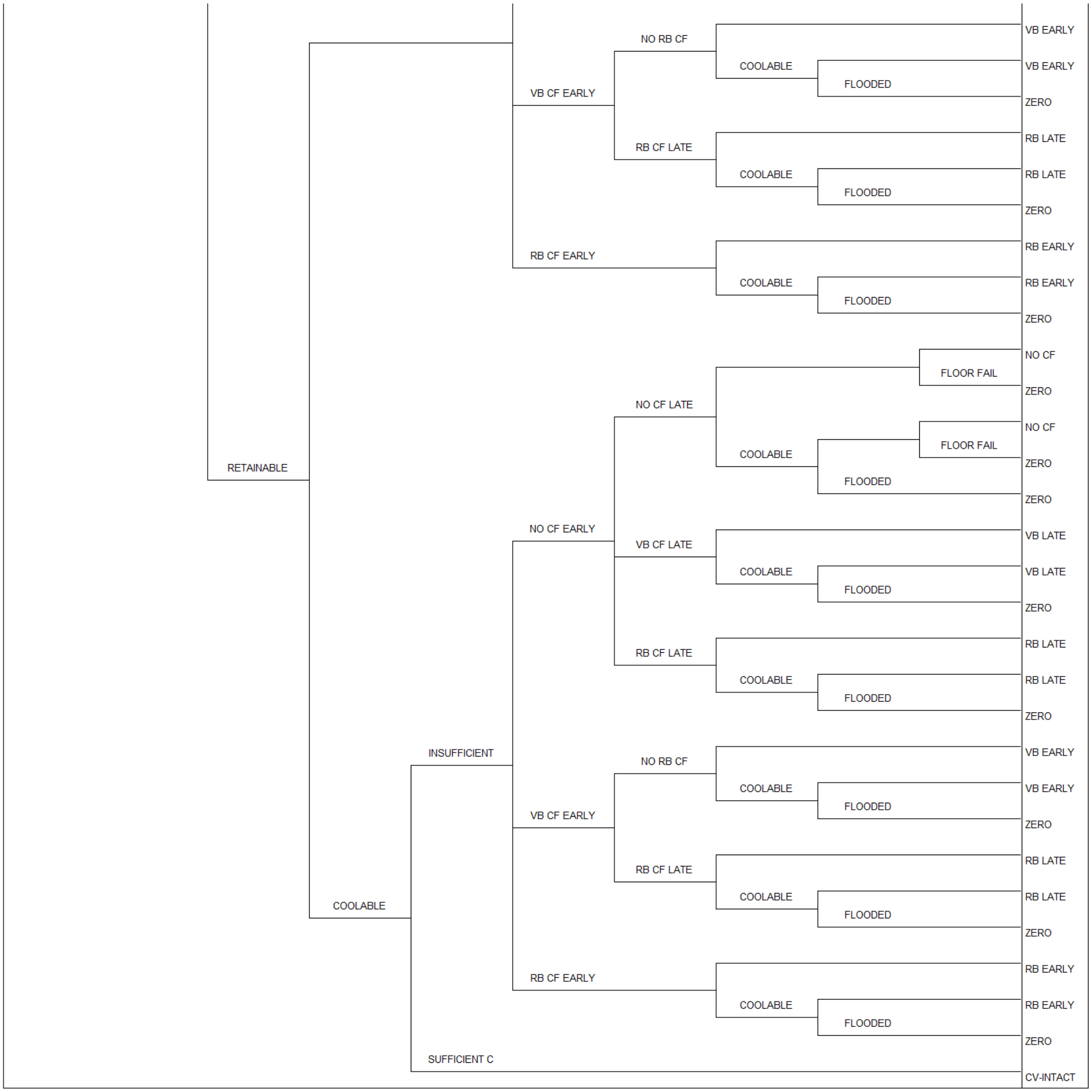


Figure 16: Generic Containment Event Tree (cont'd)

Table 1: OPG Risk Based Safety Goals

Criteria	Average Risk (per year)	
	Administrative Safety Goal	Safety Goal
Severe Core Damage[1] (per unit)	10^{-5}	10^{-4}
Large Release[2] (per unit)	10^{-6}	10^{-5}

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

[2] Large Release is a release of airborne fission products from the containment to the environment large enough to require prolonged population relocation.

Table 2: Quantitative Hazard Screening Criteria

Criterion	Description (Note 1,2,3)	Direct Containment Bypass or Failure (Note 4)	Reference
QN1	SCDF < 10^{-6} / yr.	No	EPRI 3002005287 [29]
QN2	Design Basis Hazard Frequency < 10^{-5} / yr. and CCDP < 0.1 (Note 5)	No	EPRI 3002005287 [29]
QN3	SCDF < 10^{-7} / yr.	Yes	EPRI 3002005287 [29]
QN4	Design Basis Hazard Frequency < 10^{-6} / yr. and CCDP < 0.1 (Note 5)	Yes	EPRI 3002005287 [29]
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 for PSA

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.

