ONTARIO POWER GENERATION

Report

OPG Proprietary	
Document Number: NK38-REP-03611-10072	Usage Classification: N/A
Sheet Number: N/A	Revision: R001

Title:
DARLINGTON NGS PROBABILISTIC SAFETY ASSESSMENT SUMMARY REPORT

Darlington NGS Probabilistic Safety Assessment Summary Report

NK38-REP-03611-10072-R001
2015-07-31

Other Reference Number:
PS008/RP/001 R01

OPG Proprietary

Prepared by: A. McNeil for: JULY 31, 2015
W. Wang, P. Eng. Date
Engineer
Risk Management
Amec Foster Wheeler

Verified by: L. Krick July 31, 2015
L. Krick, P. Eng. Date
Senior Engineer
Risk Management
Amec Foster Wheeler

Reviewed by: A. McNeil for: JULY 31, 2015
B. Hryciw, P. Eng. Date
Section Manager
Risk Management
Amec Foster Wheeler

Approved by: for R Harman
S. Kaasalainen, P. Eng. Date
Director
Risk Management
Amec Foster Wheeler

Reviewed by: OPG for Mariana Mussat
G. Khawaja Date Aug 4 2015
Senior Technical Engineer
Nuclear Safety and
Technology Department

Reviewed by: OPG for A. Moisin
S. Bedrossian Date
Senior Technical Engineer
Nuclear Safety and
Technology Department

Concurred by: OPG A. Moisin Aug 04, 2015
A. Moisin Date
Section Manager
Nuclear Safety and
Technology Department

Concurred by: OPG J. Vecchiarelli Aug. 4, 2015
J. Vecchiarelli Date
Manager
Nuclear Safety and
Technology Department

Accepted by: OPG Sorin Aug 4/2015
E. Sorin Date
Manager
Darlington Reactor Safety
Department

Table of Contents

Page

List of Tables and Figures

Page

Revision Summary

Revision Number	Date	Comments
R000	May 2012	Initial issue.
R001	July 2015	Revised for 2015 DARA update.

Executive Summary

The objective of Probabilistic Safety Assessment (PSA) at OPG Nuclear is to provide an integrated review of the adequacy of the safety of the current station design and operation for each nuclear power station. The station PSAs are required to meet the intent of the Canadian Nuclear Safety Commission (CNSC) Standard S-294 [R-1].

A nuclear PSA identifies the various sequences that lead to radioactive releases, assigns them to different categories of consequences, and calculates their frequencies of occurrence. Additionally, the PSA is used to identify the sources of risk and assess the magnitude of radiological risks to the public from potential accidents due to operation of nuclear reactors while at power as well as during outages. 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 Darlington NGS PSA followed a quality assurance plan consistent with Canadian Standards Association standard CSA N286-05, Management System Requirements for Nuclear Power Plants [R-2]. The PSA used 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 [R-3].

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

The baseline Darlington NGS probabilistic safety assessments are documented in several reports:

- A hazard screening assessment identifies the hazards that require assessment in a PSA model.
- The Level-1 and Level-2 internal events at-power 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 seismic PSA assesses the risk of severe core damage from seismic events occurring while the reactor is at full power, and provides an estimate of the risk of large release as a result of seismic events.
- 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 internal flooding PSA assesses the risk of severe core damage from internal floods occurring while the reactor is at full power, and a bounding estimate of large release as a result of internal floods.

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

The severe core damage frequency and large release frequency for each hazard are less than OPG's safety goal limits.

1.0 INTRODUCTION

The objective of Probabilistic Safety Assessment (PSA) at OPG Nuclear is to provide an integrated review of the adequacy of the safety of the current station design and operation for each nuclear power station. The station PSAs are required to meet the intent of the Canadian Nuclear Safety Commission (CNSC) Standard S-294 [R-1].

A nuclear PSA identifies the various sequences that lead to radioactive releases, assigns them to different categories of consequences, and calculates their frequencies of occurrence. Additionally, the PSA is used to identify the major sources of risk and assess the magnitude of radiological risks to the public from accidents due to operation of nuclear reactors while at power as well as during outage. 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 Darlington Nuclear Generating Station (NGS) or Darlington Risk Assessment is referred to as DARA. The DARA studies provide an estimate of the station risk in its current configuration and are required for compliance with 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 Darlington NSG PSA followed a quality assurance plan consistent with Canadian Standards Association standard CSA N286-05, Management System Requirements for Nuclear Power Plants [R-2]. The PSA used 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 [R-3].

Ontario Power Generation has safety goals for severe core damage frequency and large release frequency, Reference [R-4], as shown in Table 1. The intent of these goals is to ensure that the radiological risks arising from nuclear accidents associated with the operation of Ontario Power Generation's nuclear power reactors are low in comparison to risks to which the public is normally exposed. The baseline DARA studies show that the risk from the operation of Darlington NGS is low.

The first Darlington NGS PSA studies for S-294 compliance were completed in 2011. All of the Darlington PSA studies were revised in 2015 as part of the regular update cycle. The updates included:

- Station design, operation, and analysis information up to the study freeze date of December 31, 2013;
- A number of model and documentation enhancements;

- The incorporation of Emergency Mitigating Equipment (EME), which has been implemented as part of OPG's post-Fukushima response; and

- Sensitivity cases to assess the risk benefit of several Safety Improvement Opportunities (SIOs) to be implemented as part of Darlington NGS refurbishment.

The current report summarizes the probabilistic safety assessments of the Darlington NGS described above and compares the results with Ontario Power Generation's Safety Goals as documented in Reference [R-4]. Results are presented for both the baseline study and for a SIO sensitivity case.

1.1 Objectives

The principal objectives of the Darlington NGS Probabilistic Safety Assessment Studies are:

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 it can be used to assist in safety-related decision making.

1.2 Scope

The baseline DARA probabilistic safety assessments are documented in eight separate reports - one hazard screening and seven PSA models, as follows:

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 internal events at-power probabilistic safety assessment, which studies the risk of severe core damage from internal events (e.g., loss of coolant accidents, steam line breaks) occurring while the reactor is at full power; i.e., it considers the challenges to reactor core cooling from accident sequences covering Design Basis Accidents and Beyond Design Basis Accidents while the reactor is at full power. This report is referred to as DARA-L1P.

3. A Level-2 internal events at-power PSA (DARA-L2P), which studies the frequency and composition of releases to the environment from severe core damage occurring due to 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 described in Item 2.

4. A Level-1 internal events outage PSA (DARA-L1O), which studies 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.

5. A seismic PSA (DARA-SEISMIC), which studies the risk of severe core damage from seismic events occurring while the reactor is at full power, and provides an estimate of the risk of large release as a result of seismic events (i.e., earthquakes).

6. An internal fire PSA (DARA-FIRE), which studies the risk of severe core damage and large release from internal fires (e.g., fires caused by station electrical equipment) occurring while the reactor is at full power.

7. An internal flooding PSA (DARA-FLOOD), which studies the risk of severe core damage from internal floods (i.e., pipe breaks of plant systems) occurring while the reactor is at full power, and provides a bounding estimate of large release frequency as a result of internal flooding.

8. A high wind PSA (DARA-WIND), which studies the risk of severe core damage from high wind occurring while the reactor is at full power, and provides an estimate of large release frequency as a result of high wind events.

The Darlington PSA models (reports 2-8 above) do not cover the following potential sources of risk:

- Hazards from chemical materials used and stored at the plant;
- Handling of radioactive material outside containment, i.e., the irradiated fuel storage bay;
- 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 are instead addressed through other screening or deterministic hazard studies, see Section 4.0.

The response of all Darlington NGS units to various initiating events is essentially identical, and it is generally only necessary to model a single unit, with this unit considered representative of all other units. Unit 2 was selected as the reference unit. Design differences between units were not incorporated in the reference model, as they are 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, the Summary Report provides the following:

(a) A short description of the Darlington NGS station and units (Section 2.0);

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

(c) An overview of PSA methods and the Level 1 and Level 2 PSA (Section 3.0) and the methods used for Level 1 Analysis (Section 5.0) and Level 2 Analysis (Section 6.0);

(d) A discussion of the SIO sensitivity case (Section 7.0); and

(e) A discussion of the main results of the DARA studies, including the baseline and sensitivity case (Section 8.0).

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

2.0 PLANT DESCRIPTION

The following subsections provide a short description of the Darlington site and plant.

2.1 Site Arrangement

The Darlington NGS facility consists of four CANDU pressurized heavy water reactor units. The station was designed and constructed in the 1980s to early 1990s, with in-service dates ranging between October 1990 and June 1993. The station has four nuclear reactors, four turbine generators, and associated equipment, services and facilities, shown in Figure 1 and Figure 2. At full power each unit produces 2651 MW(th), generating a net output of 881 MW(e). The electrical output from each reactor-turbine generator set is generated at 24 kV, 60Hz and 0.9 power factor and delivered to the 500 kV switchyard. The turbine-generator set can operate for sustained periods if the reactor power is greater than 30% full power.

Each unit was originally designed and evaluated for a 30-year lifetime. OPG is working towards refurbishment of Darlington, which will extend the life of the station.

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 conventionally steam-driven turbine generator. The associated heat source is a heavy water (D_2O) moderated, pressurized heavy water cooled, natural uranium dioxide fuelled, horizontal pressure tube reactor. This type of nuclear steam supply is used in all electrical nuclear power stations built in the province of Ontario.

2.2 Buildings and Structures

The Darlington NGS contains the following buildings and structures:

(a) Four reactor building structures;

(b) Four reactor auxiliary bays;

(c) A powerhouse comprising four turbine halls, four turbine auxiliary bays, and a central service area;

(d) A vacuum structure;

(e) Four combined cooling and service water pumphouses;

(f) An emergency electrical power and water supply complex, consisting of an emergency service water pumphouse, emergency power supply generator sets buildings, emergency power supply fuel management structures, and emergency electrical rooms and associated tunnels;

(g) Two administrative buildings;

(h) A Water Treatment Building;

(i) Two Fuelling Facilities Auxiliary Areas, including two irradiated fuel bays;

(j) Two standby generator areas;

(k) A Heavy Water Management Building;

(l) Tritium Removal Facility;

(m) Flammable Storage Building;

(n) High-Pressure Gas Cylinder Storage Building;

(o) Sewage Treatment Plant;

(p) Emergency Response Team Facility;

(q) Hazardous Material and D_2O Storage Building;

(r) A Main Security Building and an Auxiliary Security Building; and

(s) Darlington Waste Management Facility.

The general arrangement of the station is shown in Figure 2. The four units at the station are each numbered and referred to as Unit 1, Unit 2, etc. The common equipment is referred to as Unit 0.

The Reactor Building, Figure 3, is a rectangular reinforced-concrete building, which serves as a support and an enclosure for the reactor and some of its associated equipment. The portion of the Reactor Building, which forms part of the containment envelope, is called the reactor vault.

The fuelling duct, which is connected to each of the reactor vaults, runs the length of the station under the vaults. It serves as a connection between the reactor and the Fuelling Facilities Auxiliary Areas at each end of the duct. A pressure relief duct connects the fuelling duct to the vacuum structure.

The containment envelope comprises the four reactor vaults, the fuelling duct, the pressure relief duct, the pressure relief valve manifold, the vacuum structure, the fuelling machine head removal area, and a fuel handling and service area at each end of the fuelling duct.

Each reactor vault is surrounded by a Reactor Auxiliary Bay. This building contains reactor auxiliaries and secondary circuits of low temperature, pressure, and generally of low radioactivity level.

The Central Service Area (CSA) serves the entire station. This area contains maintenance and workshop areas, stores, laboratories, electrical and air conditioning equipment.

2.3 Reactor

The reactor consists of a cylindrical, horizontal, single-walled stainless steel vessel called the calandria. It provides containment for the heavy water moderator and reflector. It is axially penetrated by 480 calandria tubes. These tubes surround the pressure tubes, which contain the fuel and heavy water coolant. The calandria, the two end shields, and the shield tank form an integral, multi-compartment structure which contains the heavy water moderator and reflector, and the light water shielding. The end shields and shield tank (filled with light water) provide part of the building operational shielding, as well as full shielding between the calandria and the reactor vault when the reactor is shutdown (see Figure 4).

2.3.1 Heat Transport System

The heat transport (HT) system consists of two identical loops, one for the north half of the reactor and one for the south half. Each loop consists of fuel channels filled with natural uranium fuel bundles surrounded by pressurized heavy water, steam generators, circulation pumps and associated piping and valves. The coolant in the fuel channels removes the heat generated by the fuel. During normal operation the heat from the fuel is generated via the nuclear fission; following shutdown heat is generated from the fuel via fission product decay. The circulating coolant transports this heat to the four steam generators. This is the primary heat sink for the reactor; thus, the system is often referred to as the primary heat transport system.

The heat transport system interfaces with a number of systems: the shutdown cooling system, which removes decay heat when the reactor is shut down; the feed and bleed system, which provides pressure and inventory control for the coolant; the D_2O recovery system, which recovers heavy water from leaks; and the emergency coolant injection system, which adds light water after the occurrence of a loss of coolant accident beyond the capacity of the D_2O recovery system.

2.3.2 Steam and Feedwater System

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

2.3.3 Inter-Unit Feedwater Tie System

After an accident, if the normal feedwater supply to the steam generators is unavailable, the Inter-Unit Feedwater Tie (IUFT) system can provide a short-term source of water to the accident-unit steam generators. Along with the safety relief valves, the IUFT can be used to cool the heat transport system. The water is supplied by the feedwater system of an adjacent unit using a header that runs the length of the station. Feedwater supply to IUFT can come from the auxiliary feed pumps in any of the units. The IUFT system is automatically started when the water level in a steam generator drops below a set level.

2.3.4 Steam Generator Emergency Cooling System

The Steam Generator Emergency Cooling System (SGECS) provides an interim water supply to the steam generators. The automatic injection of SGECS water will maintain the steam generators as effective heat sinks for the heat transport system until such time as the emergency service water system is available.

SGECS is comprised of two water tanks and two air accumulators, with associated valves and piping. Each water tank is pressurized by one of the air accumulators and supplies water to two steam generators. The water tanks are filled with demineralized water from the feedwater system.

2.3.5 Steam Relief System

The steam relief system protects the steam generators from overpressure and is also used for rapid cooling of the primary heat transport system when needed. Three types of valves can be uses to reject steam from the steam generators: the atmospheric steam discharge valves (ASDVs), the condenser steam discharge valves (CSDVs), and the instrumented steam relief valves (ISRVs). The ASDVs and ISRVs discharge steam into the atmosphere. The CSDVs discharge steam into the condenser, where the steam is condensed and returns to the feed cycle.

2.3.6 Shutdown Cooling System

The shutdown cooling system (SDC) provides an alternative method to remove decay heat from the primary heat transport coolant when the reactor is shutdown. The system consists of a set of pumps and heat exchangers that are normally isolated from the primary heat transport circuit, but can be connected when needed. The shutdown cooling system has a much smaller capacity to remove heat than the steam generators, as the reactor produces significantly less heat in the shutdown state. The shutdown cooling system is the preferred heat sink when the unit is in the Guaranteed Shutdown State (GSS).

2.3.7 Moderator System

During normal plant operation the moderator system is used to slow the neutrons produced by fission in order to sustain the chain reaction and maintain criticality. Additionally, a small fraction of the heat produced by the fuel is transferred to the moderator during normal at-power operation. The moderator system includes heat exchangers to remove this heat. After an accident, the moderator can be used as an additional heat sink to remove decay heat from the reactor. This additional heat sink is an important, unique feature of the CANDU reactor design.

2.3.8 Unit Control System

Each unit is operated and controlled independently by a dual digital control computer system. Important process variables and devices controlled by the dual computer system include:

(a) Reactivity control devices, which includes the liquid zone control valves, the adjuster, absorber and shut-off rods, and gadolinium poison addition into the moderator;

(b) Primary heat transport pressure and inventory control components such as the D_2O liquid feed and bleed valves, the D_2O steam bleed valves, and the pressurizer heaters;

(c) Steam generator level control system components such as the two large and one small level control valves per steam generator;

(d) Steam generator pressure control components such as the turbine governor valves, the CSDVs and the ASDVs; and

(e) Moderator temperature control system components such as the three temperature control valves in the service water side of the moderator heat exchangers.

2.3.9 Powerhouse Steam Venting System

The Powerhouse Steam Venting System (PSVS) is designed to vent steam from the powerhouse in the event of the secondary side piping failure, minimizing the effect of harsh environment on the equipment located in the powerhouse. The system consists of wall mounted, air and spring operated dampers of louvers located at a lower elevation on the powerhouse north wall and at a high elevation on the Reactor Auxiliary Bay walls, and dampers of gravity ventilators located on the roof of the Turbine Hall. The dampers of the louvers and gravity ventilators open automatically on a high temperature signal. The open flow areas at high elevations provide an escape route for steam, while the make-up air is supplied by the open dampers at the lower elevation.

2.3.10 Special Safety Systems

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

(a) Shutdown System No. 1 (SDS1);

(b) Shutdown System No. 2 (SDS2);

(c) Emergency Coolant Injection (ECI) System; and

(d) Negative Pressure Containment (NPC) System.

2.3.11 Shutdown System No. 1

The primary method of quickly terminating reactor operation is the release of 32 gravity-drop, spring-assisted, neutron-absorbing shut-off rods. The shut-off rods are housed in 32 assemblies positioned vertically through the reactor core, with the rods themselves above the core during high power operation. The SDS1 system employs an independent, triplicated system which senses the requirement for reactor trip and de-energizes direct current clutches to release all of the shut-off rods into the reactor core.

2.3.12 Shutdown System No. 2

The second method of quickly terminating reactor operation is the rapid injection of neutron-absorbing gadolinium nitrate solution into the bulk moderator through eight horizontal nozzles. The SDS2 employs an independent, triplicated system which senses the requirement for this rapid shutdown and opens fast-acting helium injection valves to force the gadolinium nitrate poison into the moderator.

The gadolinium nitrate solution is stored in eight tanks, connected to a horizontal injection nozzle in the calandria by stainless steel piping. Helium under pressure is stored in a tank that is isolated from the gadolinium nitrate tanks by a duplicated set of quick-opening valves. Opening of the valves causes the helium to pressurize the poison tanks, forcing the gadolinium nitrate solution through the injection nozzles and into the moderator.

2.3.13 Emergency Coolant Injection System

The emergency coolant injection system automatically provides make-up cooling water to the heat transport system following a postulated loss-of-coolant accident (LOCA). The system also provides one of the long-term heat sinks for emergency core cooling. The ECIS, with most of its major equipment centralized in the central service area, is designed to serve all four units.

The ECIS does not operate during normal plant operation, but is in a poised standby mode.

For the initial high-pressure ECI injection, light water coolant is drawn from the injection water storage tank and pumped to the affected unit. Upon depletion of the water stored in the injection water storage tank, a recovery mode (long-term injection) is established manually. During this long-term injection phase, a mixture of light (ECI) water and heavy (heat transport) water is drawn from the recovery sump in the pressure relief duct and is recirculated to the affected heat transport system. The Post-Accident Water Cooling System (PAWCS) can be used to cool the recirculated water, providing a long term heat sink.

2.3.14 Containment Systems

The containment system is a special safety system that forms an envelope around the nuclear components of the reactor and the reactor coolant system. It is composed of a number of systems and subsystems whose collective purpose is to prevent a significant release of radioactive material, which may be present in the containment atmosphere following certain postulated accident conditions, to the outside environment. The physical barrier, which minimizes the outflow of radioactive material, is called the containment envelope, and the system whose main purpose is to prevent the design pressure of the containment envelope from being exceeded following an accident is called the containment system. The containment system includes provisions for controlling and maintaining a negative pressure within the containment envelope before and after accidents. The containment system quickly reduces the containment pressure to a subatmospheric level following a large energy release within containment and, hence, minimizes uncontrolled releases to the outside environment. Containment includes an Emergency Filtered Air Discharge System (EFADS) to maintain containment at a sub-atmospheric pressure in the long term following an accident, while providing a filtered discharge path to minimize long-term radioactive releases to the environment.

2.3.15 Support Systems

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

2.3.15.1 Electrical Power Systems

The electrical system of the Darlington NGS is designed to satisfy the high reliability requirements of nuclear systems. The design features dual (odd and even) bus arrangements for both unit and common systems, high capacity standby power supplies, and ample redundancy in equipment. There are four distinct classes of power (Classes IV, III, II, and I), as well as the Emergency Power Supply (EPS).

Class IV power is the main site electrical power supplied from a combination of the provincial electrical grid and the station generating unit transformers; Class III power is typically supplied by Class IV power, but has backup supplies and includes four standby generators; Class II is an AC power system to supply control and monitoring systems and is supplied by Class I power via inverters; Class I is a DC power system to supply control and monitoring system. Class I has battery backup supplies.

EPS is a separate power system consisting of its own on-site power generation (two Emergency Power Generators (EPGs)) and AC and DC distribution systems whose normal supply is from the Class III power system. The purpose of the EPS system is to provide power to selected safety-related loads following events postulated to impact the normal Class IV / III / II / I power distribution, including events that impact more than one unit.

2.3.15.2 Service Water Systems

The service water systems provide cooling water for various loads. The service water systems for Darlington NGS consist of:

(a) Low Pressure Service Water System: Each unit has a Low Pressure Service Water (LPSW) system taking untreated lake water from the forebay. This water is used to cool loads at low elevations. After passing through the various loads, the water is returned to the lake via the condenser cooling water discharge duct.

(b) Powerhouse Upper Level Service Water system: The Powerhouse Upper Level Service Water (PULSW) system supplies tempered water of 10°C in winter and untempered lake water in summer from the LPSW system to various continuously used equipment. This system serves all loads where potential heavy water freezing is a problem, as well as loads located at high elevations in the reactor building that are beyond the maximum pressure available from the LPSW system.

(c) Recirculated Cooling Water System: The Recirculated Cooling Water (RCW) system is a unitized closed loop system which supplies demineralized water to continuously used equipment. This system supplies cooling water to certain vital equipment requiring treated water, at a temperature above the freezing point of heavy water, at a pressure sufficiently high to prevent localized boiling in certain heat exchangers, and of a quality sufficiently high to minimize corrosion, fouling, and activation by radiation.

(d) Emergency Service Water System: The Emergency Service Water (ESW) system is independent and physically separated from the normal water systems. It is primarily used to supply cooling water to essential safety-related loads when normal service water supplies are unavailable. One ESW system supplies the required loads for all four units. So that this system does not remain dormant for long periods of time, it is used to supply the normal requirements of the irradiated fuel bay heat exchangers, secondary control areas (Group 2 ventilation), the Auxiliary Service Water System, and the fire water supply.

(e) Circulating Water System: The Circulating Water system is an open loop system to supply cooling water to the condensers to maintain the design backpressure of the turbine exhaust during full load operation. The circulating water is discharged back to the lake through the discharge duct.

(f) Auxiliary Service Water System: The auxiliary service water system supplies water for cooling purposes in the Central Service Area and other common areas. The system is supplied from the ESW system.

(g) Demineralized Water System: This system supplies make-up water to systems using demineralized water including RCW and the condensate make-up system.

(h) Domestic Water System: This system supplies hot and cold potable water to domestic fixtures in the station including the drinking fountains, showers, washrooms, and kitchens.

Failures of the last three systems are not analyzed in detail as part of the PSA assessment.

2.3.15.3 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 and inflating airlock seals. Each unit has its own air supply, with certain key loads supplied by backup air from bottles, to ensure operability in the event of failure of the normal supply. On loss of unit instrument air, instrument air supply from another donor unit can be valved in manually via an inter-unit tie.

In addition, the station has a common instrument air system to supply the central service area, fuelling facilities auxiliary areas, vacuum structure, pumphouses, water treatment building, heavy water management building, and ESW pumphouse.

The service air system supplies compressed air to all areas in the station including the service area and other buildings. In addition, the service air system supplies the air requirements of the common instrument air system.

2.3.15.4 Powerhouse Ventilation System

The powerhouse ventilation system provides heating and cooling to the station buildings. Failures of this system are studied for the steam protected rooms in the powerhouse, reactor auxiliary bay and reactor building. Failure of the cooling and ventilation in these rooms may result in equipment failures in the support or mitigating systems.

2.3.15.5 Emergency Mitigating Equipment

As a result of Fukushima, OPG has implemented Emergency Mitigating Equipment (EME) for Darlington NGS. The EME was designed to cope with a total loss of heat sink caused by an extended loss of all AC power. EME also provides an additional mitigating function for a variety of accident sequences considered in the DARA studies that involve a total loss of heat sinks due to other causes.

The intent of EME is to restore selected reactor cooling and monitoring functions as much as possible using temporarily installed and portable equipment. The available equipment for Phase I EME consists of the following:

(a) EME Generator: A 150 kW 600V diesel generator.

(b) 2 large diesel pumps each with suction, discharge hose and manifold to supply steam generators and moderator.

(c) 2 small diesel pumps each with suction, discharge hose and manifold to supply heat transport system, steam generators and IFBs.

(d) Portable Uninterruptable Power Supplies (PUPSs) are provided for each Unit and Unit 0 to power instruments for essential EME parameters, prior to the depletion of the EPS and Class I batteries. Control Maintenance will connect the PUPSs to the instruments, to provide additional coping time and allow intermittent monitoring until the Generator is placed in service.

2.4 Two-Group Separation

The Darlington NGS design uses group separation to minimize the possible consequences of events that could cause widespread damage, and to provide defence in depth. Each group contains equipment to shut down the reactor, remove decay heat, and monitor the reactor status. The Group 1 and Group 2 systems are physically separated.

The following systems are Group 1:

- SDS1: Shutdown System No. 1
- SDC: Shutdown Cooling
- IUFT: Interunit Feedwater Tie
- FW: Feedwater
- Class IV, III, II, I Electrical Power
- Instrument air (normal distribution)

The Group 1 control functions are performed from the main control room (MCR).

The following systems are Group 2:

- SDS2: Shutdown System No. 2
- ISRVs: Instrumented Steam Relief Valves
- EPS: Emergency Power Supply
- SGECS: Steam Generator Emergency Cooling System
- ESW: Emergency Service Water
- ECI, PAWCS: Emergency Coolant Injection and Post-Accident Water Cooling System
- Containment
- EFADS: Emergency Filtered Air Discharge System

The Group 2 systems are seismically qualified to withstand a design basis earthquake (DBE) and designed to withstand the severe atmospheric conditions created by the design basis tornado. The Group 2 controls functions are performed from secondary control areas.

3.0 OVERVIEW OF PSA METHODS

Probabilistic safety assessment is based on the idea that the product of the frequency of occurrence of an event and the consequence of the event represents a useful and meaningful quantity. This product is defined to be the risk from the event and is expressed in units of consequence per unit of time. For example, consider a residential sump pump that fails on average once every four years. If the consequence of the pump failing is $1000 in property damage, then the average risk from failure of the pump is $250 per year.

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

For a nuclear generating plant, the events studied are those leading to damage to fuel in the core or releases of radioisotopes into the environment. Consistent with the requirements of S-294 [R-1], Ontario Power Generation has completed hazard screening, Level 1 and Level 2 PSA to assess the risk from Darlington NGS:

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

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

Level 1 probabilistic safety assessments have been prepared for full reactor power operation for the following types of initiating events based on the hazard screening results:

- Internal initiating events (e.g., steam line break, loss of coolant accidents);
- Seismic events;
- Internal Fire (fires initiated by in plant sources, e.g., electrical equipment);
- Internal flooding (floods originate from water sources internal to the plant); and
- High winds (including both straight line winds and tornadoes).

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

- An outage seismic PSA was not performed as the risk from a seismic event while a single unit is shutdown is bounded by the risk from seismic event while all units are at high power. The accident progression is slower when the unit is in outage, giving more time for operator action; and the time at risk while the unit is in outage is small compared to the time at-power. Thus, the risk is smaller for outage.

- An outage high wind PSA was not performed as the risk from a high wind while a single unit is shutdown is bounded by the risk from high wind event while all units are at high power. The accident progression is slower when the unit is in outage, giving more time for operator action; and the time at risk while the unit is in outage is small compared to the time at-power. Thus, the risk is smaller for outage.

- An outage internal fire PSA was not performed as the overall risk of severe core damage due to fire while the unit is at-power is low; the time at risk during an outage is small; and the risk management controls during outage limit the risk of an internal fire.

- An outage internal flood PSA was not done as the overall risk of severe core damage (SCD) due to flooding is low. The low risk of SCD due to flooding is due to the low initiating event frequency, the physical separation of the Group 1 and Group 2 systems and the separation of odd and even equipment. As these factors are the same from both at-power and outage operation, a low at-power risk of SCD implies the outage risk will also be low.

The full scope Level 2 PSA has been prepared for at-power internal events. Limited scope Level 2 assessments have been prepared for seismic events, outage internal events, fire events, internal flooding, and high wind as follows:

- The Level 2 assessment for seismic events considers the likelihood of consequential failure of containment due to an earthquake, and then provides a bounding assessment of large release frequency due to seismic failure modes of containment following severe core damage caused by a seismic event.

- The Level 2 assessment of outage internal events reviews the potential for unique containment challenges or bypass pathways in the outage state caused by severe core damage from an internal initiating event occurring while the reactor is in the guaranteed shutdown state.

- For the Level 2 assessment of fire events, the fire scenarios are screened based on frequency, and potential impact on containment functionality. The scenarios that are not screened out are used to calculate an estimate of large release frequency.

- Level 2 assessment for internal flooding was not performed due to the very low frequency of severe core damage caused by these events.

- The Level 2 high wind assessment considered the potential failure of containment systems due to wind impacts. Large release frequency is then estimated based on the types of sequences that appear in the high wind results.

In the following sections, the methods used for hazard screening, Level 1 PSA, and Level 2 PSA are described.

4.0 HAZARD SCREENING METHODS

A hazard is an event or natural phenomenon that has the potential to pose some risk to 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 probabilistic safety assessment, and identify which hazards need to be assessed by a PSA.

4.1 External Hazards 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:

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.

The hazard screening flow diagram of steps is shown in Figure 5. 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 criterion 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 IAEA, 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.

At this stage of the screening, all qualitative criteria are examined and if the hazard still has not been screened out by any of the seven deterministic criteria, quantitative screening would be required. The OPG Guide for External Hazard Screening recommends using the EPRI criterion for quantitatively screening of external events, using the initiating event frequency, as shown below.

[QN1] The frequency of the hazard is less than 10^{-6} per year, unless there is evidence that this frequency is near a cliff edge effect. If so, the hazard may be screened out if the frequency is less than 10^{-7} year.

Once a hazard has been subject to all qualitative and quantitative criteria, a more detailed assessment using PSA is recommended.

4.1.2 Human-Induced External Hazards

All human-induced (man-made) external hazards identified for the Darlington NGS, were reviewed and examined against the methodology described in Section 4.1.1. All human-induced hazards are screened out, and do not require a PSA. A list of the human-induced hazards assessed is presented in Table 2.

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 the 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:

a) Canadian and International regulations and standards, and

b) Information on credible hazards at the plant site.

c) 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 described Section 4.1.1. A set of RLCs were defined and used in the screening analysis. Among the twenty five natural hazards assessed, all of them were screened out, except earthquake, tornado, and high wind as they may cause some potential damages to certain SSCs, which may have impact on Group 2 systems. A list of the natural external hazards considered is presented in Table 3. Seismic and high wind (including straight-line winds and tornados) PSA assessments were performed; see details in Section 5.5 and Section 5.6, respectively.

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 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, man-made hazards with other man-made 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. The combined hazard assessment did not identify any hazard combination that requires a PSA assessment.

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:

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. Determine likelihood of event occurring. Screen-out events quantitatively, based on the likelihood of event occurring.

The screening flow diagram of steps is the same as for the external events as shown in Figure 5. 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 Darlington PSA studies, the hazard screening only considered internal hazards not already assessed in DARA.

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. In order to conduct the quantitative screening the hazard's mean frequency and its uncertainty need to be estimated. If the frequency of the hazard is greater than the Screening Frequency Level (SFL), the hazard is screened in and need to be assessed by PSA. The SFL value for the screening analysis is taken as 10^{-6} occ/yr. This SFL also aligns the station's safety goal target for LRF and has been widely used in numerous S-294 PSA analyses.

4.2.2 Internal Hazards Screening Results

The internal hazards identification included mechanical, chemical, electrical hazards, initiated from the inside of the plant (such as turbine missiles, load drops, accidental release of chemicals, and electromagnetic interferences). The internal hazards identified are listed below:

- Mechanical missile impact;
- 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 impact (e.g., vehicles, movement of toxic on-site goods);
- Electromagnetic interference; and
- Static electricity.

The above internal hazards were assessed and all of them were screened out, some based on the consequences (qualitatively) and some based on their extremely low probability of occurrence (quantitatively). Internal hazards for which a PSA already exists were not considered. As a result of the screening assessment, no new internal hazard was identified to be included in the Darlington PSA.

5.0 LEVEL 1 PSA METHODS

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

Typically, the first PSA study for a station will be a Level 1 At-Power internal events PSA. 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 and Level 2 At-Power PSA models were used to aid in the development and quantification of the internal events outage, seismic, fire, internal flooding and high wind PSAs.

5.1 Level 1 At-Power Internal Events

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

The major activities of a Level 1 Internal Events PSA are listed below:

(a) Identification of initiating events based on a review of station operating experience and knowledge gained from previous probabilistic safety assessment studies. The identification of initiating events is discussed in Section 5.1.1.

(b) Development of a scheme to group sequences into a manageable number of consequence categories based on degree of fuel damage, as discussed in Section 5.1.2.

(c) Development of event trees. Event trees are a tool that establishes what consequences can occur from a particular initiating event, given success or failure of the systems credited with mitigating the initiating event. Development of the DARA 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 (including support systems that interface with the mitigating systems). The development of the fault trees is discussed in Section 5.1.4.

(e) Development of a component reliability database with, to the extent possible, information specific to Darlington NGS. The reliability database is needed to support the fault tree analysis mentioned above. The sources for the data in the component reliability database are discussed in Section 5.1.4.

(f) Assessment of the effect of human error on system performance using Human Reliability Analysis (HRA). The potential for human errors must be incorporated along with hardware failures in the system level fault trees and event trees, and the human error probabilities systematically estimated and assigned. Human errors are referred to as “human interactions” in DARA. The HRA is discussed in Section 5.1.5.

(g) Integration of event trees with the system fault trees, and risk quantification. This step combines the accident sequences described in the event trees with the system logic contained in the system fault trees to produce integrated fault trees representing each of the fuel damage categories. The integration process is described in Section 5.1.6.

Although the above listed tasks are carried out in the indicated order, the process is iterative in nature and entails re-assessing the results of a previous task based on insights gained from a subsequent one.

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

5.1.1 Initiating Events Identification and Quantification

An 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 and quantifying the initiating events is the first step in the Level 1 PSA process.

In DARA-L1P, consistent with the above definition, the initiating events under consideration are primarily those plant failures that could lead directly, or in combination with other failures, to damage to fuel in the reactor. The list of DARA initiating events includes events leading to a hostile environment in the powerhouse, i.e., steam line breaks and feedwater line breaks. In addition, consideration is given to initiating events leading to damage to irradiated fuel in a fuelling machine while in transit from the reactor to an irradiated fuel port, or to irradiated fuel while being transferred through an irradiated fuel port.

Although DARA-L1P is an internal events PSA, it does include events associated with loss of off-site power (loss of the bulk electrical system) and events leading to failures in the service water intake.

The objective of the initiating event selection task was to obtain as complete coverage as possible of credible initiating events. To create the initiating event list, past Ontario Power Generation probabilistic safety assessments were reviewed, as were the plant operating experience and station condition records, and other published PSAs. In addition, insight from the fault tree modelling, discussed in Section 5.1.4, identified other initiating events.

The complete list of initiating events considered in DARA-L1P is provided in Table 4.

The initiating events are quantified primarily using Bayes' Theorem. In a Bayesian approach, an assessment is made of generic (prior) experience that is then updated by station-specific experience. This technique allows general experience and knowledge about a given event to be combined with actual operating experience gained with the station under study. It is especially useful for quantifying the frequency of events 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 sequence of initiating event and failure of mitigating systems may potentially result in a different end state at the plant. The plant end states will vary in terms of the severity and timing of fuel damage. Fuel damage categorisation is carried out to simplify the subsequent evaluation of consequence and risk. Each Fuel Damage Category (FDC) represents a collection of event sequences judged to result in a similar degree of potential fuel damage. The FDCs are used as end-states in the Level 1 event trees discussed in Section 5.1.3. In addition, groupings of the fuel damage categories are used to transition from the Level 1 PSA to the Level 2 PSA (see Section 6.1).

The range of events or event sequences covered by the FDCs is defined by the scope of DARA. From the event tree analysis described in Section 5.1.3, general types of accident sequences can be identified. They are in general order of decreasing severity of fuel damage:

(a) Sequences with the potential for loss of core structural integrity (severe core damage).

(b) Loss of fuel cooling requiring the moderator as a heat sink.

(c) Prolonged loss of heat sink.

(d) Inadequate cooling to fuel in one or more core passes following a large loss-of-coolant accident with successful Emergency Cooling Injection System initiation.

(e) Sequences leading to fuel damage in one channel with and without an accompanying automatic containment isolation.

(f) Loss of Heat Transport System integrity followed by successful ECI initiation with no significant fuel damage.

The lower consequence threshold for significance is deemed to be the occurrence of a loss of heat transport system integrity resulting in ECI initiation. Although fuel damage is not likely, the event is considered to have the potential for significant economic consequence due to the downgrading of heavy water, and the loss of revenue due to prolonged shutdown of the accident unit. At the other extreme are the unlikely events that have the potential for severe consequences involving the loss of core structural integrity. Table 5 presents the FDCs used in DARA. These FDCs are also used to calculate the frequency of severe core damage, used for comparison to the relevant Ontario Power Generation safety goal. Severe core damage is defined to be the sum of the FDC1 and FDC2 frequencies.

5.1.3 Event Tree Analysis

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

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

These 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 initiating event, usually a plant malfunction. Following the identification of the initiating events, the next step is to consider what systems are required to mitigate the event and show how the accident could progress if failures of the mitigating systems were also to occur, until a previously defined end state is reached.

Event tree analysis requires the following to be predefined:

(a) A list of initiating events to be considered.

(b) Definition of sequence end states.

(c) Definition of mitigating systems.

Figure 6 shows a generic event tree for a large loss-of-coolant accident at a CANDU plant. A LOCA is typically a pipe break in the heat transport system. Following a large LOCA, three systems are postulated to mitigate releases of radioisotopes: the shutdown systems, ECI and the heat sink function of the moderator system. The potential plant state must be assessed if one or more of these systems fail. These three systems form the branch points in the event tree. The event tree is read from the left, starting at the initiating event IE-LOCA. The first systems credited with preventing fuel damage are the shutdown systems. Failure of both SDS1 and SDS2 is represented by the event tree branch point "SD". SDS1 and SDS2 are fast acting, diverse and independent systems. The convention used to interpret an event tree is that success of the system is the top path and failure is the lower. If the shutdown systems fail, rapid loss of core structural integrity is expected. FDC1 is assumed to occur. If reactor shutdown is successful, the decay heat from the fuel must still be removed to prevent fuel damage. Two systems are credited for this function: automatic ECI injection and the moderator as a heat sink. If ECI fails, represented by the event tree branch point "ECI", then the moderator is credited to prevent severe core damage. However, if the moderator system fails, a slow loss of structural integrity is expected. Then the end state is FDC2, one of the fuel damage categories included in the definition of severe core damage. If the moderator system is successful, the less severe FDC3 category is assigned.

If both shutdown and ECI are successful, the end state FDC9 is reached. This category represents no significant fuel damage, and no release to the public, but has significant economic consequences.

Once the Level 1 event trees have been created, the systems that have been identified as mitigating systems in the event tree analysis require fault tree modelling to calculate the probability of failure of the mitigating function. Fault tree analysis is described in the next section.

5.1.4 Fault Tree Analysis

A fault tree (FT) is a logic diagram that models the possible causes of a particular fault, usually a system failure, and is used to calculate the probability that the fault occurs. In DARA, fault trees are used to quantify the probability of the failure of the mitigating systems that appear in the event trees discussed in Section 5.1.3, and for the support systems. Table 6 lists the systems modelled by fault trees in the DARA-L1P study. Figure 7 depicts the relationship between the event trees and fault trees. System fault tree analysis is used to calculate the probability of an event tree branch point given a specific set of events that fail the system.

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

The "CAFTA" software code is used for developing and quantifying the fault tree [R-5].

For example, consider emergency make-up water to the steam generators. For this system, the failure mode of interest might be "fails to supply adequate water to the steam generator when required". Figure 8 shows a partially completed fault tree with this event at the top. Starting from this top event, the fault tree analyst poses the question "*How can this event occur?"*. The answers to this question become the inputs to this top event. For example, Figure 8 shows that ESW to the steam generators can fail if the piping fails due to water hammer, or if there is no flow from check valve NV42. For each of these contributors, the process of examining how they can occur is repeated, until no further insights can be obtained about the behaviour of the system. Typically, the fault tree is developed either to predefined system boundaries, or to the individual system components.

In constructing a fault tree model, a number of design and operational features are assessed.

(a) System capability: For example, how much water flow is required for the steam generator to be a successful heat sink?