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	[QN3]
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 – Explosions	[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]
Nearby Nuclear Event	[QL-5]
Fixed Sources – Toxic Gas Release: Ajax Water Treatment Plant	[QL-3]
Fixed Sources – Toxic Gas Release: Duffin 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

External Natural Hazard	Screening Criterion
Earthquakes	Screened in
Slope Instability	No hazard
Subsidence	No hazard
Soil Frost	No hazard
Flooding Due to Runoff	[QN1][QL-6]
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: 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
Loss of HTS Inventory Control	D2OFDL	Pipe break in D_2O feed system upstream of check valve 3331-NV1 or -NV2

Table 5: Initiating Events in the PARA-L1P

Category	Label IE-44-	Description (PARA-L1P)
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 [1]	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

[1] 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.

Table 5: Initiating Events in the PARA-L1P

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 low pressure service water (LPSW)
Forebay event	FOREBAY	Adverse conditions in the forebay
Loss of HPSW System	LOHPSW	Total loss of high pressure service water
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

Table 5: Initiating Events in the PARA-L1P

Category	Label IE-44-	Description (PARA-L1P)
	LO5320BUA	Loss of power to unit Class IV 4.16 kV bus BUA
	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

Table 5: Initiating Events in the PARA-L1P

Category	Label IE-44-	Description (PARA-L1P)
Heat Transport Flow Diversion	SDCMV	Spurious opening of both shutdown cooling isolation valves in one or more quadrants
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

Table 5: Initiating Events in the PARA-L1P

Category	Label IE-44-	Description (PARA-L1P)
ECI Blowback contd.	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)
	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)

Table 5: Initiating Events in the PARA-L1P

Category	Label IE-44-	Description (PARA-L1P)
ECI Blowback contd.	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 6: 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	*

Table 6: 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
Shutdown System E	Y	N	*
Annulus Gas System	Y	Y	*
Digital Control Computer	Y	Y	*
Heating 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	*
Pressure Relief Valves	N	N	Y
Containment Isolation, Airlocks and Hydrogen Ignition System	N	N	Y
Boiler Room and Fuelling Machine Vault Air Cooling Units	N	N	Y
Hydrogen Ignition System	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 7: PARA-L1O Plant Operational States

Input Parameter	Plant Operational State (POS)		
	A	B	C
GSS	Dumped	Dumped	Dumped
HTS Inventory Level	Primary side of all boilers full	Primary side of some boilers drained and isolated	Primary side of all boilers full
HTS Boundary Configuration	Closed	Closed	Closed
Typical HTS Pressure (ROH)	HTS depressurized	HTS depressurized	HTS pressurized
Typical Primary Heat Sink (Circulation)	SDCS pumps	SDCS pumps	SDCS pumps
Typical Primary Heat Sink (Heat Removal)	SDCS HXs	SDCS HXs	Bleed cooler or boilers
Typical Backup Heat Sink (Circulation)	SDCS pumps	SDCS pumps	SDCS pumps
Typical Backup Heat Sink (Heat Removal)	SDCS HXs	SDCS HXs	Bleed cooler or boilers
Emergency Heat Sink	EBWS supply to boilers, heat rejection via SRVs	EBWS supply to boilers, heat rejection via SRVs	EBWS supply to boilers, heat rejection via SRVs
Time Average (days) - Duration per Unit per Year	29.8	42.3	5.11

Table 8: 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
BLOWDOWN	Loss of boiler blowdown	-	-	Y
LEAK1	HTS leak inside containment from depressurized HTS greater than capacity of D_2O make-up	Y	Y	-
LLEAK	Small HTS leak inside containment from depressurized HTS within capacity of D_2O make-up	Y	Y	-
LOCA1	Rupture of pressurized HTS within the capacity of D_2O make-up	-	-	Y
LLOCA	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 outside containment through ECIS piping	-	-	Y
U1LSLB-OC	U1 large steamline break	Y	Y	Y
U5678-LSLB-OC	Large steamline break at Pickering NGS B	Y	Y	Y
U1LFLB	U1 large feedline break	Y	Y	Y
PHFREEZE	Spurious operation of powerhouse venting during cold weather	Y	Y	Y
U15678-BREAK-IC	High energy line break inside containment from any high power unit	Y	Y	Y