(b) Fault detection: For example, if a component has failed, when and how can its failure be detected?

(c) Common cause failures: For example, if a pump has failed due to any number of causes will any of the remaining redundant pumps fail to operate due to the same cause of failure as the first?

(d) Failure criteria: For example, what fundamental failure modes lead to failure of ESW to the steam generators?

(e) Fault tolerance: For example, if the electrical systems have failed, what is the impact on the system?

The basis for system capability and the failure criteria is based on analysis from a variety of sources, including the safety analysis contained in the Darlington NGS Safety Report, Operational Safety Requirements (OSR), Abnormal Incidents Manuals (AIMs), and assessments and regulatory submissions.

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

Once the fault tree is constructed, it is linked with the system reliability database, a database containing the information to calculate the probability of each event in the fault tree. In DARA, failure rate, test and maintenance data are assigned to the fault tree primary events from a central type code table that is linked to the system reliability databases. This type code table defines failure rates for the various components at the Darlington NGS. 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 fault trees.

The nuclear industry has adopted a Bayesian approach for obtaining component failure rates. The Bayesian approach is based on the use of both the "prior knowledge" and the plant-specific data in deriving the failure rates. Three industry sources, U.S. Nuclear Regulatory Commission (NRC) [R-6], T-book [R-7], and Westinghouse Savannah River Company [R-8], were used for obtaining generic data. The DARA component reliability database is based on a Bayesian calculation of the equipment failure rates reflecting Darlington operational data from 1999 to 2013 inclusive.

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.

5.1.5 Human Reliability Analysis

Human errors can affect the performance of systems, and in some cases be significant contributors to risk. Thus, human reliability analysis (HRA) is an important part of DARA. The potential for human errors must be incorporated along with hardware failures in the system level fault trees, and human error probabilities systematically identified and assigned.

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

In principle, every piece of equipment or system in the plant is susceptible to failure because of human error; however, human errors that contribute directly to the failure of individual components are included in the equipment reliability database (i.e., reflected in the component failure rate) and need not be identified in fault trees. The human errors of interest to the fault tree analyst arise under five sets of circumstances:

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

(b) Where an annunciated equipment or system failure occurs but this failure is not responded to by the operator prior to an initiating event;

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

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

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

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

In order to systematically quantify the human interactions in DARA, Ontario Power Generation uses a human interaction taxonomy. This taxonomy classifies the human interactions in DARA-L1P into three parts: Part 1 contains the *simple* interactions that, by definition, occur prior to an initiating event; Part 2 contains *complex* human interactions that occur prior to initiating events; and Part 3 contains the *complex* interactions that occur after an initiating event.

Simple human interactions have the following characteristics:

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

(b) They involve directly manipulated components (e.g., a valve handwheel or a handswitch) or directly viewed main control room display devices.

(c) They occur prior to an initiating event.

The task of assigning preliminary (screening) human error probabilities for the simple human interactions is made easier and faster using a simple method requiring only 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. The simple human interactions are reviewed by the Human Reliability Assessment (HRA) Specialist. In some cases, the probability is requantified using the Technique for Human Error Rate Prediction (THERP) described in Reference [R-9].

For the complex human interactions that occur prior to initiating events, the same process may be followed to obtain a preliminary (screening) quantification. These human interactions are complex because they include system-level functions that involve more than just direct physical manipulation of a component, such as the setting of computer control program parameters or modes. The preliminary quantifications are then reviewed by the HRA Specialist on a case-by-case basis and if required are requantified using THERP methodology described in Reference [R-9].

Post-initiating event complex human interactions usually occur during abnormal conditions and are, therefore, more difficult to identify, analyze, and quantify. Additionally, interactions involved in handling unit upsets are also unlike other interactions as they may take place in dynamic and uncertain situations. Such actions depend upon the cognitive functions of diagnosis and decision-making. These actions are knowledge-based; they are based on fundamental principles of process and safety system operation and on 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: whether the task is straightforward, of average complexity, or very complex; the time available; and the quality of indication available in the main control room to indicate that action is required. The preliminary quantifications are then reviewed by the HRA Specialist. Like the pre-initiating event complex human interactions, in some cases these probabilities are requantified using THERP methodology described in Reference [R-9].

5.1.6 Fault Tree Integration and Evaluation

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

The information required to quantify the fuel damage categories is stored in the fault trees and event trees. In order to combine the two, the event tree logic is converted into fault tree logic with a top event for each fuel damage category. These fault trees are referred to as the high level logic. The events in the high level logic are the initiating events and the branch points from the event trees. The high level logic is then integrated with the mitigating system event trees; the top events in the mitigating system fault trees 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 fault tree. Figure 9 illustrates this process.

The CAFTA software stores and evaluates the fault trees [R-5]. The CAFTA program was developed by Electric Power and Research Institute (EPRI). The FTREX program is used to quantify the results [R-10].

The solution of a fault tree is a listing of the combination of an initiating event, equipment failures, and human errors that leads to the occurrence of the fault tree top event, with each combination containing the minimum number of failures that have to occur to cause the top event. Such combinations are also called minimal cutsets.

The solution of the fault tree calculated using CAFTA is truncated. That is to say, contributors below a certain frequency are not included in the solution. Truncation is necessary because of computational limits. The truncation level selected should be low enough that all significant contributors are captured. The Level 1 At-Power PSA Guide recommends that the solution of the integrated fault tree for each FDC be truncated at either 4 orders of magnitude below the most likely minimal cutset in that FDC or at 1E-12 occ/yr, whichever is the highest. For FDC2, the top cutset frequency is in the 3E-08 occ/yr range, so a truncation of 3E-12 occ/yr is 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:

- Importance analysis to identify systems and components that are important to the FDC results;
- Parametric uncertainty analysis to determine the lower and upper limits of the two-sided 90% confidence interval for the frequency of each FDC; and
- Sensitivity analysis used to evaluate the impact on the results of a number of assumptions made in the event tree analysis and fault tree analysis, as well as assumptions impacting the quantification of initiating events, undeveloped events, and human error events.

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

5.2 Outage Internal Events

DARA-L1P considers internal events occurring at 100% full power operation. However, the Darlington NGS has periods of planned outage to perform routine maintenance and testing that cannot be done during full power operation. Typically, a unit has a planned outage for less than 10% of the operating cycle. The reactor power continues to decrease exponentially after reactor trip. Reactor power is typically around 0.6% full power on the first day of an outage.

The 2011 DARA-L1O assessment was developed following the methodology for preparation of a Level-1 Outage PSA as described in the OPG Outage PSA Guide. The 2011 model was used as the basis for developing the 2015 bounding assessment described in Section 5.2.8.

The Outage PSA uses many of the same techniques as used in the At-Power PSA. The PSA process for outage uses initiating events, event tree analysis and fault tree analysis, like the At-Power PSA. However, different initiating events can occur in the outage state, and the event tree and fault tree must reflect the plant configurations during the outage (e.g. HT system pressurized or depressurized). The plant configurations modelled as part of the outage PSA are typically described as plant operational states (POS).

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

5.2.1 Plant Operational State (POS) Identification and Analysis

The purpose of Plant Operational State analysis is to define the various outage plant scenarios and group them into fewer, representative and bounding states for which the plant status, configurations and system failure criteria are considered sufficiently stable. POS analysis is unique to Outage PSA. During unit shutdown, plant system configurations and parameters are dynamic, changing with respect to time. The dynamic nature of shutdown, specifically system configurations, process parameters and varying system failure mechanisms, result in an excessively large number of unique plant scenarios to be analyzed. In the definition of the POSs, only normally planned plant configurations are considered.

Firstly, Pre-Plant Operational States (Pre-POSs) are identified; Pre-POSs are defined as unique outage plant configurations wherein all parameters of interest (system configuration and parameters, e.g., heat transport system pressure, primary heat sink, HTS pressure) are considered stable for the duration of the state. Pre-POS are the highest resolution of the outage states. The Pre-POSs are grouped into POSs. For DARA-L1O, eight pre-POSs were identified and have been grouped into five representative POSs. The five POSs are used in other aspects of the Outage PSA, including accident sequence analysis using event trees. Table 7 provides a summary of the final POSs used in the DARA-L1O model. The parameters used to define the POSs are listed in the leftmost column.

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 initiating events that could occur during the identified outage POSs. An outage initiating event (IE) is defined as a malfunction that can, either independently or in conjunction with other plant conditions or configurations, lead to fuel damage when the unit is in the guaranteed shutdown state.

The process described below was used to identify, group and quantify outage state initiating events:

- The outage IE identification process uses a number of different steps and different sources of information, so that the basis for the Outage PSA is as comprehensive as possible.

- The identified IEs are grouped on the basis of similar mitigation requirements, in order to simplify the accident sequence analysis.

- The frequency of occurrence of each initiating event (or IE group) is estimated, so that the overall risk of core damage can be calculated.

Table 8 presents the list of outage initiating events for the DNGS Level 1 Outage PSA, and which POS each initiating event can occur in. Some initiating events can occur only in specific plant configurations. For example, ice-plugs are used during some maintenance activities on the HT system, but can only be used while the HT system is depressurized. So the ice-plug failure initiating event can only occur during the POSs with a depressurized HT system (POSB, POSC, and POSD).

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

The event tree process for the internal outage events trees is similar to that used for the at-power event trees described in Section 5.1.3.

The overall process followed to develop the ETs for DARA-L1O is as follows:

1. For each unique IE/POS combination, identify the mitigating systems credited for the IE based on a review of the accident analysis and plant operating procedures.

2. Determine the end states of interest in the ET analysis. For DARA-L1O, these are the outage fuel damage categories as shown in Table 9.

3. Develop the accident sequence logic depending on the success and failure of the mitigating functions credited for the IE.

4. Add the branch point label for each mitigating system failure as the logic is being developed on the failure branch of the ET.

5. Assign a FDC to each ET sequence end state.

5.2.4 Outage System Fault Tree Analysis

The fault tree analysis process for the internal outage PSA is the same as for the at-power PSA. However, the fault tree models are significantly different to reflect the outage configurations of the system.

The system FT models are specific to the outage PSA. Each fault tree includes a brief overview of the system analyzed, top event definitions, assumptions, failure criteria, FT diagram, data table, results expressed as minimal cutsets, system failure probability and importance indices. Table 6 lists the systems modelled by fault trees in DARA-L1O.

5.2.5 Reliability Data Analysis

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

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

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

5.2.6 Human Reliability Analysis

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

While the methodology for quantifying human interactions in the Outage PSA is generally the same as in the At-Power model (see Section 5.1.5), the effort required to identify, quantify and model human interactions in Outage PSA is not trivial. The human interactions during outage states require the consideration of the many testing and maintenance activities, procedures, and manual initiation of certain mitigating systems. The HRA specialist considers the outage POSs and system configurations to better understand required operator actions, recall actions, and possible testing and maintenance activities during a given POS.

5.2.7 Model Integration, Quantification, and Additional Analyses

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

For each consequence category, the magnitude of the associated consequence needs to be calculated. The product of frequency and consequence is calculated for each category and summed to obtain an overall estimate of risk. These are used in absolute terms to assess the overall safety design adequacy, and in relative terms to identify the dominant risk contributors. The acceptability of the Darlington NGS risk estimates is judged based on comparison with the risk-based safety goals and targets established by OPG [R-4].

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:

- Identification of systems and components that are important to the FDC results;
- Parametric uncertainty analysis to determine the lower and upper limits of the two-sided 90% confidence interval for the frequency of each FDC; and
- Sensitivity analysis used to evaluate the impact on the results of a number of assumptions made in the event tree analysis and fault tree analysis, as well as assumptions impacting the quantification of initiating events and undeveloped events.

5.2.8 DARA-L1O 2015 Bounding Assessment

The 2011 DARA-L1O assessment was prepared in accordance with the OPG Level 1 Outage PSA Guide. The 2015 DARA-L1O update is a bounding assessment, undertaken in accordance with the principle in S-294 that the level of detail in a PSA should be consistent with the level of risk.

The overall objective of 2015 DARA-L1O analysis was to demonstrate that the results of the Internal Events Level 1 Outage PSA for DNGS from 2011 are bounding, and to provide an updated severe core damage frequency (SCDF) estimate for 2015 reflecting the current Darlington design and operation to the extent practical for a limited scope bounding assessment. This has been accomplished as follows:

1. A full scope quantitative update was completed for the outage Plant Operational State (POS) parameters (as described in Section 5.2.1), outage initiating event (IE) frequencies (as described in Section 5.2.2), component failure rates, and frequencies of planned test and maintenance procedures (described in Section 5.2.3), based on the incorporation of recent Darlington NGS experience up to the study freeze date of December 13, 2013.
2. The potential impact of event tree and fault tree model changes from the 2015 DARA-L1P study has been qualitatively assessed, with changes made to selected Level 1 Outage event trees and fault trees as necessary.
3. The integrated DARA-L1O model was modified based on the 2015 DARA-L1P to included credit for Phase 1 EME.
4. The integrated DARA-L1O model has been requantified in order to obtain a revised set of baseline cutsets for severe core damage.

5.3 At-Power Internal Fire

The 2011 DARA-FIRE assessment was developed following the methodology for preparation of an Internal Fire PSA as described in the OPG Fire PSA Guide. The 2011 model and analysis were used as the basis for developing the 2015 bounding assessment described in Section 5.3.14.

The OPG Fire PSA Guide has been developed based on NUREG/CR-6850 [R-11]. The major activities of the Fire PSA methodology and its application in the development of the DARA-FIRE assessment are summarized in the subsections below.

An internal fire PSA is built from the internal events PSA for the corresponding plant operational state. The scope of the DARA-FIRE model is limited to internal fires initiated with the unit at power with the potential to cause severe core damage. Internal fires considered are those initiated by component failures and human errors associated with systems inside the plant.

The DARA-FIRE model considers sequences that result in severe core damage. Severe core damage is defined as the sum of the FDC1 and FDC2 frequencies. As shown in Section 7.0, severe core damage at Darlington is dominated by the FDC2 frequency. In the fire PSA, FDC1 sequences (failure to shutdown the reactor) are not assessed due to the low frequency in the internal events model, the fail safe design of the two shutdown systems (SDS1 and SDS2) and the physical separation of SDS1 and SDS2 which makes it unlikely a fire could impact both systems.

The DARA-FIRE analysis used the DNGS Fire Safe Shutdown Analysis (FSSA).

5.3.1 Phased Approach to Fire PSA

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

Phase 1 focuses on areas of the plant that contained cables / equipment from both Group 1 and Group 2. These areas, called pinch points, represent the highest potential for risk-significant fires. The Phase 1 analysis addresses the effect of fires upon Unit 2 and upon common systems and areas (e.g., Emergency Power Generators and Unit 0).

The decision to perform a Phase 2 Fire PSA is based on the risk results from Phase 1 and consideration of the expected additional insights that would be obtained from a full Phase 2 assessment compared to the Phase 1. For Darlington, to obtain a complete understanding of the Fire Risk a full Phase 2 Fire PSA assessment was performed.

The objectives of the Fire PSA were:

- To identify areas of the plant with particular vulnerability to fires while the reactor is at high power;
- Identify fire scenarios that potentially have the greatest contribution to risk while the reactor is at high power;
- Characterize differences between the units that may affect risk;
- Analyze multi-unit fire scenarios; and,
- Provide an estimate of SCDF and an estimate of LRF for both single-unit and multi-unit scenarios.

In the sections below, which summarize the fire methodology, the focus is on the requirements for the Phase 2 analysis.

The fire PSA logic is based on the internal events PSA logic for the forced shutdown event tree. As the fire PSA is developed based on the internal events PSA, the major tasks in the fire PSA are associated with identifying possible fire scenarios, the zones the fires can impact, affected equipment and cables, and quantifying the consequences of the fire scenarios.

The Fire PSA methodology is broken down into 18 tasks:

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

The integration of these tasks is shown in Figure 10. Those boxes in Figure 10 shown in grey are only required for a full Phase 2 analysis. The methods prescribed in the

Fire PSA Guide are iterative. Several of the tasks listed above involve calculation of severe core damage frequency due to fires in various plant locations. With each subsequent calculation, the methods used to assess the risk for the various scenarios are refined. This iterative approach is used to identify high risk areas and to focus the detailed fire analysis on these areas. A brief summary of the methodology used for DARA-FIRE is provided in the following sections.

5.3.2 Plant Partitioning

This first task in the fire PSA involves the division of the plant into discrete areas called physical analysis units (PAUs). This requires defining the overall analysis boundary to ensure that those plant locations where a postulated fire could impact the PSA are included in the analysis. Once the overall analysis boundary is defined, the buildings that are within the boundary are examined for potential sub-division into PAUs. The PAUs used in the DARA-FIRE assessment are based on those identified in the DNGS Fire Protection Program documented in the Fire Hazard Assessment (FHA). This approach allows the fire PSA to rely on the existing programmatic controls and design requirements for maintaining the integrity of the associated compartment boundaries.

5.3.3 Fire PSA Component and Cable Selection

The development of a fire PSA requires identifying components necessary for safe shutdown and long-term decay heat removal following a fire. A fire can affect the equipment credited for safe shutdown by either being in the same area as the credited equipment or by being in the same area as the cables related to the credited equipment. For example, a fire in the same area as the power cables for a pump could result in failure of the pump, even if the pump itself was remote from the fire.

The purpose of this task is to identify the equipment to be included in the fire PSA, determine where in the plant, and in which PAU the equipment is located.

The selection of components required for safe shutdown following a fire is based on the systems credited in the Darlington Fire Safe Shutdown Analysis (FSSA) with the addition of components associated with the additional heat sink credits relying on IUFT, ESW to the moderator, and EME.

Once the equipment to be credited following a fire event has been identified, then the locations and routing of all cables that impact this equipment must be identified. This information can then be used to determine the fire PSA components potentially affected by postulated fires at different plant locations.

5.3.4 Qualitative Screening

The physical analysis units, described in Section 5.3.2 are screened to identify those PAUs where the contribution of fire risk to severe core damage is expected to be relatively low or nonexistent compared to other PAUs. The screening criteria considered the following:

- The type of equipment in the PAU;

- The types of ignition sources in the PAU, and the ability to introduce transient ignition sources into the area;
- Impact of the ignition sources on mitigating systems.

5.3.5 Fire-Induced Risk Model

This task involves the development of a logic model that reflects plant response following a fire. This includes modelling the plant response to fire-induced events and modifying the internal events PSA to reflect postulated equipment failures. The scope of the equipment credited in the fire risk model is limited to those components identified in Section 5.3.3.

The DARA-L1P model was modified and manipulated to produce a fire-induced risk model. Events in DARA-L1P were set to “failed” to represent the equipment that would be failed in the fire scenario.

5.3.6 Fire Ignition Frequencies

To calculate the risk due to an internal fire, the fire ignition frequencies (FIFs) for each PAU must be assessed. The frequencies were calculated based on generic data in NUREG/CR-6850 [R-11] and [R-12] and the plant populations of equipment that can be an ignition source (e.g., pumps, electrical equipment), identified by plant walkdowns and other appropriate means.

The DNGS fire PSA project is limited to Unit 0 and Unit 2. The calculation of FIFs for Unit 0 and Unit 2, however, required calculation of FIFs for all of the PAUs that are within analysis boundary. This was accomplished by:

1. Conducting fixed ignition sources (FISs) walkdowns of Unit 2 PAUs; and
2. Assuming that Unit 2 is spatially representative of the other three operating units, replicating the Unit 2 FISs walkdown data for PAUs in Units 1, 3 and 4.

Canadian CANDU fire experience data was reviewed to determine the applicability of using the NUREG/CR-6850 generic data [R-11]. The qualitative review of CANDU operating experience with fire events found Canadian experience sufficiently similar to U. S. experience documented in NUREG/CR-6850 [R-11] and concluded that it is reasonable to use that industry-wide generic data for fire bin frequencies for DARA-FIRE.

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

5.3.7 Quantitative Screening

The development of a fire PSA allows for a quantitative screening of PAUs based on contribution to SCD for a given PAU. This task estimates SCD frequency for each compartment as well as the cumulative risk associated with the screened compartments (i.e., those not retained for detailed analysis). With the information from the fire model and fire ignition frequencies (described in Sections 5.3.5 and 5.3.6), the contribution to severe core damage by PAU can be calculated. Based on the severe core damage contribution of each PAU, the areas of the plant are further screened, using industry standard screening criteria from Reference [R-11].

Areas of the plant that are screened during this step still are retained in the fire PSA model and contribute to overall risk from fire, they are just excluded from the detailed fire analysis that is used to assess the risk significant areas.

5.3.8 Scoping Fire Modeling

The scoping fire modelling refines the initial frequency results obtained in the quantitative screening process. The scoping fire modeling is used to develop explicit fire scenarios within the PAUs. This task involves the use of generic fire models for various fire ignition sources so that simple rules can be used to define and screen fire ignition sources (and therefore fire scenarios) in an unscreened fire compartment. Fire scoping models are developed for all fire areas.