Table 8: Initiating Events for PARA-L1O

IE-LABEL	DEFINITION	APPLICABLE POS		
		POS A	POS B	POS C
LOPIC-HIGH	Loss of HTS pressure & inventory control leading to high pressure	-	-	Y
LOPIC-LOW	Loss of HTS pressure & inventory control leading to low pressure	-	-	Y
SDC-INV	Loss of HTS inventory leads to failure of SDCS circulation	Y	Y	Y
LOBES	Loss of off-site power	Y	Y	Y
LOSWYD	Loss of switchyard	Y	Y	Y
LOSST	Loss of System Service Transformers or associated breakers	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 low pressure service water	Y	Y	Y
FOREBAY	Adverse conditions in forebay affects service water supply	Y	Y	Y
LOHPSW	Total loss of high pressure service water	Y	Y	Y
LORCW	Total loss of recirculated cooling water	Y	Y	Y
TLOIA	Total loss of instrument air	Y	Y	Y

Table 9: High Wind Hazard and Wind Speed Ranges

Sub-interval	Wind Speed (km/hr)		Wind Speed Frequency Distribution Parameters (per year)					
	Range	Mid Pt	5th	25th	50th	75th	95th	Mean
F1-1	117 - 137	127	1.61E-02	4.27E-02	8.15E-02	1.50E-01	3.15E-01	1.11E-01
F1-2	137 - 158	147	2.26E-03	6.78E-03	1.42E-02	2.90E-02	7.84E-02	2.41E-02
F1-3	158 - 180	169	3.02E-04	1.03E-03	2.33E-03	5.13E-03	1.57E-02	4.51E-03
F2-1	180 - 203	191	3.82E-05	1.45E-04	3.63E-04	8.65E-04	2.90E-03	8.08E-04
F2-2	203 - 227	215	6.75E-06	2.38E-05	6.25E-05	1.58E-04	5.96E-04	1.60E-04
F2-3	227 - 253	240	2.49E-06	5.98E-06	1.27E-05	2.83E-05	1.15E-04	3.18E-05
F3-1	253 - 285	269	1.71E-06	3.89E-06	4.89E-06	7.67E-06	2.50E-05	8.65E-06
F3-2	285 - 332	308	4.56E-07	1.31E-06	1.97E-06	4.61E-06	7.84E-06	3.13E-06
F4	332 - 418	375		6.67E-08	2.72E-07	3.16E-06	3.98E-06	1.35E-06
F5	>418			2.34E-13	2.08E-12	1.46E-07	1.81E-07	5.01E-08

Table 10: PARA-L2P Plant Damage States

PDS	Representative Accident Sequence
PDS1	No representative sequence required
PDS2A	Not used.
PDS2B	Out-of-core LOCA with failure of moderator cooling, ECIS injection and recovery, and FADS.
PDS2C	Out-of-core LOCA with failure of moderator cooling, ECIS injection and recovery, FADS, and igniters.
PDS2D	Not used.
PDS2E	Out-of-core LOCA with failure of moderator cooling, ECIS injection and recovery, ACUs in the accident unit, and FADS.
PDS2F	Out-of-core LOCA with failure of moderator cooling, ECIS injection and recovery, ACUs in the accident unit, igniters, and FADS.
PDS2G	Out-of-core LOCA with failure of moderator cooling, ECIS injection and recovery, igniters, and FADS, and a large containment envelope impairment.
PDS2H	Out-of-core LOCA with failure of moderator cooling, ECIS injection and recovery, ACUs in the accident unit, igniters, and FADS, and a large containment envelope impairment.
PDS2I	Not used.
PDS2J	Out-of-core LOCA with failure of moderator cooling, ECIS injection and recovery, FADS, igniters, and a small containment envelope impairment.
PDS2K	Out-of-core LOCA with failure of moderator cooling, ECIS injection and recovery, FADS, ACUs in the accident unit and igniters, and a small containment envelope impairment.
PDS3-2U	Secondary side line break with EBWS failure in Unit 4 and a total loss of heat sinks in Unit 1.
PDS3-6U	Total loss of heat sinks in all 6 Pickering units.
PDS4	Multiple steam generator tube rupture, failure of ECIS and moderator cooling.

Table 11: Pickering NGS A Release Categorization Scheme

Release Category #	Description
RC1	Large early release with potential for acute offsite radiation effects and/or widespread contamination (greater than 3% core inventory of I-131/Cs-137).
RC2	Release in excess of 10^{14} Bq of Cs-137 but less than RC1 occurring within 24 hours.
RC3	Release in excess of 10^{14} Bq of Cs-137 but less than RC1 occurring after 24 hours.