This task has two main objectives:

- To screen out those fixed ignition sources that do not pose a threat to the targets within a specific fire compartment; and,

- To assign severity factors to unscreened fixed ignition sources.

To accomplish these goals, the scoping fire modelling refines the calculation of SCD frequency for each PAU.

5.3.9 Detailed Circuit Failure and Failure Mode Likelihood Analysis

The development of a fire PSA requires detailed circuit failure analysis and circuit failure mode and likelihood analysis. Detailed circuit failure analysis involves identifying how the failure of specific cables impacts the components credited in the Fire PSA. For example, not only can a fire result in failure of equipment, the fire may also result in spurious actuation of equipment, due to possible failure mode of the cables and control logic associated with the equipment.

Circuit failure mode and likelihood analysis task involves the evaluation of the relative likelihood of various circuit failure modes (e.g. failure to operate when required, spurious operation). This added level of resolution applies to those fire scenarios that are significant contributors to the risk.

Circuit analysis was not performed for cables required in the FSA. The scope of DARA-FIRE circuit analysis included cable failure mode and failure mode likelihood analysis of IUFT and the ESW to the moderator for the reference unit (Unit 2). These functions were added to the scope of credited safe shutdown equipment credited in the fire PSA, see Section 5.3.3. This task includes analysis of circuit operation and functionality to determine whether the cable's fire induced failure could result in undesirable equipment operation. In such cases, a probabilistic assessment of the likelihood that a fire induced failure causes a spurious operation is performed. Given that fire induced cable damage occurs, an appropriate conditional probability is assigned.

5.3.10 Detailed Fire Modeling

Detailed fire modeling was used to perform fire ignition source (scenario) specific fire modeling to address risk significant scenarios in cases where the scoping fire modelling described in Section 5.3.8 produced overly conservative results. The detailed fire modelling included:

- Explicit treatment of the MCR to address fire induced forced abandonment;
- Explicit analysis of multi-compartment scenarios;
- Potential MCR scenarios, potential turbine generator scenarios, potential high energy arcing fault scenarios and potential cable fire scenarios.

The abandonment times for operators in the DNGS Main Control Room (MCR) envelope were assessed for electronic equipment fires and for transient combustible fires within the MCR envelope.

The purpose of multi-compartment analysis is to calculate the probability of compartment interaction caused by a hot gas layer due to smoke propagation. The calculation is the product of multiplying the probability of a hot gas layer in the PAU (i.e., the probability that the fire creates a hot smoke layer) by the PAU barrier failure probability (i.e., failure of fire doors, dampers and penetrations). The multi-compartment analysis used the hot gas layer development timing defined in Reference [R-13].

5.3.11 Post-Fire Human Reliability Analysis

A review of DARA-L1P was performed to identify the post-initiator operator actions modeled as human failure events along with their associated human error probability (HEP); pre-initiator operator actions and operator actions associated with non-fire induced events were excluded from consideration.

For each fire-related basic event that represents a post-initiator operator action modeled as human failure, HEP multipliers were developed for fire PSA adjustments. The method to apply the HEP adjustment considered the following factors

- Location (either inside the MCR actions or outside the MCR actions);
- Time available (based on DARA-L1P HRA documentation);
- Complexity of the action (based on DARA-L1P HRA documentation);
- Availability of instrumentation;

- Availability of path to equipment for field actions.

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

No additional credit was taken for potential post-fire shutdown actions that were not already modeled in the internal events at power PSA.

5.3.12 Fire Level 1 PSA Quantification

The development of a fire PSA requires the integration of the fire risk model with the damage consequences calculated for each scenario.

The development of the fire risk quantification is typically an iterative process. As various analysis refinement strategies are developed, they are incorporated into the fire risk model.

The scope of work for fire quantification involves the use of the fire PSA model, described in Section 5.3.5, to quantify SCD frequency for each of the fire PSA scenarios.

The scoping fire modeling (Section 5.3.8) provided a conservative and simplified means to develop an initial refinement to the bounding treatment in the quantitative screening (Section 5.3.7). The scope of work for detailed fire PSA quantification involves the use of the fire PSA model with the modified post-fire HEPs (Section 5.3.11) and performing additional model quantifications to calculate severe core damage frequency. In the quantitative screening, the SCD frequency estimates were done at the PAU level. In the final quantification, information gathered during walkdowns conducted for scoping modelling (Section 5.3.8) and additional analysis of other Darlington NGS design inputs (e.g., equipment and cable tray layout drawings) was used to refine treatment of PAUs that had high estimated SCDFs in initial bounding assessment (Section 5.3.7). This refinement typically divided risk significant PAUs into multiple fire initiating events (scenarios) to represent the individual fire ignition sources. In some cases, multiple fire ignition sources in a PAU were grouped and treated as a single fire initiating event so long as such grouping did not result in overly conservative risk estimates.

5.3.13 Assessment of Unit-to-Unit Differences

The scope of work resulted in specific numerical results for the Unit 2 PAUs and other site PAUs that are common to all four units. Quantification of separate SCDFs and release frequencies for Units 1, 3, and 4 are not specifically included. Because fire risk characterization is needed for the entire plant site, the anticipated symmetry / consistency in the design and construction of the entire four unit site is being relied upon to support a qualitative approach.

A side-by-side comparison of the Unit 1, 3 and 4 PAUs to the analyzed Unit 2 PAUs was created using fire zone information from the FSA and the FHA. Equipment layout drawings and general arrangement drawings were also consulted. A walkdown was performed to assess the differences between the units. The walkdown confirmed the physical differences between the units are relatively minor. The top contributing scenarios are not impacted by any of the identified differences and no new scenarios were identified that would be expected to contribute significantly to fire-induced risk.

5.3.14 DARA-FIRE 2015 Bounding Assessment

The 2011 DARA-FIRE assessment was prepared according to the OPG Fire PSA Guide. The 2015 DARA-FIRE update is a bounding assessment. The overall objective of the 2015 DARA-FIRE report was to provide an estimate of the 2015 DARA-FIRE results and to support a qualitative confirmation that the 2011 DARA-FIRE results are bounding. This has been accomplished as follows:

1. Update of the fire ignition frequencies to include use of the latest U.S. industry guidance [R-21] and generic ignition frequency data [R-22], including a conservative treatment of the impact of DNGS-specific fire experience. The revised ignition frequencies have a broad impact on the fire PSA risk estimate as they impact all fire scenarios.

2. This bounding assessment quantifies the conditional core damage probabilities (CCDPs) for the fire scenarios using the latest 2015 DARA-L1P model, described in Section 5.1. Use of the revised model has a broad impact on the fire PSA risk estimate as it impacts the probability of each individual scenario progressing to severe core damage following the postulated initiating fire. The updated 2015 DARA-L1P model includes all relevant engineering and operational changes up to the study freeze date of December 31, 2013, including credit of Phase 1 Emergency Mitigating Equipment (EME).

3. The fire impact assessed in each of the fire scenario CCDP cases in the 2011 DARA-FIRE has been updated in this assessment to include consideration of the impact of the scenario on EME deployment and the availability of the EME injection path.

4. The 2011 DARA-FIRE assessment was based on the previous revisions of the FHA and FSSA. Design and operational changes captured in the 2011 revisions of the FHA and FSSA that would impact the DARA-FIRE update are expected to be minor according to the description of the changes contained in the scoping documents for the update of the FHA/FSSA. This means that there have not been substantial changes in the definitions of the fire zones or the number and location of ignition sources within the plant. Therefore, changes captured in the revised FHA and FSSA are expected to impact only a limited set of fire PSA scenarios with a small impact on the overall risk quantification; and have not been included in the 2015 DARA-FIRE bounding assessment.

5.4 At-Power Internal Flood

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

The 2011 DARA-FLOOD assessment was developed following the methodology for preparation of an Internal Flood PSA as described in the OPG Flood PSA Guide. The 2011 model and analysis were used as the basis for developing the 2015 bounding assessment described in Section 5.4.7.

Like the fire PSA described in Section 5.3, the impacts of internal flooding events are related to the physical location of equipment in the plant. The station must be divided into areas, and the potential initiators in each area assessed, and the impacts of the initiators determined.

The flooding analysis is focused on two primary objectives: areas of the plant that contain equipment from both Group 1 and Group 2 systems (referred to as “pinch-points”), or areas which might completely disable all of Group 1 or Group 2, as these areas represent the highest potential for degradation of the plant mitigation capability; and conservative estimation of risks associated with the other areas of the plant. A major input into the Internal Flooding PSA is the At-Power Internal Events PSA (DARA-L1P). The At-Power Internal Events PSA is used to determine which components need to be evaluated for flooding impacts, and is also used as the basis for the quantification of the internal flooding severe core damage frequency.

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

1. Identification of Flood Areas and Systems Structures and Components (SSCs).
2. Identification of Flood Sources.
3. Internal Flood Qualitative Screening.
4. Potential Flood Scenario Characterization.
5. Internal Flooding Initiating Event Frequency Estimation.
6. Flood Consequence Analysis.
7. Evaluate Flood Mitigation Strategies.
8. Internal Flooding Accident Sequence and Level 1 PSA Quantification.
9. Sensitivity and Uncertainty Analysis.
10. Support Task – Plant Walkdowns.

Figure 11 shows the tasks for the flooding PSA.

The flooding PSA focuses on sequences that lead to severe core damage (FDC1 and FDC2) caused by an internal flood. Failure to shutdown sequences (FDC1) are not quantified as the frequency of FDC1 is several orders of magnitude lower than FDC2 in the DARA-L1P model (see Table 14) and the potential for flooding events to adversely affect the shutdown systems, which fail safe on loss of power or loss of actuation inputs, is minimal.

5.4.1 Identification of Flood Areas, SSC and Flood Sources

Like the fire PSA, the first step of the flooding PSA is to partition the plant into the flood areas that will form the basis of the analysis. As part of this task the flood areas are defined based on physical barriers, mitigation features, and propagation pathways. The flood areas were defined based on the partitions in the FSA.

Once the flood areas are defined, the SSCs in each flood area modelled by the internal event PSA are identified.

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

5.4.2 Internal Flood Qualitative Screening

This step performs a qualitative screening considering the sources of flooding, the flood propagation pathways and the consequences of the flood. The objective is to qualitatively screen out many low risk internal flood scenarios.

The following rules were used when screening:

- The area is outside of Unit 2 (the reference unit) or Unit 0 (common unit);
- The area does not contain any equipment credited in the FSA (see Section 5.3.4);
- The area contains no Group 1 equipment affecting FDC2;
- The area contains no Group 2 equipment affecting FDC2;
- The area contains no credible flood source, or credible propagation path.

The unscreened areas are the pinch-point areas for the flooding assessment.

5.4.3 Potential Flood Scenario Characterization and Consequence

This step identifies and characterizes the potential flood scenarios to be included in the analysis. This task characterizes the consequences for each flood-induced initiating event by considering the following factors:

- Type of flood source, including the type of pressure boundary failures (e.g., spray, large leak, major structural failure), capacity of the flood source (e.g., unbounded lake source, closed tank);
- Spill rate;
- Flood location;
- Time to reach the critical flood volume (e.g., to submerge equipment, or lead to propagation into another area);
- The impact on the SSCs modelled in the PSA.

5.4.4 Internal Flooding Initiating Event Frequency Estimation

This step identifies flooding induced initiating events and estimates their frequency of occurrence. The flooding failure rates are based on generic EPRI data from Reference [R-14].

5.4.5 Flood Mitigation Strategies

This step is to identify and evaluate the strategies that can be employed by plant operators to mitigate the consequences of the flood. These actions can include terminating the source of the flood by isolating the break, or stopping the pumps that supply the flood source, or open doors to divert water away from sensitive equipment.

The evaluation of human failure events in the internal flood scenarios differs from the internal events PSA. Specifically, the appropriate scenario-specific impacts on Performance Shaping Factors (PSFs) were considered for both control room and ex-control room actions based on the following items:

- Additional workload and stress (above that for similar sequences not caused by internal floods) ;
- Availability of indications;
- Effect of flood on mitigation, required response, timing, and recovery activities (e.g., accessibility restrictions, possibility of physical harm);
- Flooding-specific job aids and training (e.g., procedures, training exercises).

5.4.6 Internal Flooding Accident Sequence and Level 1 PSA Quantification

This step includes the finalization of flood scenario development and completing internal flood accident sequence models based on modifying the internal events PSA model. The DARA-FLOOD model is based on small event trees for each flooding scenario. These event trees model the possible mitigating actions described in Section 5.4.5. Based on success or failure of the mitigating actions equipment availability is determined. To assess core damage frequency with the given available equipment, the DARA-FLOOD model uses conditional core damage probabilities, calculated from the internal events PSA, which are then combined with the initiating event frequencies and operator action probabilities from the event trees to calculate severe core damage. The conditional core damage probabilities are based on the forced shutdown event tree logic, with the equipment postulated to be unavailable due to the flood failed in the fault tree model.

Qualitative sensitivity and uncertainly analyses were included as part of the quantification of the 2011 DARA-FLOOD model.

5.4.7 DARA-FLOOD 2015 Bounding Assessment

The 2011 DARA-FLOOD assessment was prepared according to the OPG Flood PSA Guide. The 2015 DARA-FLOOD update is a bounding assessment. The overall objective of the 2015 DARA-FLOOD report was to provide an estimate of the 2015 DARA-FLOOD results and to support a qualitative confirmation that the 2011 DARA-FLOOD results are bounding. This has been accomplished as follows:

1. Update of the piping rupture frequencies with the latest EPRI data [R-23].

2. Assessment of postulated flooding scenarios impact on deployment of the Emergency Mitigating Equipment (EME), including accessibility of the deployment locations and the associated HEPs. Generally, the flooding scenarios credit EME for preventing severe core damage using the same logic modelled in DARA-L1P.

3. Re-quantification of CCDP using the 2015 DARA-L1P model and re-quantification of Severe Core Damage Frequency (SCDF) for all postulated flood scenarios.

4. The qualitative screening, flood area identification, and flood source identification are based on the FSA/FSSA. As described in Section 5.3.14, the revisions to these documents are expected to be minor, and no change was made to the qualitative screening, flood area identification, and flood source due to the bounding nature of the 2015 DARA-FLOOD assessment.

5.5 At-Power Seismic

The DARA-SEISMIC assessment has been developed following the methodology for preparation of a seismic PSA as described in the OPG Seismic PSA Guide. The major activities of the Seismic PSA methodology and its application in the development of the DARA-SEISMIC assessment are summarized in the subsections below.

The primary steps in developing the seismic PSA 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 seismic PSA was created based on the internal events At-Power PSA, DARA-L1P.

The DARA-SEISMIC model considers sequences that result in severe core damage (FDC1 and FDC2). Like the fire PSA, FDC1 sequences (failure to shutdown the reactor) are not assessed following a seismic event. Failure to shutdown following a seismic event is highly unlikely as SDS2 is seismically qualified, and selective active components of the SDS1 system (mainly the shutoff rods) are seismically qualified. The two shutdown systems are highly reliable, and both have a fail-safe design.

Similar to the Fire and Flood studies, the Seismic PSA Guide also outlines a Phased approach with two phases defined:

- **Phase 1 - PSA-Based Seismic Margin Assessment (SMA)** - In Phase 1, a Probabilistic Safety Assessment-based Seismic Margin Assessment (PSA based SMA) is performed based on the methodology described in Reference [R-15]. This focused approach uses a plant model based on DARA-L1P with the addition of new seismic failure modes; the new seismic failure events are developed from a seismic margin approach with generic variabilities and the seismic risk is calculated based on a point estimate format that does not include a full uncertainty analysis.

- **Phase 2 - Limited Seismic PSA (SPSA)** – 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 SPSA. 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.

For Darlington, a Phase 2 Seismic PSA study was performed.

Major elements of the DNGS SPSA consist of the following tasks as listed below:

- Seismic Hazard Characterization
- Plant Logic Model Development
- Seismic Response Characterization
- Plant Walkdown and Screening Reviews
- Seismic Fragility Development
- Seismic Level 1 PSA Quantification
- Alternate Unit Analysis (excluded from DARA-SEISMIC assessment)
- Seismic PSA Documentation

The integration of these tasks is shown in Figure 12.

5.5.1 Seismic Hazard Characterization

The first step in the seismic PSA is to model the site-specific seismic hazard. The seismic hazard is representation of the possible earthquakes and seismic activity that can be experienced at the site. The seismic hazard is a plot of the peak ground acceleration versus the annual frequency that the ground acceleration will be exceeded (typically described as the frequency of exceedance). Figure 13 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 analysis. The seismic PSA assess the risk of severe core damage for earthquakes with a frequency up to 1E-04 occurrences per year (recurrence interval of 10,000 years or less). Current seismic standards such as CSA N289.1-08 [R-20] require use of the 1E-04 per year frequency for design of new nuclear power plants and for evaluation of the seismic capacity of existing plants.

5.5.2 Plant Logic Model Development

This task involves two related but separate sub-tasks: development of the event tree logic for the risk quantification model, and development of the seismic equipment list (SEL), which lists the components credited in the seismic PSA. This task relies upon the internal events PSA and other safe shutdown analyses to define the functions, systems, and components required to mitigate seismic initiating events.

The equipment included in the SEL is limited to the seismically qualified components in the systems required to prevent SCD and credited in the design basis seismic safe shutdown analysis (e.g., SDS2, ESW, ECI, EPS, EPGs, and required support systems), plus the emergency mitigating equipment. The systems in the reference unit (i.e., Unit 2) and the common systems (i.e., Unit 0) are assessed. A starting point for the SEL is the fire safe shutdown equipment list. The seismic model was expanded to credit additional systems and equipment (ESW to the moderator, PAWCS, and EME).

5.5.3 Seismic Response Characterization

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

The ground oscillation of any seismic event can be described by a combination of frequencies. This is called the spectrum of the seismic event. Each potential seismic event may have a different spectrum. The different frequencies in an earthquake’s spectrum will be transferred to the building in different ways. The response of site buildings determines how the earthquake will affect the credited equipment in the seismic PSA 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 structural response of the site buildings. This method is based on the existing design basis earthquake (DBE) seismic response analyses for the site buildings, prepared as part of the design for the Darlington NGS, with updates to reflect the shapes of the new seismic hazard curves. In addition to characterizing the overall building response, this task defines the local accelerations for the credited equipment. In Phase 2, soil-structure interaction analysis was performed for key site structures to remove any conservatism from the structural responses used in the Phase 1 analysis.

5.5.4 Plant Walkdown and Screening Reviews

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 SPSA. The plant walkdowns included reviews of the SEL items in one unit and the items in the systems common to all four units. The 2015 DARA-SEISMIC update included a walk down to assess additional components required for crediting EME.

5.5.5 Seismic Fragility Development

The likelihood that a given piece of equipment will fail for a given seismic hazard is based on the fragility of the equipment. The fragility of the equipment is a conditional failure probability that the equipment will fail when subjected to a specific acceleration caused by a seismic event. The likelihood the equipment will fail increases as it is subject to greater acceleration. Figure 14 shows an example fragility curve. Figure 14 shows that if the example equipment is subject to an acceleration of 1g, the failure probability is 80%.

Preliminary fragilities were determined through a combination of walkdown review of the as installed configurations, experience-based estimates, and equipment-specific fragility calculations using the Conservative Deterministic Failure Margin (CDFM) methodology [R-16]. In some cases more refined fragilities were derived using the Separation-of-Variable method [R-17] and [R-18], for risk contributing equipment. This method includes estimates of median seismic capacity and uncertainty.

5.5.6 Seismic Level 1 PSA Quantification

To build the seismic PSA model, the information on the seismic response of the buildings and the seismic fragility of the equipment must be used to calculate the probability of equipment failures and these new events added to the seismic PSA.

This task involves the integration of the seismic fragility information described in Sections 5.5.3 to 5.5.5 with the overall plant logic model, by adding the fragility information to appropriate sequences and basic events in the plant logic model.

In the quantification of DARA-SEISMIC, the seismic hazard curve was divided into discrete intervals. Eight intervals were used to represent the different seismic hazards; Table 10 shows the intervals used for DARA-SEISMIC. These intervals are the initiating events for the DARA-SEISMIC study. In this approach, the hazard curve is divided into discrete ground motion intervals. The SSC fragilities are calculated specifically for each interval (e.g., at the mid-point or geometric mean of the interval), and then the corresponding fragility probabilities are inserted as basic events into accident sequence models, along with the hazard frequency for that interval (e.g., frequency of “interval G3” is calculated as the annual exceedance frequency at the beginning of G3 minus the annual exceedance frequency at the end of G3). A different set of fragility events and associated accident sequence logic are developed and quantified for each interval, and then the sequence frequencies for each interval are combined.

5.6 At-Power High Wind

The DARA-WIND assessment has been developed following the methodology for preparation of a high wind PSA as described in the OPG High Wind Hazard PSA Guide. The major activities of the high wind PSA methodology and its application in the development of the DARA-WIND assessment are summarized in the subsections below.

The primary steps in developing the high wind PSA are identifying the high wind hazard, identifying the high wind targets, developing wind-borne missile fragilities for the high wind targets, evaluating the fragility of the high wind targets, developing the high-level plant logic, and quantifying the high wind scenarios. The high wind PSA was created based on the internal events At-Power PSA, DARA-L1P.

Figure 15 shows how each step feeds into the overall DARA-Wind study. The methodology applied in the high wind hazard assessment uses a high level approach in determining fragilities based on wind capacity. The approach is realistic with conservative assumptions to simplify the analysis where needed.

5.6.1 High Wind Hazard Analysis

The first step in the high wind PSA is to identify the potential contributing wind hazards at the site. The primary hazard includes straight winds (thunderstorms and extratropical cyclones), hurricanes and tornadoes. The wind hazard curve is developed for peak gusts in open terrain at 10 m height. Terrain, height, and averaging time adjustments shall be performed to adjust gust wind data to 3 second gust speed at a height of 10 m in flat open terrain. Figure 16 shows an example of high wind hazard curves.

Similar to the seismic results, the high wind results are reported for high winds with a frequency up to 1E-04 occ/yr.

5.6.2 Plant Logic Model Development

This task involves two related but separate sub-tasks: development of the event tree logic for the risk quantification model, and identification of target systems, structures, and components (SSCs) that are included in the high wind PSA model. The high wind plant logic model examines the response of plant SSCs to the defined high wind hazard, and then combines this response with the response of the plant to the initiating event, given the degraded condition of pant SSCs the challenges faced by the operator due to the wind hazard. The focus of the high wind analysis is estimation of severe core damage frequency for a single reference unit, with consideration of the common unit and adjacent unit impacts on the reference unit.

5.6.3 Analysis of Windborne Missile Risk

Windborne missile fragility is defined as the probability of target damage (failure) from windborne missiles for a given value of peak gust wind speed. Wind-borne missile risk includes:

i. Flying missiles that hit/damage an exterior target.

ii. Flying missiles that enter a building and hit an interior target.

iii. Flying missiles that originate within a building and hit an interior target.

The windborne missile risk analysis considered the risk from all potential missiles at and near the site. Missile data were collected from the site walkdown, plant layout and SSC drawings.

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

The missile fragility functions were developed for the dominant wind hazards at the site. A single hazard developed set of missile fragility functions was used for all hazards provided the fragility functions were judged to be conservative for other hazards. Missile fragility functions specific to individual hazards were developed to address cases where the single hazard missile fragility function was judged to be too conservative for application to other hazards.

The windborne missile risk considered failure of building components in the determination of flying missile risk and missile fragilities for targets. The failed building components (such as cladding, roof top equipment, roof elements, and loose contents) were assumed to be available missiles at appropriate wind speeds associated with the failure of the building envelope components for that building type.

The windborne missile fragilities were represented by missile hit, missile penetration, perforation, spall, or other damage relationship appropriate for the target.

5.6.4 High Wind Fragility Development

Wind fragility is defined as the conditional probability of failure for a given value of peak gust wind speed. The general objective of the wind fragility study is to assess the aerodynamic wind forces which may result in damage to buildings housing safety-related equipment and their contents and to determine associated uncertainty.

High wind capacities and corresponding fragilities were developed for the identified targets. The fragility of screened-in targets was assessed using an advanced code-based methodology. This method applies the basic code-based approach with code and load-effect calculations and considers wind direction, terrain roughness, blockage, and structure enclosure state. The 50th percentile fragilities were taken to represent the mean fragility and were used in the risk quantification to represent the nominal point estimate fragility of a given component. The fragility of EME targets, such as the EME storage building, sliding failure mode, and overturning failure mode, was developed for DARA-Wind.

5.6.5 High Wind Hazard Site Walkdown

The high wind Hazard walkdown includes a walkdown of credited SSCs and a missile survey. The walkdowns of SSCs were performed by a qualified team in order to confirm all the structures and their condition, vulnerability of the equipment, etc. The walkdowns of the windborne missile survey were conducted by a qualified team that covers each missile source zone at the entire site. The survey collected data on the types, numbers, and locations of potential missiles (e.g., construction materials, equipment, automobiles, signs, trees, and vulnerable structures that are likely to fail in windstorms).

5.6.6 Plant Response Model Quantification

Quantification of the high wind PSA models requires the integration of the wind hazard curves from Section 5.6.1 and the combined fragility curves from Section 5.6.4 along with the non-high wind or random failure modes according to a Boolean representation of ways the plant response is assumed to lead to core damage.

This task involves the integration of the high wind hazard and fragility information with the overall plant logic model, by adding the fragility information to appropriate sequences and basic events in the plant logic model.

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

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

6.0 LEVEL 2 PSA METHODS

Section 5.0 described the methods used for the Level 1 PSA assessments of Darlington NGS. In the Level 1 PSA, the goal was to quantify the frequency of fuel damage. Once the fuel has been damaged, there is the potential for radioactive material to be released from the fuel into containment. The Darlington NGS design includes a containment system (described in Section 2.3.14) to prevent the release of any radioactive material in the station from being discharged into the environment.

The Level 2 PSA studies the system failures and accident phenomena that might result in a release to the environment, and the timing and magnitude of the release. This information is combined with the Level 1 DARA-L1P model to quantify the frequency of possible releases.

The DARA-L2P model has been developed following the methodology for preparation of a Level-2 PSA as described in the Level 2 PSA Guide. The major activities of the Level-2 PSA methodology and its application in the development of DARA-L2P are summarized in the subsections below.

6.1 Interface with Level 1 PSA

The Darlington Level 1 At-Power Internal Events PSA (DARA-L1P) generates results in the form of frequencies of nine Fuel Damage Categories, described in Section 5.1.2, representing a wide range of possible outcomes. The possible outcomes include the most severe involving failure to shutdown (FDC1) to relatively benign where there are no fuel failures and release is limited to the equilibrium fission product inventory of the Heat Transport System (HTS) (FDC9). A subset of the FDCs (1-7), those that involve release of significant quantities of fission products from the core, is used to develop the interface between Level 1 and Level 2, the Plant Damage States (PDSs). The plant damage states serve to reduce number of the sequences assessed in the Level 2 analysis to a manageable number while still reflecting the full range of possible accident sequences and their impacts on the plant.

Only two FDCs are used to represent the range of sequences that result in severe core damage, FDC1 for rapid accident progression resulting from failures to shut down the reactor when required and FDC2 for all other sequences. FDC1 is conservatively assumed to cause early consequential containment failure and is assigned to a unique PDS, PDS1.

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

- PDS2 represents sequences affecting a single unit with release into containment;
- PDS4 represents single unit sequences with a release pathway that bypasses containment;

- PDS3 represents sequences affecting more than one unit.

Random containment system failures are associated only with PDS2 and were identified by means of a Bridging Event Tree (Figure 17) that led to the creation of seven subcategories, labelled PDS2A-G.

As described in Section 1.0, Unit 2 is the reference unit for the PSA study. In order to develop the logic for PDS3, additional simplified modelling of the other three units was undertaken to partition the FDC2 logic into sequences that impact a single unit, and sequences that could impact more than one unit.

FDCs 3-7 represent the range of accidents that fall under the general heading of "design basis events". These were allocated to PDS5 and 6 respectively, depending on whether the initiating event involves containment bypass (PDS6) or not (PDS5).

FDCs 8-9 are excluded from Level 2 analysis on the basis that the radionuclide releases from these in-plant sequences would be negligible.

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

The Level 1 PSA is used to identify initiating events that are the largest contributors to the frequency of the plant damage state. These sequences are then reviewed to select a representative sequence that bounds the consequence. The approach follows the guidance of the International Atomic Energy Association (IAEA) as this method selects a sequence that "largely bounds" the PDS. The representative sequences chosen for each PDS are summarized in Table 11.

6.2 Containment Event Tree Analysis

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

A CET is a logic model that addresses uncertainties in the ability to predict the potential impacts of accident progression and associated physical phenomena on containment response. Figure 18 shows a simplified containment event tree. 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 and its continued integrity at a given stage of accident progression (e.g., *"Is containment integrity maintained?"* or *"Does core concrete interaction occur?"*). The CET branch points represent major events in accident progression and the potential for fission product release to the environment. The CET also represents the evolution of the progression with time so the same nodal question may appear more than once in the tree as conditions inside containment change. The focus of the CET is to estimate the probabilities of the various ways that containment failure may occur leading to a release to the environment.

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

6.3 Containment Fault Trees

Containment system fault trees are required for quantification of the frequencies of the end-states PDS2A – PDS2G in the Level 1/Level 2 PDS2 bridging event tree, which is shown in Figure 17, and includes the following branch headers:

CEI: Impairment of Containment Integrity Avoided

ACU: Reactor Vault Cooling System Condenses Steam

IGN: Hydrogen Igniters Control Possible Hydrogen Burn

FADS: Emergency Filtered Air Discharge System Filters and Vents (not credited in the baseline DARA-L2P assessment)

The fault tree models used in the quantification of the Level 2 PSA are listed in Table 6. Fault tree representations for failure of these containment functions have been developed, reflecting the likelihood that random equipment failure or human error will prevent the operation of the system on demand or during the mission. Containment failures arising as a consequence of severe accident progression are addressed in the CET.

6.4 Release Categorization

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

- The magnitude of release in Becquerel (Bq) of specific radionuclides considered important to offsite impacts (e.g., isotopes of cesium or iodine); and

- The timing of the release, either early in the accident sequence (where “early” is less than 24 hours) or late (after 24 hours).

Seven RCs cover the full range of possible releases and provide enough discrimination to evaluate safety goal frequencies. An eighth category is used to represent basemat melt-through, when the core debris is postulated to penetrate the floor of the fueling machine duct. Table 12 presents the release categories used in the DARA-L2P analysis. Large release frequency (LRF) is defined to be the sum of RC1 through RC3.

6.5 MAAP-CANDU Analysis

MAAP-CANDU (Modular Accident Analysis Program – CANDU) is a severe accident simulation code for CANDU nuclear stations [R-19]. It is used to calculate the consequences of severe accidents and is designated as a CANDU Owners Group (COG) Industry Standard Toolset (IST) code. MAAP-CANDU originated from MAAP developed for Pressurized Water Reactor (PWR) and Boiling Water Reactor (BWR) systems by Fauske and Associates (FAI) and is part of the EPRI suite of probabilistic safety assessment tools.

MAAP-CANDU can simulate the response of a CANDU power plant during severe accident sequences. The code quantitatively predicts the evolution of a severe accident starting from full power conditions given a set of system faults and initiating events through events such as core melt, primary heat transport system failure, calandria vessel failure, shield tank failure, and containment failure.

Severe accident analysis carried out using MAAP-CANDU is the cornerstone of the Level 2 PSA. There are at least five distinct roles for the code, as outlined below;

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

6.6 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 release category.

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

6.7 Level 2 Outage Assessment

Given the low risk of fuel damage from internal events occurring while the unit is in GSS, a full Level 2 study of the outage risks was not performed. Instead a bounding assessment of the large release was performed while the unit is in outage.

The at-power Level 2 assessment (DARA-L2P) demonstrated that a large release can only occur if severe core damage has occurred, so the large release frequency while the unit is in outage can be bounded by the frequency of severe core damage while the unit is in outage.

The plant configuration in each POS was reviewed for potential containment failures (random failures, containment bypass, or consequential containment failure). A limited number of outage specific considerations were identified that might impact the severe accident progression.

Additional MAAP-CANDU analysis was performed to assess the consequences of the identified outage sequences.

6.8 Level 2 Fire Assessment

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 three steps:

- Screening of low risk scenarios (collective SCD frequency < 1E-07). The low risk scenarios are not assessed further and are conservatively assumed to result in a large release.
- Screening of remaining scenarios based on potential multi-unit impact, or potential to impact Level 2 functions. The potential impacts on Level 2 included:
    - Fire-induced failure of containment;
    - Failure of containment due to random failures or phenomenological effects based on the Level 2 At-Power Internal Events PSA; and
    - Random failures of the primary heat transport system during transient leading to containment bypass LOCA.
- The unscreened sequences were then assessed to determine the number of units impacted by a scenario. The appropriate containment event trees (CETs) from the Level 2 At-Power Internal Events PSA were evaluated for these groups to determine the fraction of each type of sequence that progresses to a large release.

The sum of the contribution from each group is then used to estimate LRF caused by internal fires.

6.9 Level 2 Seismic Assessment

The Level 2 seismic PSA included the following tasks:

- Estimate of the seismic fragility of containment components (containment robustness assessment);
- Estimate of LRF due to seismic events.

Additional walkdowns and fragility calculations, using the same techniques as those described in Section 5.5.5, were used to assess the possible failure of containment due to seismic events.

To estimate LRF due to seismic events, the cutsets were partitioned into three groups

- Sequences with single unit failure and no containment bypass;
- 2-unit sequences; and
- 3- or 4-unit sequences.

The containment failure probability is a combination of:

- Seismically-induced failure of containment;
- Failure of containment due to random failures or phenomenological effects based on the Level 2 PSA (DARA-L2P); and
- Random failures of primary heat transport (PHT) box-up leading to containment bypass.

6.10 Level 2 High Wind Assessment

The Level 2 high wind assessment was performed using insights from the Level 2 At-Power Internal Events PSA. To estimate LRF, the high wind SCD cutsets were partitioned into four groups:

- Sequences with single unit failure and no containment bypass;
- Sequences where there is a bypass of containment;
- 2-unit sequences; and
- 3- or 4-unit sequences.

The appropriate containment event trees (CETs) from the Level 2 At-Power Internal Events PSA were evaluated for these groups to determine the fraction of each type of sequence that progresses to a large release. The sum of the contribution from each group is then used to estimate LRF caused by high winds.

7.0 SAFETY IMPROVEMENT OPPORTUNITIES

The DARA-2015 models assessed the benefit of five safety improvement opportunities. Five SIOs are considered in the sensitivity case model:

- Duplication of powerhouse steam venting system (PSVS) programmable controller to improve the reliability of the PSVS system.
- Installation of a third Emergency Power Generator qualified to withstand a more severe seismic event than the Design Basis Earthquake (DBE) that the existing EPGs are designed to withstand.
- Provision of an alternate and independent supply of water as an emergency heat sink to provide make-up water to the steam generators, primary heat transport system, and calandria, with water supplied by new firewater pumps.
- Containment Filtered Venting System (CFVS). CFVS is a new system to prevent failure of containment due to overpressure following severe accidents at multiple units.
- Shield tank over pressure (STOP) relief. The STOP modification adds a rupture disc to the shield tank and prevents shield tank overpressure failure by relieving the pressure in the shield tank in a controlled manner.

Note the last two SIOs for CFVS and STOP only affect the progression of severe accidents following the occurrence of severe core damage, so these SIOs are only assessed as part of the LRF quantification.

The PSA implementation of each SIO is based on the design information available at the time of preparation of DARA. For some SIOs, the design is nearing completion and detailed information is available; for other SIOs, the design is at an earlier stage. The testing and maintenance practices are assumed to remain the same as the baseline case. Future DARA model updates will reflect the actual design and operation of the SIOs with better accuracy.

The SIO sensitivity results are presented in Table 13.

8.0 SUMMARY OF RESULTS

8.1 Frequencies of Severe Core Damage and Large Release

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

- Frequency of severe core damage; and
- Frequency of large release.

Table 13 compares the results of the PSA studies described in Sections 5.0, 6.0 and 7.0, with the OPG safety goals for individual hazards on a per-unit basis.

Table 13 also shows the aggregated SCDF and LRF results for all hazards for a single unit, using simple addition. However, no widely accepted methodology exists for risk aggregation and simple addition may lead to overly-conservative and biased results.

The SCDF aggregated by simple addition on a per-reactor basis was calculated by adding the per-reactor SCDF for each of the hazards. The LRF aggregated by simple addition on a per-reactor basis was calculated by adding the per-reactor LRF for each of the hazards.

OPG has both safety goal limits and targets. The safety goal limit represents the limit of tolerability of risk exposure above which action shall be taken to reduce risk. The safety goal target represents the desired objective towards which the facility should strive to the extent practicable.

The results in Table 13 show that the severe core damage frequency results for individual hazards is well below the OPG Safety Goal Limit of 1E-04 per reactor-year. Moreover, the severe core damage frequency results are below the OPG Safety Goal Target of 1E-05 per reactor-year. Similarly, the large release frequency results are below the OPG Safety Goal Limit of 1E-05 per reactor-year, with most of the results being below the OPG Safety Goal Target of 1E-06 per reactor-year. The SIO changes will provide a signficant reduction in risk, reducing both the SCDF and LRF results for all of the hazards assessed by the PSA studies.

The internal events PSAs assess the full range of fuel damage and release categories defined in Table 5. The frequencies of fuel damage categories for the at-power internal events PSA (DARA-L1P) is presented in Table 14. The results in Table 14 show that failure to shutdown is a negligible contributor to severe core damage frequency. The frequency of fuel damage for outage internal events (DARA-L1O) by POS is presented in Table 15. The outage results in Table 13 show that the risk is below the OPG Safety Goal Target, and that when the SIOs are credited, SCDF and LRF are further reduced.

As described in Section 6.1, the fuel damage categories used as end states in the Level 1 PSA are partitioned into Plant Damage States (PDSs) to use as inputs into the Level 2 PSA. Table 16 presents the frequencies of the plant damage states, and Table 17 presents the results of DARA-L2P.

8.2 Conclusions

The PSA for the Darlington Nuclear Generating Station (DARA) is performed in accordance with CNSC Standard S-294, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants. The S-294 compliant DARA was first completed in 2011 using methodologies for which CNSC's acceptance has been obtained. The 2015 DARA update addresses Level 1 and Level 2 PSA aspects for various internal and external events, for both at-power and outage operating conditions, including internal events, internal fire, internal flood, seismic, high winds, as well as an external and internal hazard screening assessment.

The 2015 DARA results demonstrate that the Darlington station satisfies OPG's safety goal limits for all internal and external hazards considered, and hence represents very low public risk. OPG continues to meet industry best practices through periodic updates to account for operating experience and changes at the station.

9.0 REFERENCES

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

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

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

[R-4] Ontario Power Generation Inc., Risk and Reliability Program, N-PROG-RA-0016, R07, June 2013.

[R-5] CAFTA, Software Manual Version 5.4, EPRI, Palo Alto, CA: 2009. Software Product ID #1018460.

[R-6] U.S. Nuclear Regulatory Commission, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants, NUREG/CR-6928, January 2007.

[R-7] The TUD Office, T-Book - Reliability Data of Components in Nordic Nuclear Power Plants, 6th Edition, ISBN 91-631-7232-1, 2005.

[R-8] Westinghouse Savannah River Company, Savannah River Site Generic Data Base Development, File # WSRC-TR-93-262, Rev. 1, May 1998.

[R-9] Swain, A.D., and H.E. Guttmann, Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, D.C., August 1983.

[R-10] FTREX User Manual Version 1.7 EPRI, Palo Alto, CA and KAERI, Daejeon, South Korea: 2013. Software Product ID #: 3002000070.

[R-11] EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities: Volume 2: Detailed Methodology, Electric Power Research Institute (EPRI), Palo Alto, California USA, and United States Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Rockville, Maryland USA, EPRI TR-1011989 and NUREG/CR-6850, 2005.

[R-12] Fire Probabilistic Risk Assessment Methods Enhancements, Electric Power Research Institute (EPRI), Palo Alto, California USA and United States Nuclear Regulatory Commission Office of Nuclear Regulatory Research (RES), Rockville, Maryland USA, EPRI TR-1019259 and NUREG/CR-6850 Supplement 1, September 2010.

[R-13] Generic Fire Modeling Treatments, Hughes Associates Project Number 1SPH02902.030, Revision 0, January 15, 2008.

[R-14] Pipe Rupture Frequencies For Internal Flood Probabilistic Risk Assessments (PRAs), EPRI, Palo Alto, CA: 2009, 1021086 R01.

[R-15] United States Nuclear Regulatory Commission, Recommendations to the Nuclear Regulatory Commission on Trial Guidelines for Seismic Margin Reviews of Nuclear Power Plants, NUREG/CR-4482, Lawrence Livermore National Laboratory, Livermore, CA, 1986.

[R-16] Electric Power Research Institute, A Methodology for Assessment of Nuclear Power Plant Seismic Margin, Revision 1, EPRI NP-6041 SL, Palo Alto, CA, August 1991.