Table 12: Summary of PARA Severe Core Damage and Large Release Frequency Results for Internal Events

Model	Severe Core Damage Frequency ($\times 10^{-5}$ per reactor-year)	Large Release Frequency ($\times 10^{-5}$ per reactor-year)
Internal Events At-Power	0.88	0.21
Internal Events Outage	0.39	0.06
OPG Safety Goal	10.00	1.00
OPG Administrative Safety Goal	1.00	0.10

Note 1:
LRF negligible compared to the order of magnitude notation chosen (i.e., x 10^{-5} per reactor-year. See Sections 6.2 and 7.2.

Table 13: Summary of PARA Severe Core Damage and Large Release Frequency Results for Fire, Seismic, Flooding and High Wind Events

Model	Severe Core Damage Frequency (x 10^{-5} per reactor-year)	Large Release Frequency (x 10^{-5} per reactor-year)
Internal Fire At-Power	1.0	0.15
Internal Fire Shutdown	Negligible (Note 1)	Negligible (Note 3)
Internal Flooding At-Power	0.49	0.15
Internal Floods Shutdown	Negligible	Negligible (Note 3)
Seismic At-Power	0.19 (Note 2)	<<0.01 (Note 2 & 4)
Seismic Events Shutdown	Negligible (Note 1)	Negligible (Note 3)
High-Wind At-Power	0.40 (Note 2)	0.11 (Note 2)
High Wind Shutdown	Negligible (Note 1)	Negligible (Note 3)

Notes:

1. The risk for a shutdown unit was shown to be bounded by the risk for an at-power unit. The PSA conservatively assumed that the unit was continuously at-power.
2. The risk was estimated for seismic events / high winds with a return period up to and including 10,000 years.
3. LRF is negligible compared to the order of magnitude notation chosen (i.e., x 10^{-5} per reactor-year). See Sections 6.7 and 7.2.
4. This is the Seismically-Induced Containment Failure Frequency (SCFF) value.

Table 14: PARA-L1P Frequency of Fuel Damage Categories

Fuel Damage Category		Frequency (per reactor-year)
Designation	**Definition**	
FDC1	Rapid loss of core structural integrity	2.7×10^{-7}
FDC2	Slow loss of core structural integrity	8.6×10^{-6}
Severe Core Damage	(FDC1 + FDC2)	8.8×10^{-6}

Table 15: PARA-L2P Release Category Frequency

Release Category	Frequency (per reactor-year)
RC1	2.1×10^{-6}
RC2	(Note 1)
RC3	2.9×10^{-8}
LRF	2.1×10^{-6}

Note 1:

No sequences were assigned to this RC.

Table 16: PARA-L1O Frequency of FDC2 by POS

Fuel Damage Category	Plant Operating State	FDC2-SD (per reactor-year)
FDC2-SD	POS A	1.72×10^{-6}
	POS B	1.29×10^{-6}
	POS C	8.97×10^{-7}
Severe Core Damage	POS A + POS B + POS C	3.9×10^{-6}

Appendix A: Abbreviations and Acronyms

Acronym	Definition
ACU	Air Cooling Unit
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
CER	Control Equipment Room
CET	Containment Event Tree
CNSC	Canadian Nuclear Safety Commission
Cs-137	Cesium-137
CSIM	Core Structural Integrity Maintained
D_2O	Deuterium Oxide (Heavy Water)
DCC	Digital Control Computer
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
GSS	Guaranteed Shutdown State
HCLPF	High Confidence of Low Probability of Failure.
HGL	Hot Gas Layer
HPECI	High Pressure Emergency Coolant Injection
HPSW	High Pressure Service Water
HRA	Human Reliability Analysis
HTS	Heat Transport System
HX	Heat Exchanger
Hz	Hertz (1 Hz = 1 cycle per second)
I-131	Iodine-131

Acronym	Definition
IE	Initiating Event
IFB	Irradiated Fuel Bay
IGN	Hydrogen Igniters
ISTB	Inter-Station Transfer Bus
kg/s	Kilograms per second
km/hr	Kilometres per hour
kV	Kilo-Volts
LCEI	Large Containment Envelope Impairment
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
occ/yr	Occurrences per year
OPEX	operating experience
OPG	Ontario Power Generation
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

Acronym	Definition
PRV	Pressure Relief Valve
PSA	Probabilistic Safety Assessment
RC	Release Category
RCWS	Recirculating Cooling Water System
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
SMA	Seismic Margin Assessment
SRV	Steam Reject Valve
SSC	Systems Structures and Components
TG	Turbine Generator
THERP	Technique for Human Error Rate Prediction
UHRS	Uniform Hazard Response Spectrum
UPS	Uninterrupitble Power Supply
VCE	Vapour Cloud Explosion