[R-17] Electric Power Research Institute, Seismic Fragility Application Guide, EPRI TR-1002988, Palo Alto, CA, 2002.

[R-18] Electric Power Research Institute, Methodology for Developing Seismic Fragilities, EPRI TR-103959, Palo Alto, CA, June 1994.

[R-19] MAAP4-CANDU - Modular Accident Analysis Program for Candu Power Plant Volume 1: User Guidance, Fauske & Associates, Inc, Burr Ridge, Illinois, 1998.

[R-20] General Requirements for Seismic Design and Qualification of CANDU Nuclear Power Plants, CSA N289.1-08, September 2008.

[R-21] The Updated Fire Events Database: Description of Content and Fire Event Classification Guidance, Electric Power Research Institute, Report 1025284, July 2013.

[R-22] Nuclear Power Plant Fire Ignition Frequency and Non-Suppression Probability Estimation Using the Updated Fire Events Database, United States Nuclear Regulatory Commission and the Electric Power Research Institute, NUREG-2169 (EPRI Report 3002002936), December 2014.

[R-23] Pipe Rupture Frequencies for Internal Flooding Probabilistic Risk Assessments, Revision 3. EPRI, Palo Alto, CA: 2013. 3002000079.

Figure 1: Site Area

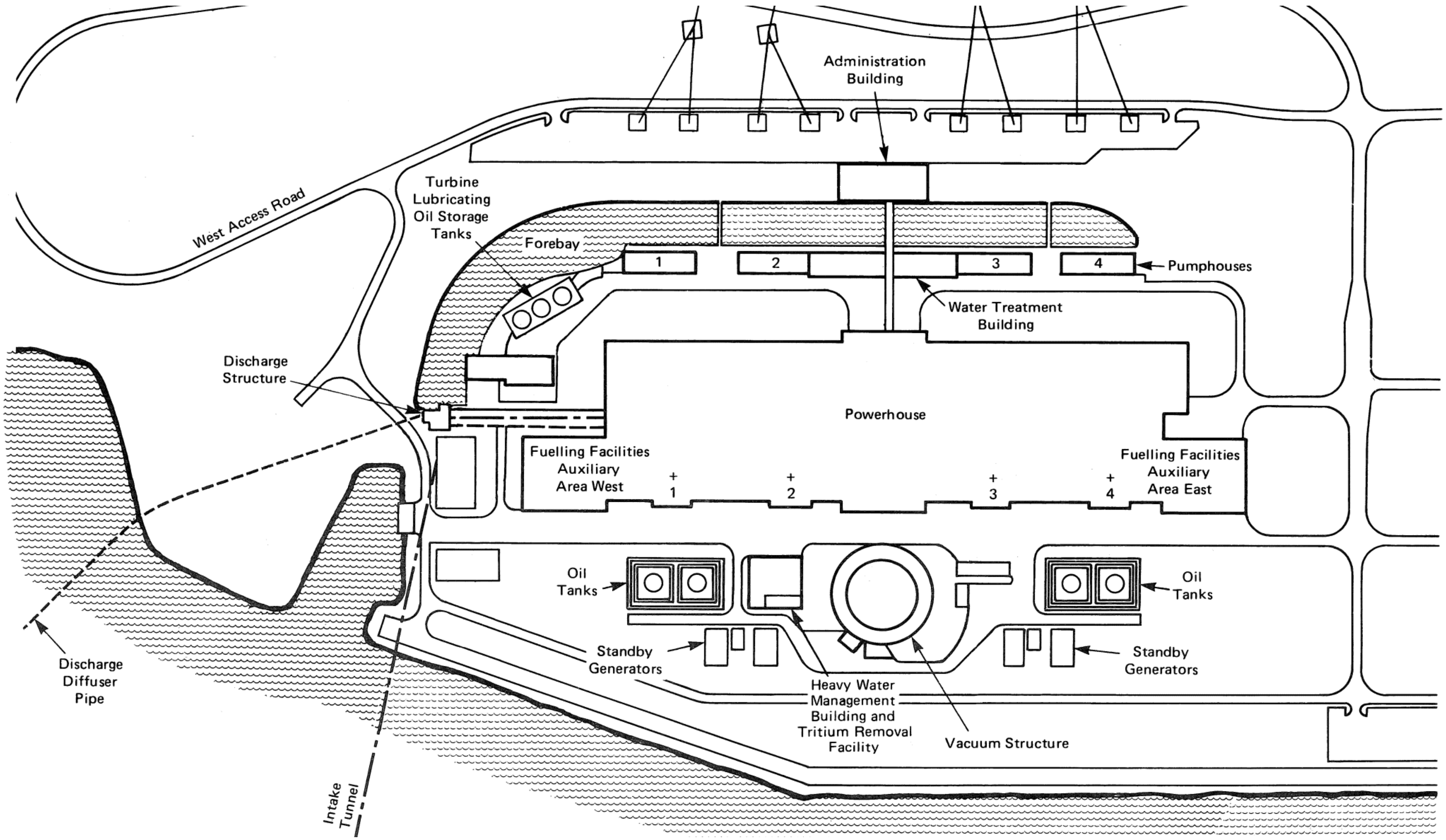
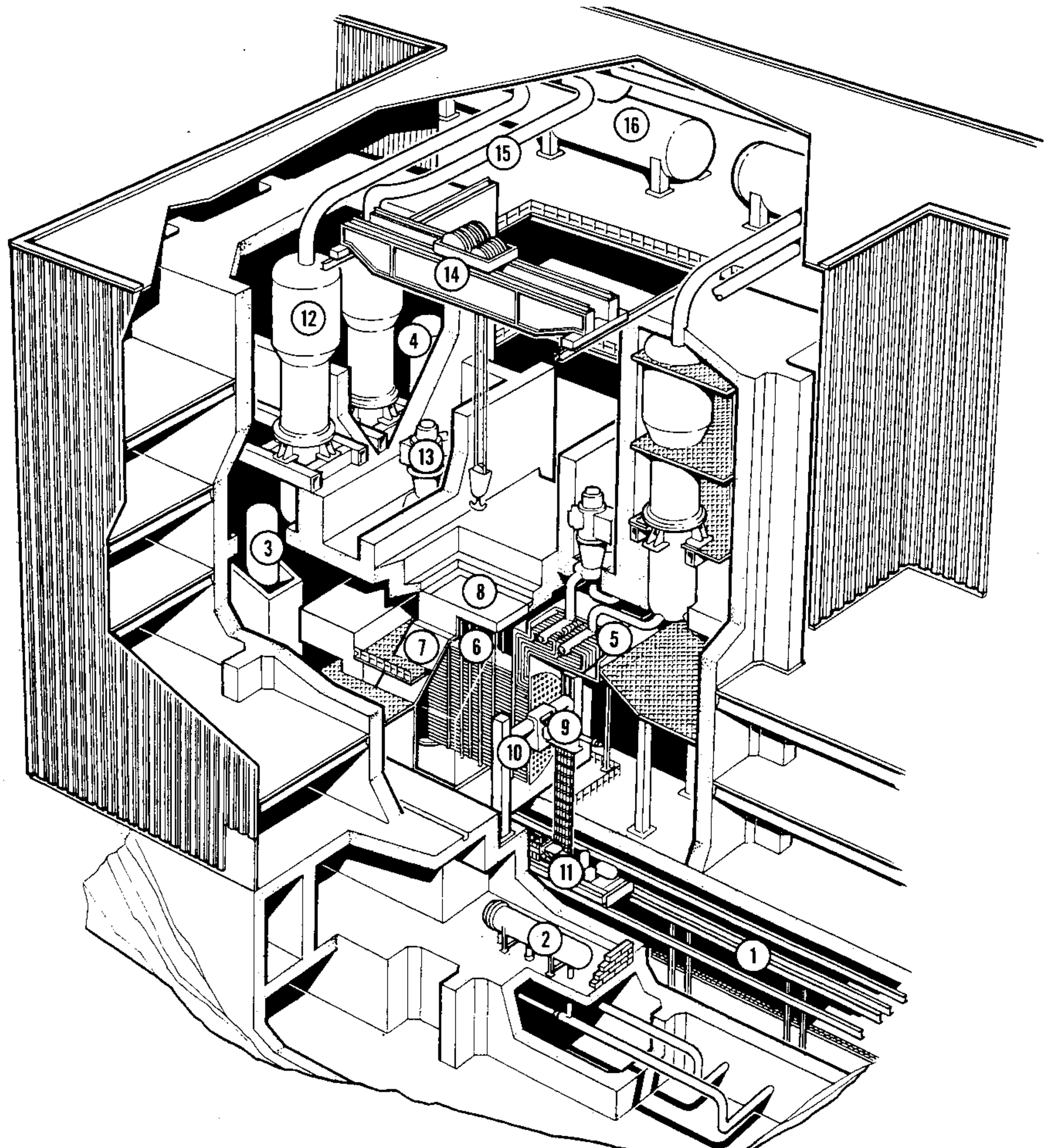
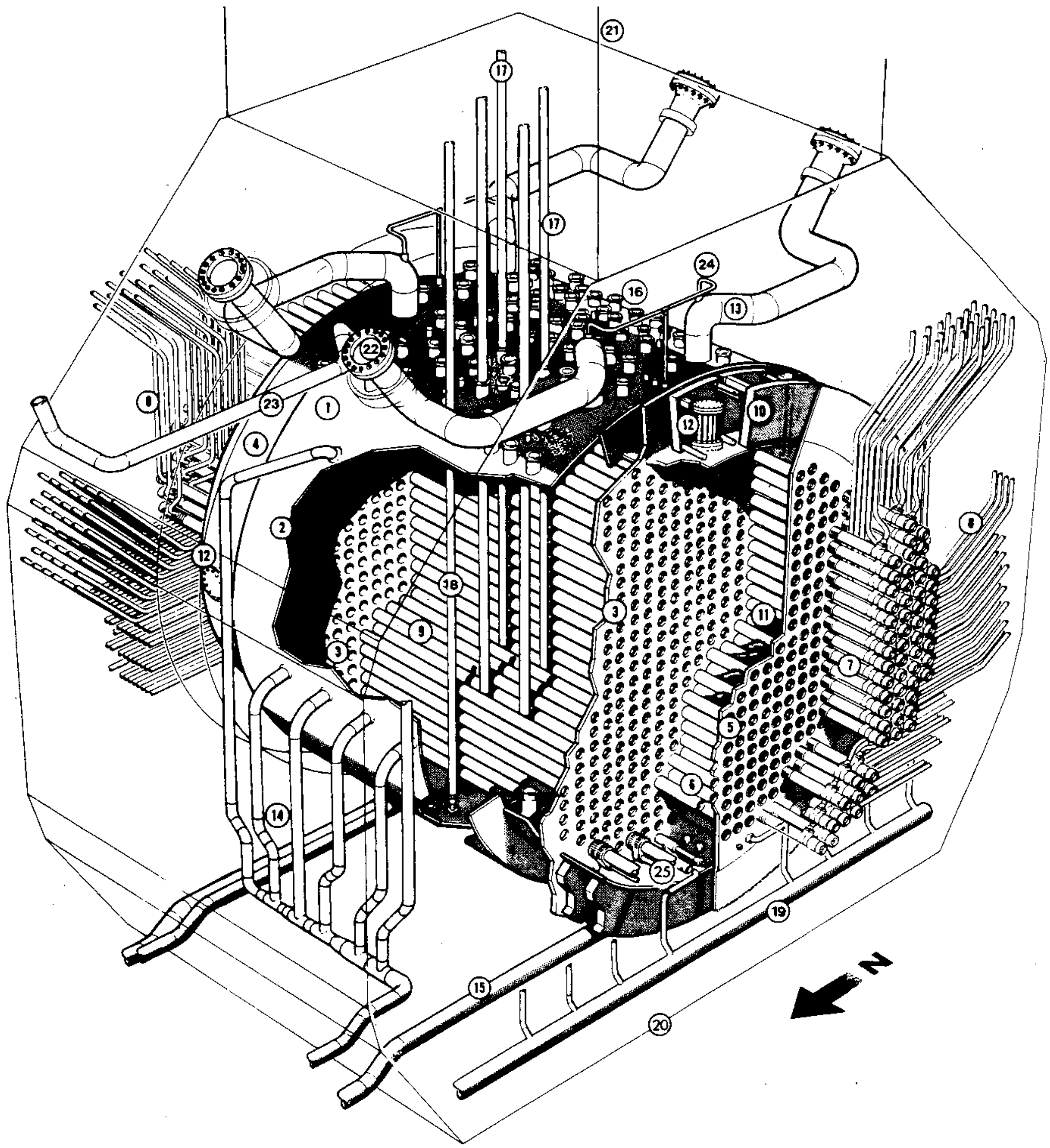


Figure 2: Darlington Station General Arrangement



1 Fuelling Duct
2 Shutdown Cooling Heat Exchanger
3 Pressurizer
4 Heavy Water Storage Tank
5 Feeder Cabinet
6 Calandria
7 Shield Tank
8 Reactivity Mechanism Deck
9 Fuelling Machine Head
10 Fuelling Machine Bridge Column
11 Fuelling Machine Transport Trolley
12 Steam Generator
13 Heat Transport Pump
14 Bridge Crane
15 Main Steam Line
16 Deaerator

Figure 3: Darlington NGS Reactor Building



1. CALANDRIA
2. CALANDRIA MAIN SHELL
3. CALANDRIA-SIDE TUBESHEET
4. CALANDRIA SUB-SHELL
5. FUELLING MACHINE-SIDE TUBESHEET
6. LATTICE TUBES
7. END FITINGS
8. FEEDERS
9. CALANDRIA TUBES
10. SHIELD TANK SOLID SHIELDING
11. STEEL BALL SHIELDING (END SHIELD)
12. MANHOLE
13. EMERGENCY DISCHARGE PIPES
14. MODERATOR INLETS
15. MODERATOR OUTLETS
16. NOZZLES FOR VERTICAL REACTIVITY CONTROL UNITS AND VIEWING PORT
17. THIMBLES FOR VERTICAL CONTROL UNITS
18. GUIDE TUBES FOR VERTICAL REACTIVITY CONTROL UNITS
19. END SHIELD COOLING PIPING
20. SHIELD TANK
21. SHIELD TANK EXTENSION
22. RUPTURE DISC ASSEMBLY
23. MODERATOR OVERFLOW
24. PRESSURE BALANCE LINES
25. INLET AND OUTLET STRAINERS

Figure 4: Reactor Assembly

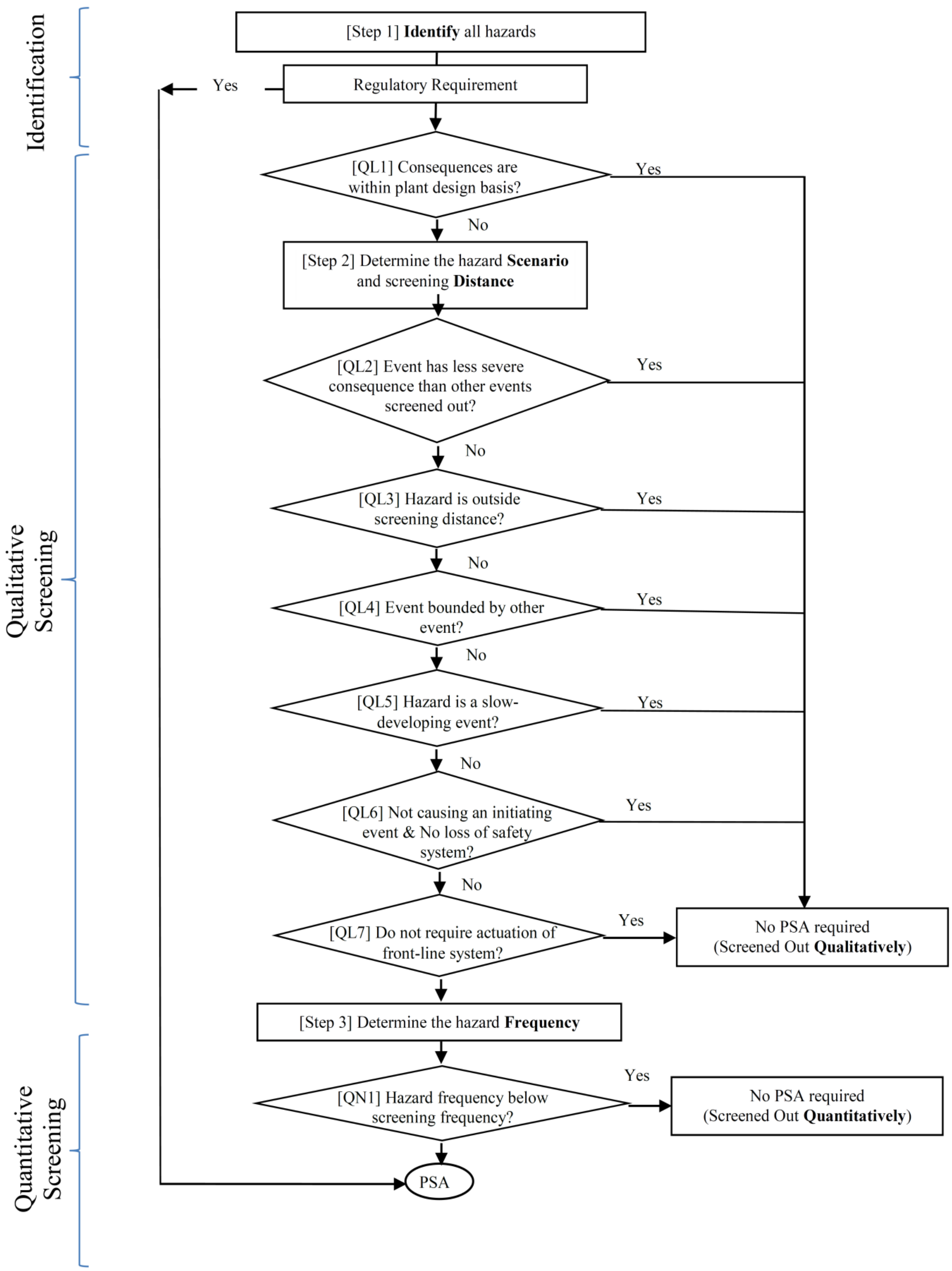


Figure 5: Hazard Screening Steps

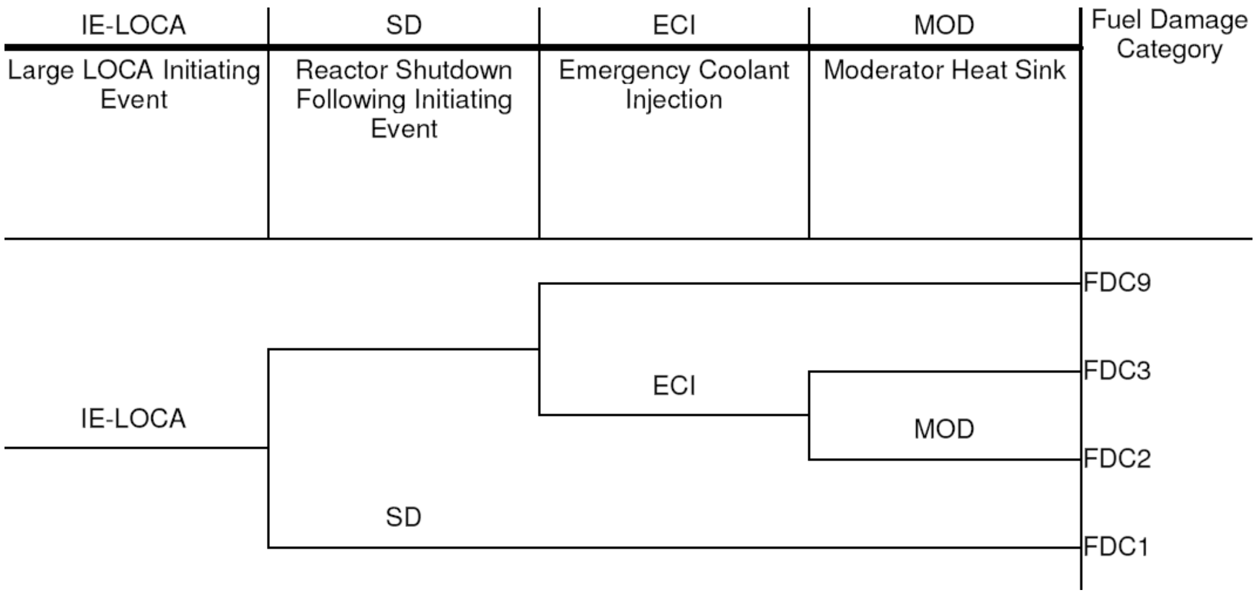


Figure 6: Example LOCA Event Tree

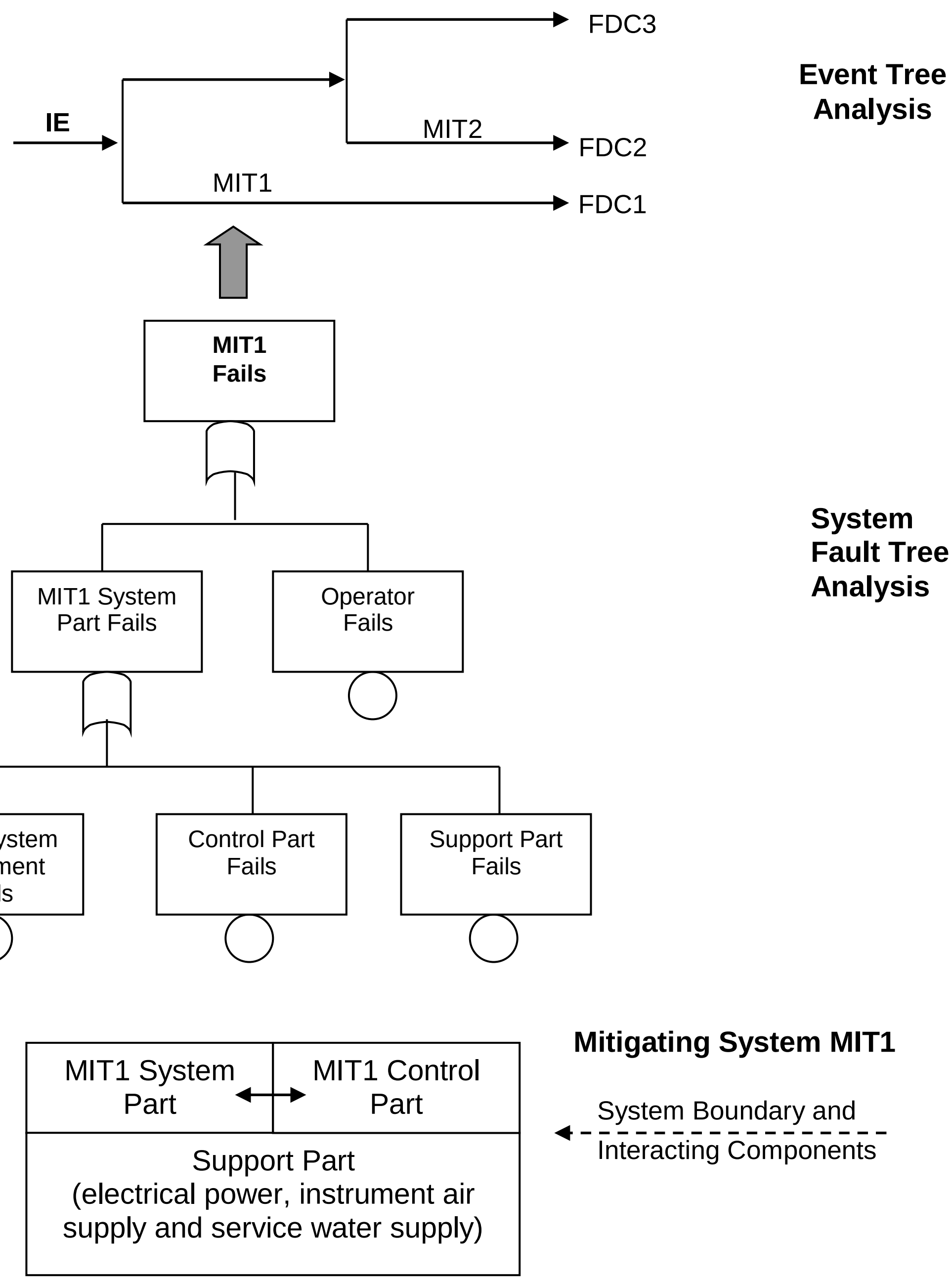


Figure 7: Fault Tree and Event Tree Integration

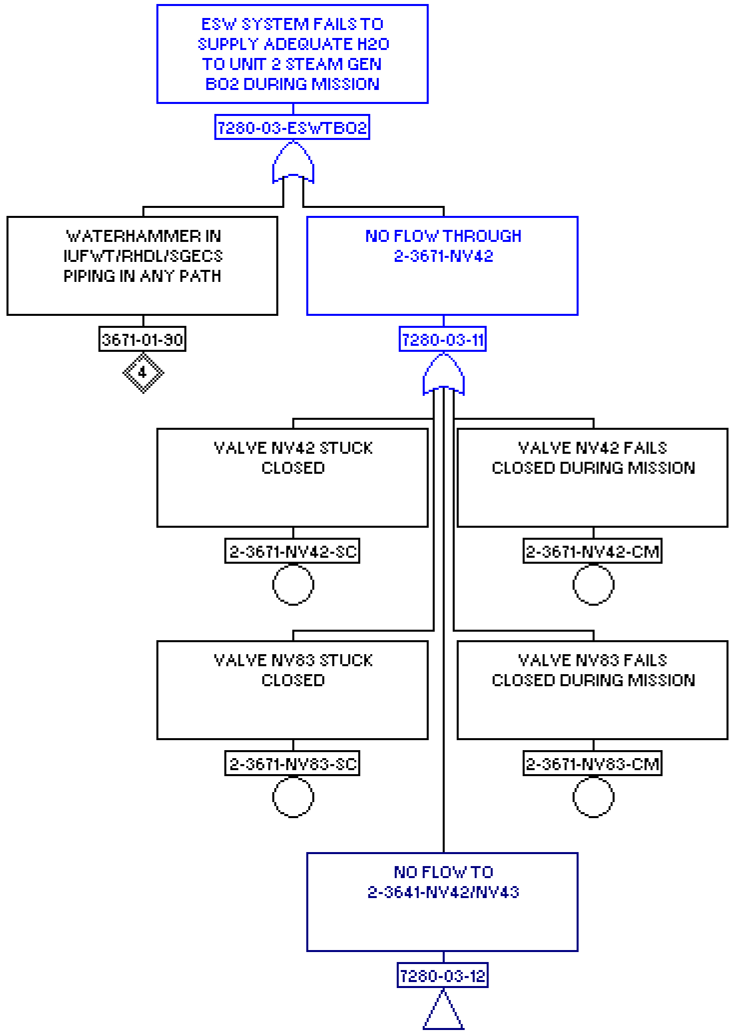


Figure 8: Example Fault Tree

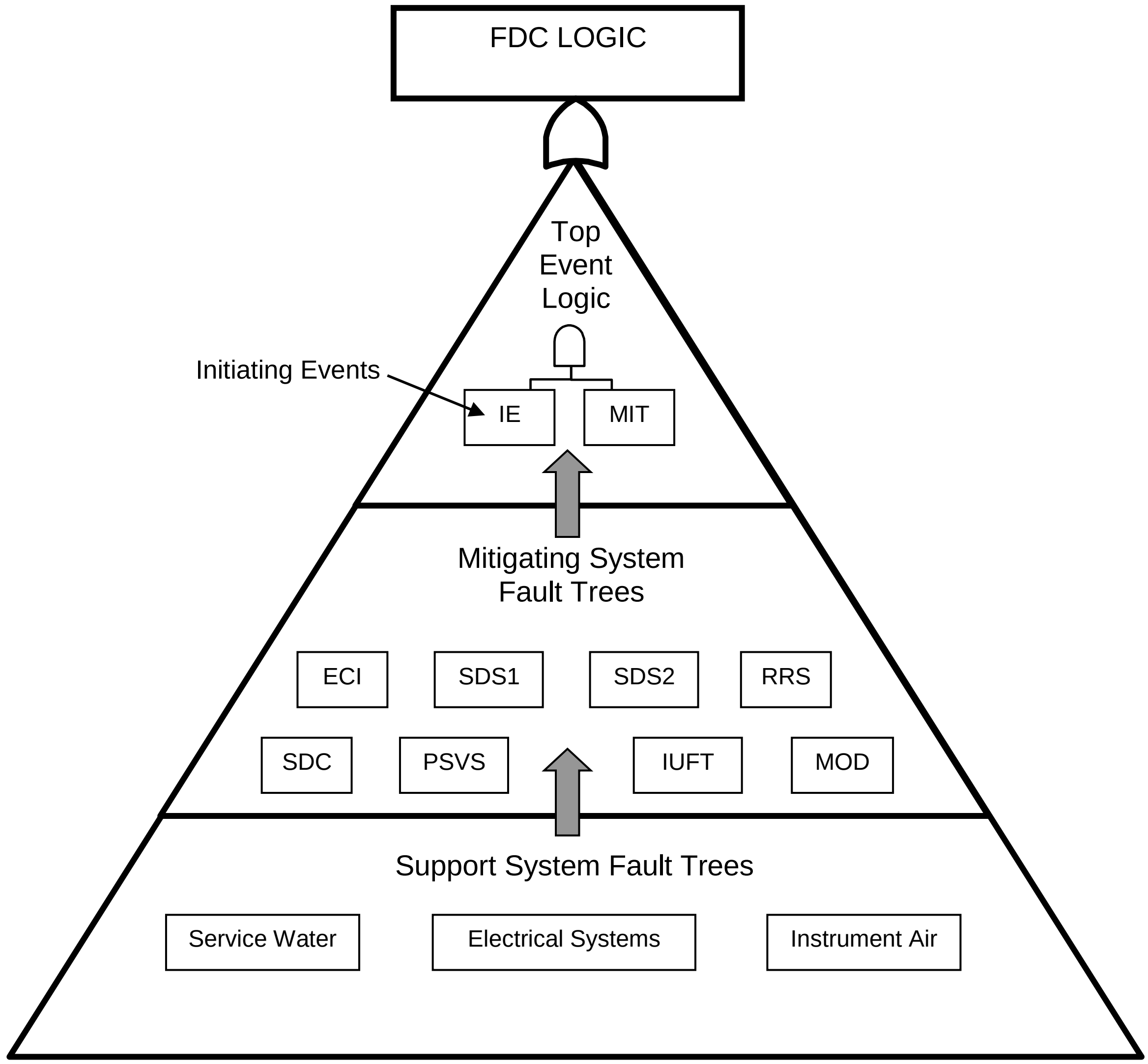


Figure 9: Fault Tree Integration

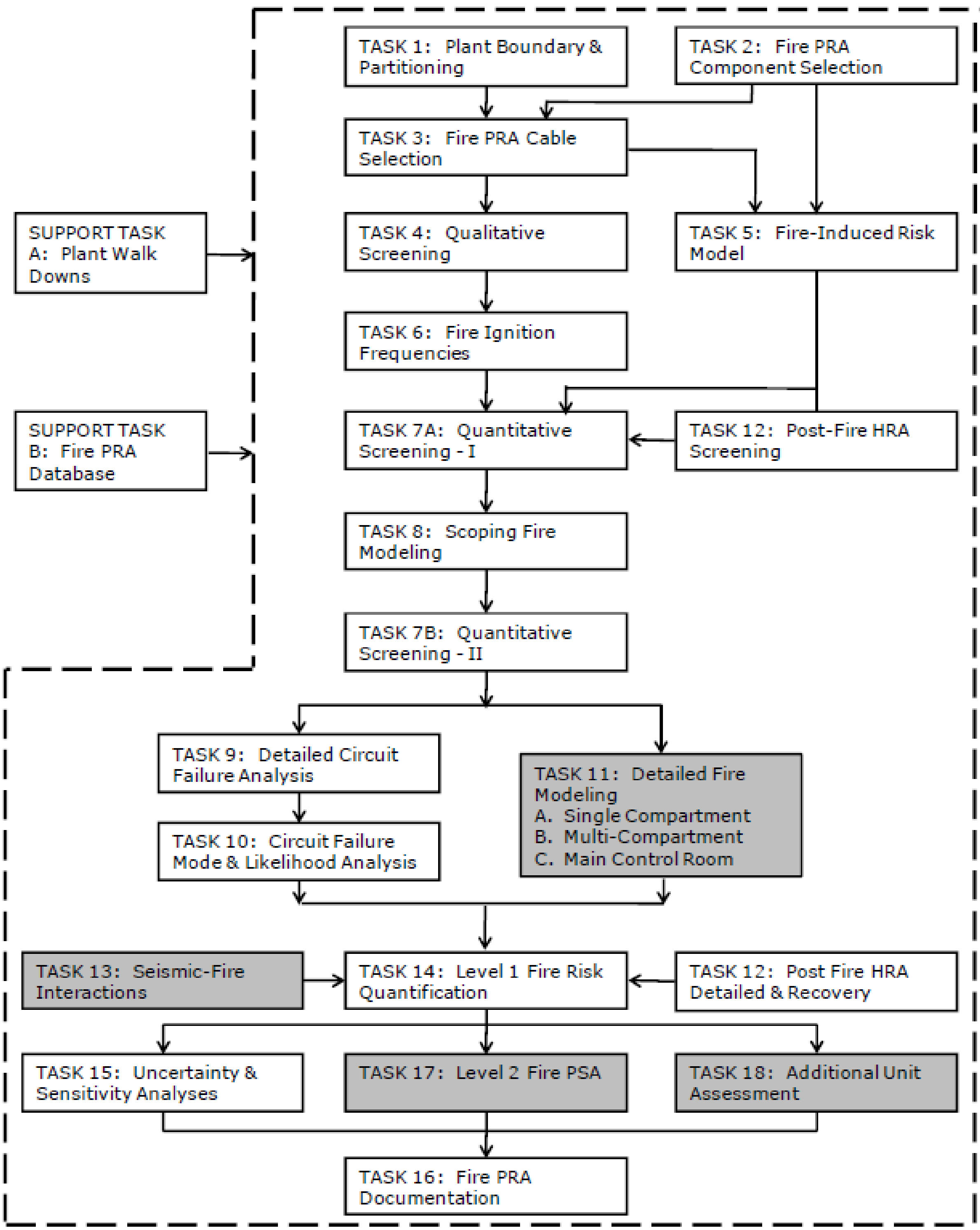


Figure 10: Fire PSA Tasks

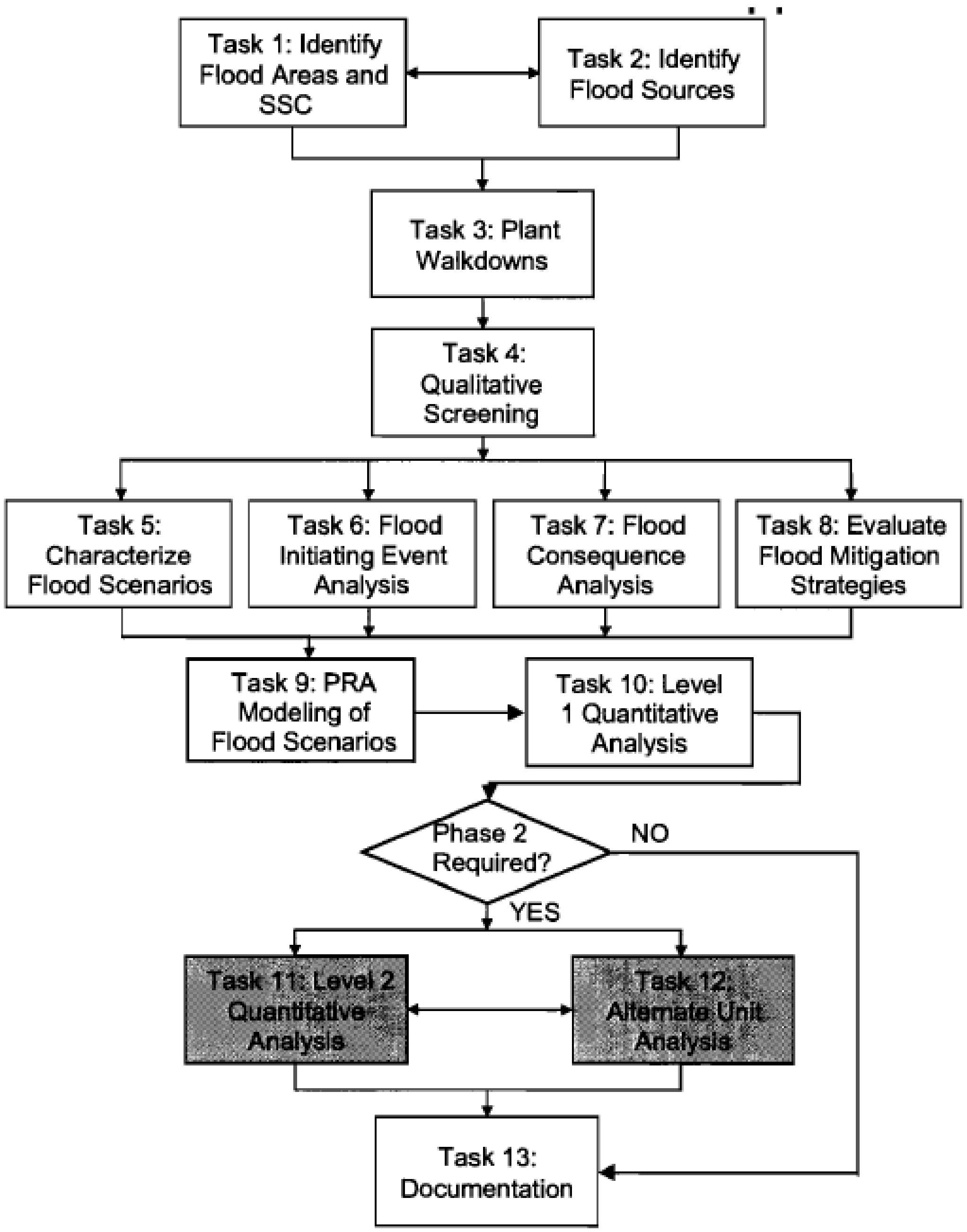


Figure 11: Internal Flood Phase 1 Tasks

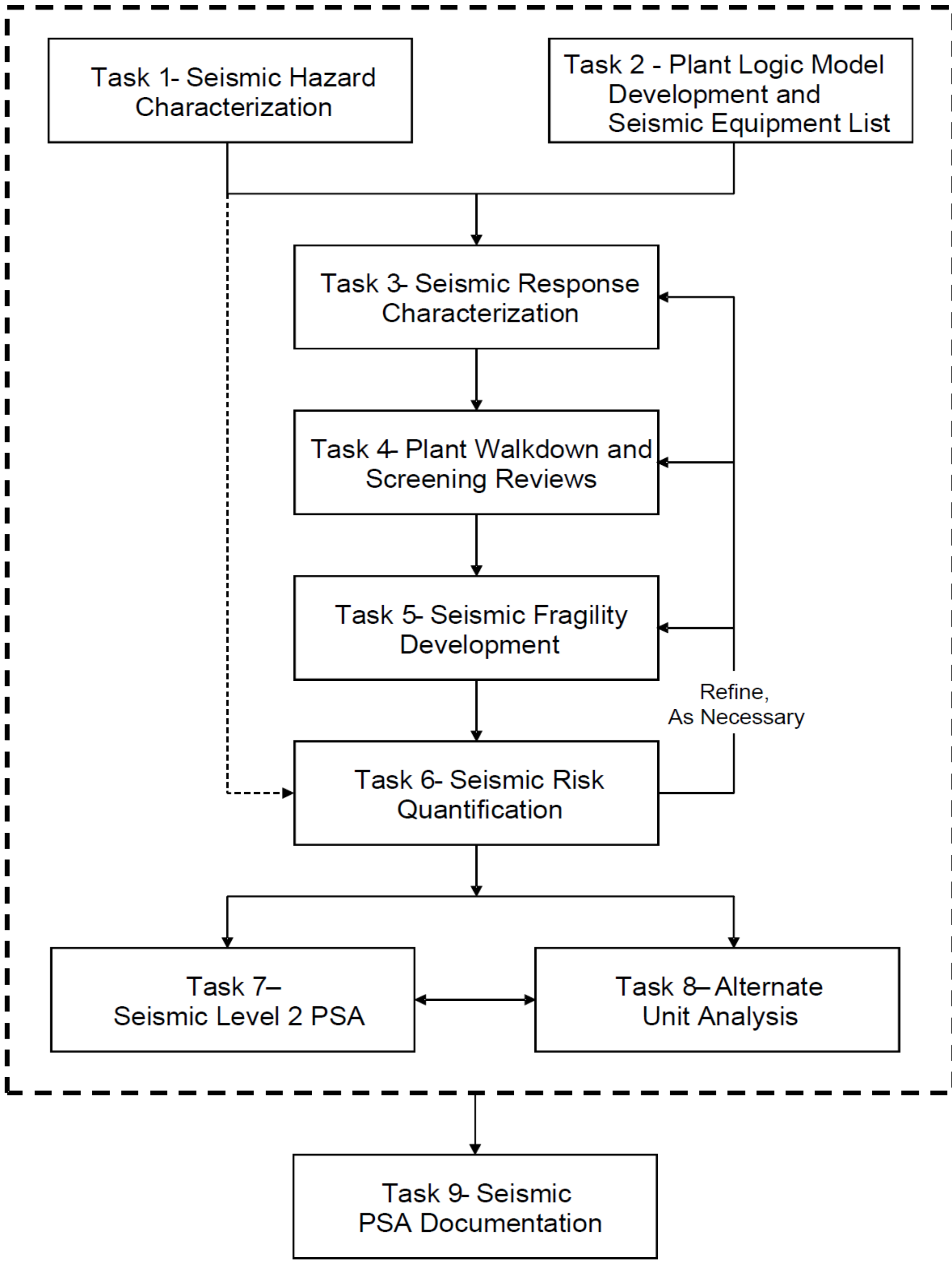


Figure 12: Seismic PSA Tasks

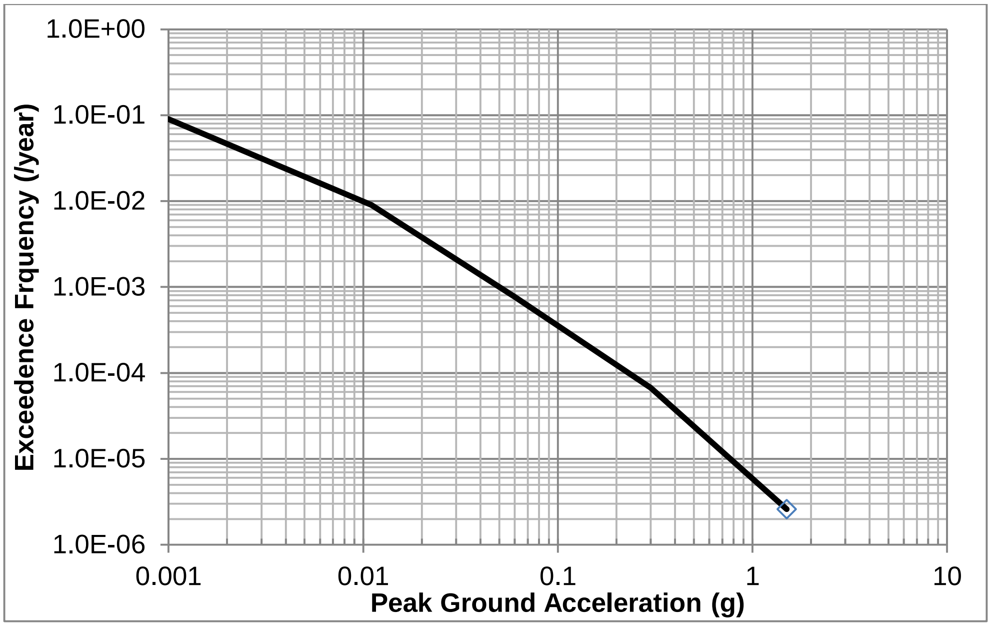


Figure 13: Example Seismic Hazard Curve

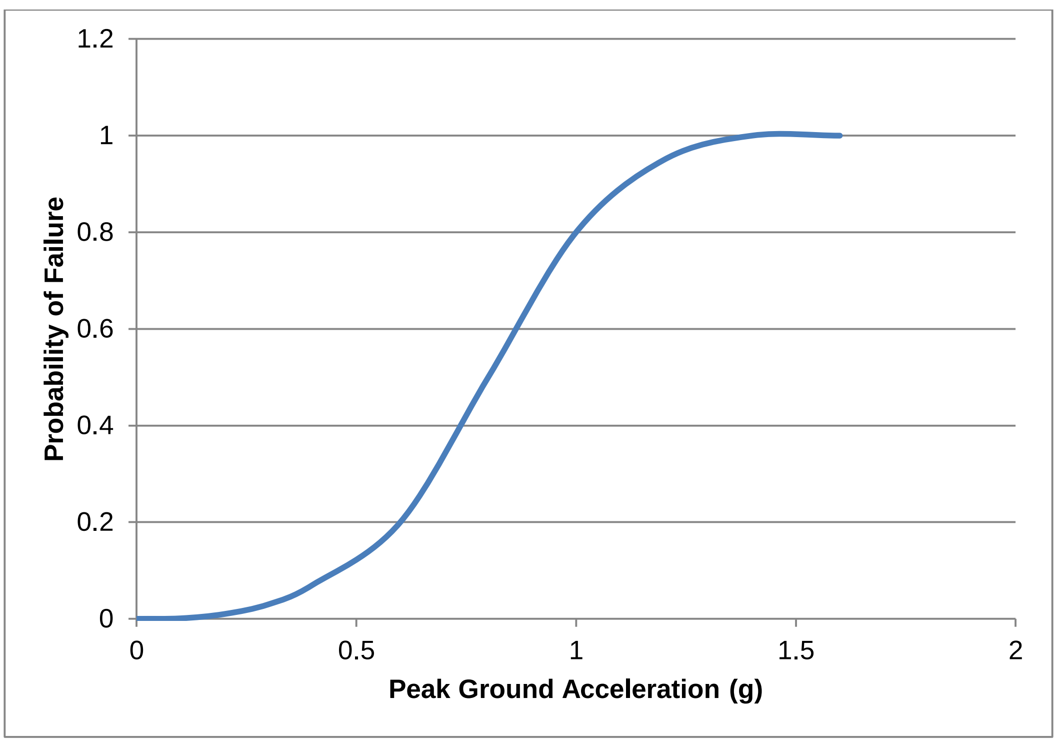


Figure 14: Example Fragility Curve

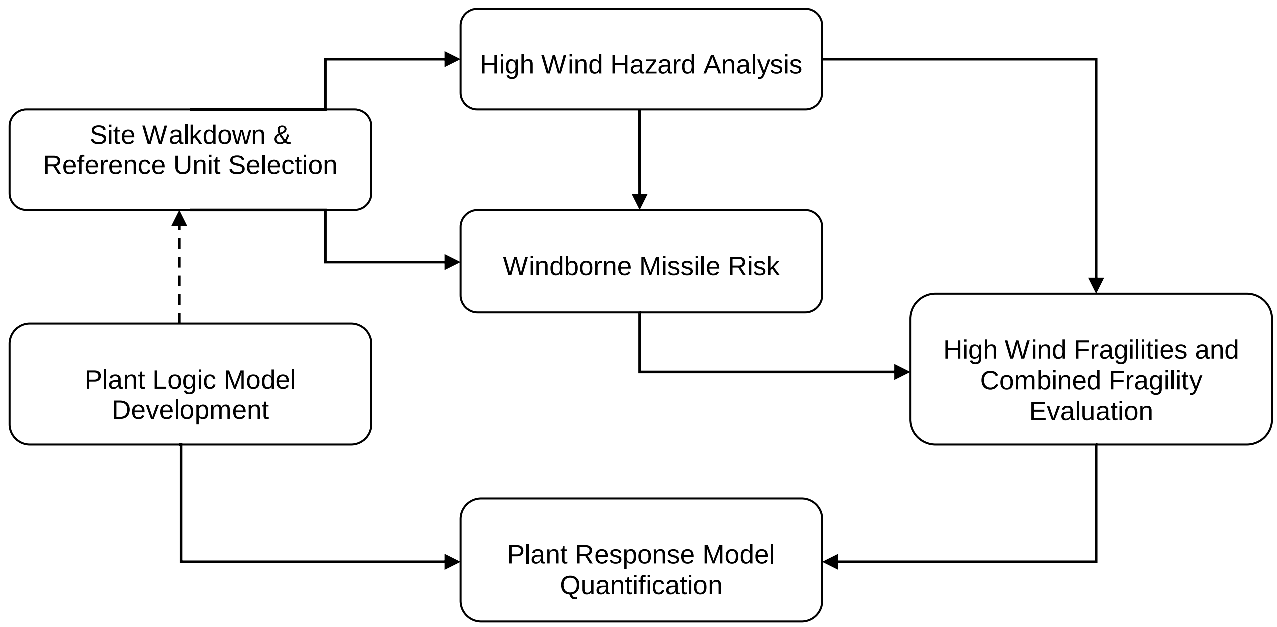


Figure 15: Overall OPG High Wind PSA Method

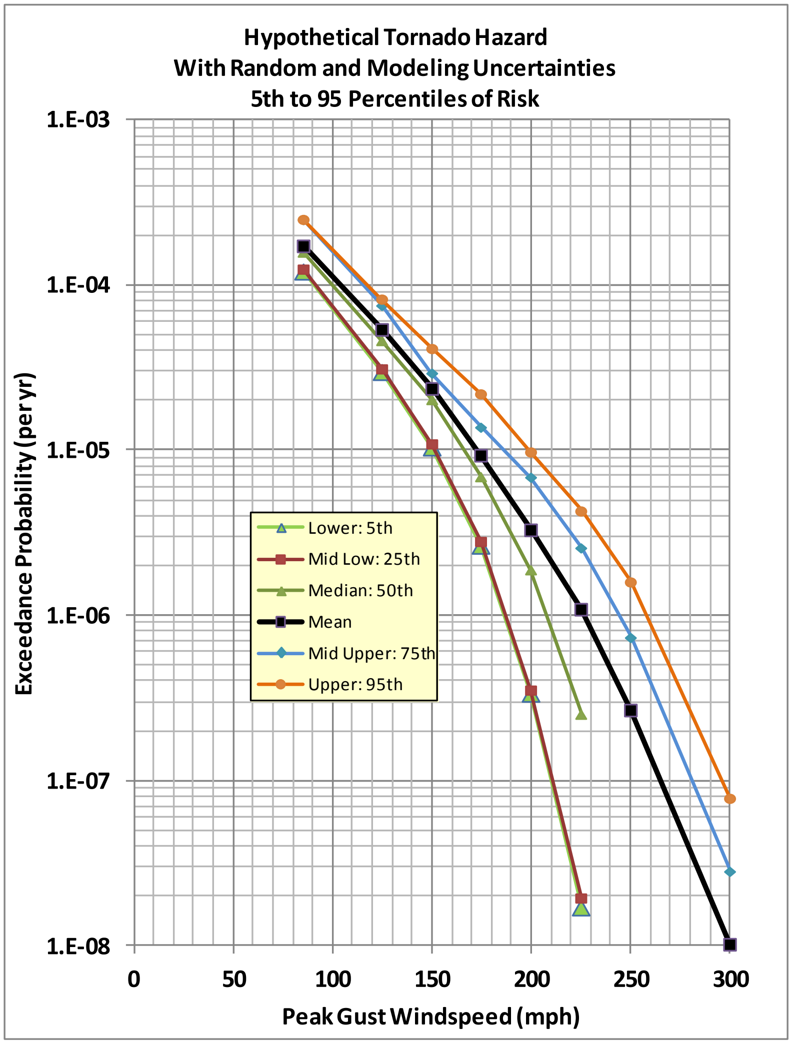


Figure 16: Example of High Wind Hazard Curves

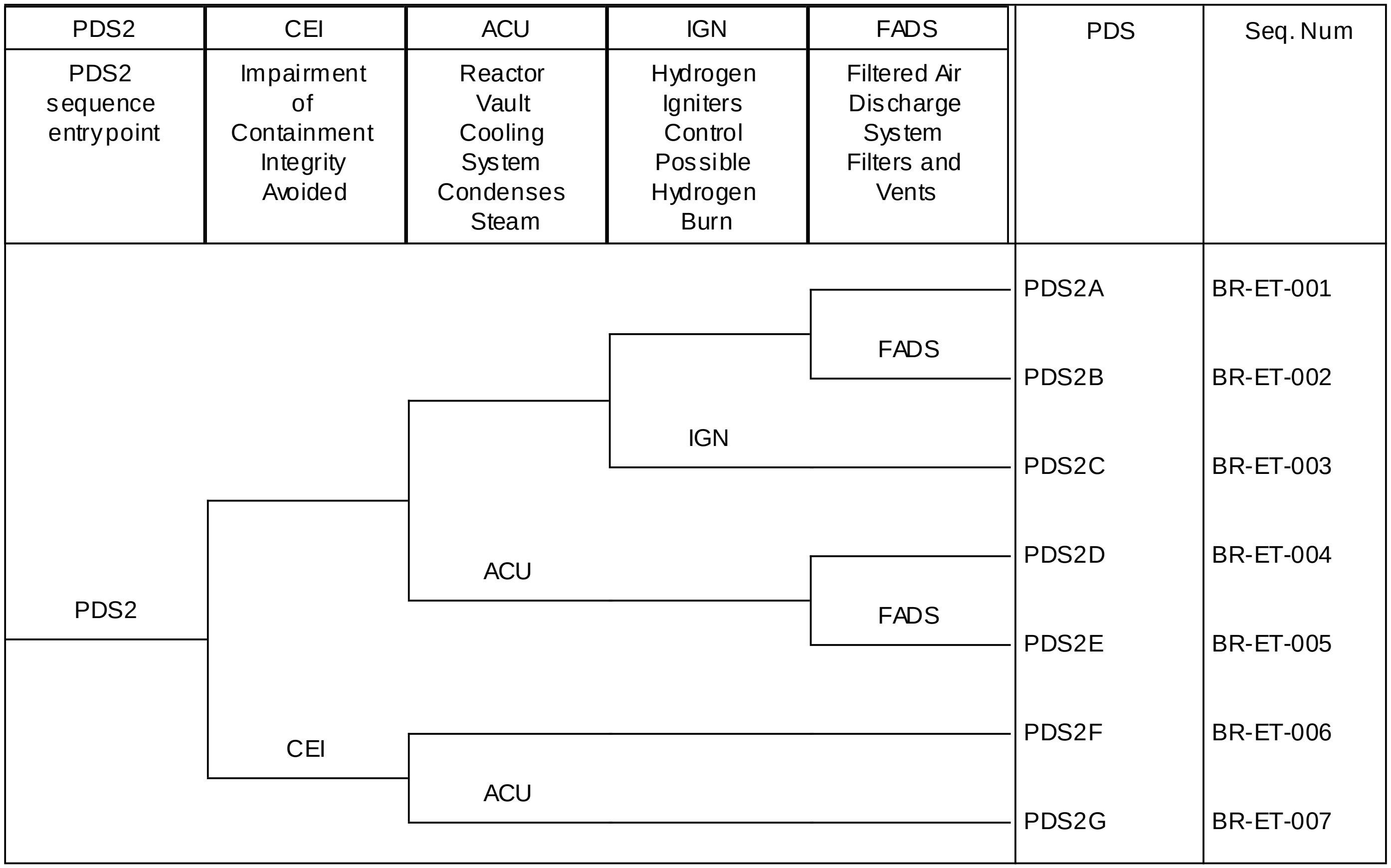


Figure 17: Darlington NGS Bridging Event Tree

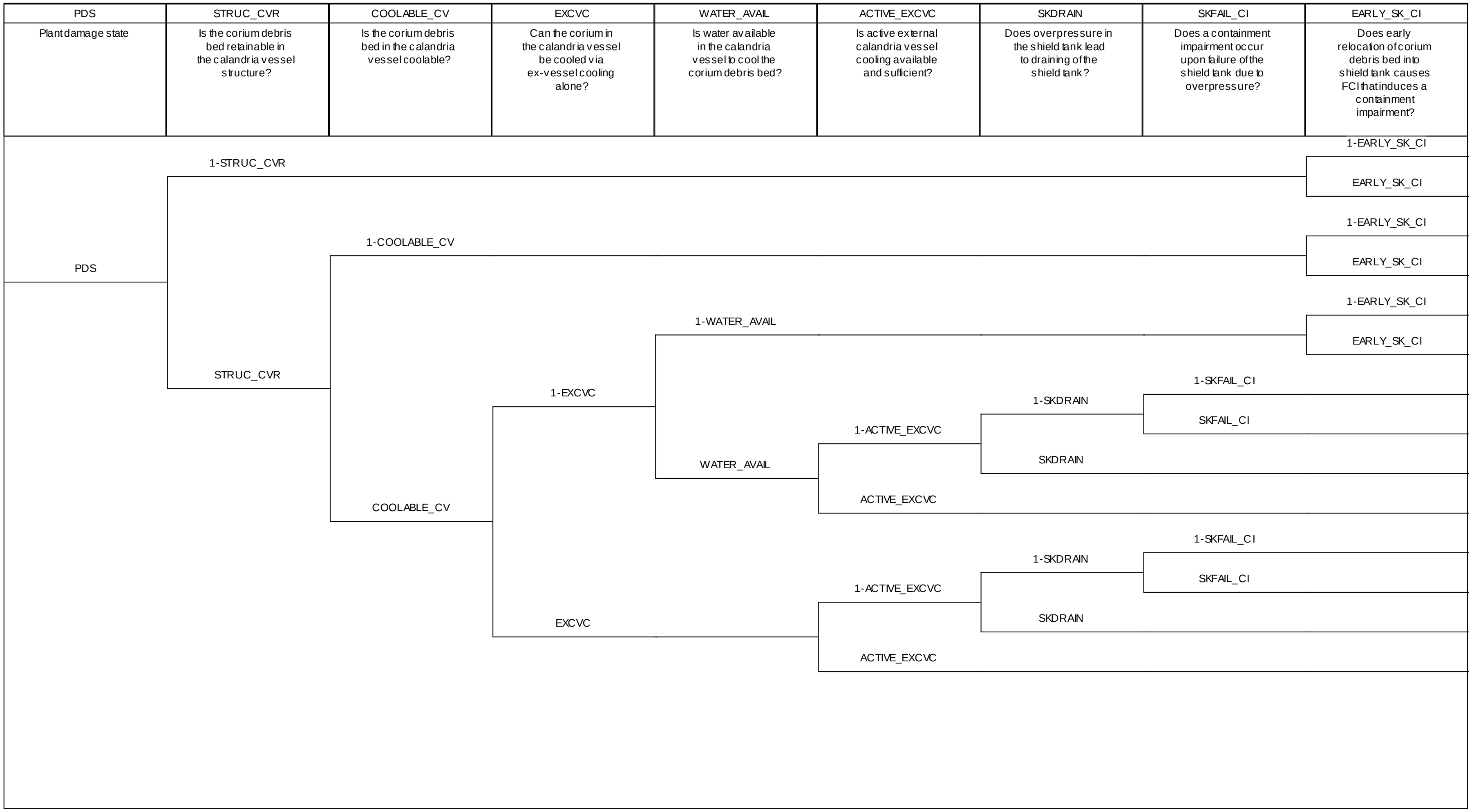


Figure 18: Simplified Containment Event Tree

Table 1: OPG Risk Based Safety Goals

SAFETY GOAL	AVERAGE RISK (PER YEAR)	
	Target	Limit
Severe Core Damage (per unit)[1]	10^{-5}	10^{-4}
Large Release (per unit)[2]	10^{-6}	10^{-5}

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

[2] Large Release is a release greater than 1 percent of the core inventory of Cs-137.

OPG's Risk Based Safety Goals are described in Reference [R-4].

Table 2: Summary of Criteria Applied for Screening of Human-Induced Hazards

Human-Induced Hazard Description	Screening
Small Airplane Crash	Screened out
Military Jet Crash	Screened out
Large Airplane Crash	Screened out
Train Accidents causing Toxic Chemical Release	Screened out
Train Accidents causing Explosion	Screened out
Road Transportation Accidents	Screened out
Small Marine Transportation Accidents	Screened out
Large Marine Transportation Vessels Accidents	Screened out
Stationary Nuclear Accidents	Screened out
Stationary Non-Nuclear Accidents causing Toxic Chemical Release	Screened out
Stationary Non-Nuclear Accidents causing Explosions	Screened out
Industrial Underground Blasts	Screened out
Industrial Dusts	Screened out
External Fires	Screened out
Orbital Debris Crash	Screened out

Table 3: Summary of Criteria Applied for Screening of Natural Hazards

Natural Hazard Description	Screening
Earthquake	PSA Required
Slope Instability	No Hazard
Subsidence	No Hazard
Soil Failure	No Hazard
Probable Maximum Flood (PMF)	Screened out
Floods due to Runoffs	Screened out
Floods due to Rivers	No Hazard
Floods due to Waves	Screened out
Floods due to Seiche	No Hazard
Floods due to Tsunami	No Hazard
Floods due to Ponds and Dams	No Hazard
Floods due to Ice-Jamming	Screened out
Extreme Low Temperature	No Hazard
Extreme High Temperature	No Hazard
Snow/Snowpack	Screened out
Freezing Rain	Screened out
Avalanche	No Hazard
Ice Storm	No Hazard
Tornado	PSA Required
High-Wind	PSA Required
Hurricane	Screened out
Lightning	No Hazard
Meteorites	Screened out
Geomagnetic Storms and Solar Flares	Screened out
Animals	Screened out

Table 4: Darlington At-Power Internal Events PSA Initiating Events

Category	Label	Description
Forced Shutdown	FSD	All reactor trips not included in other initiating events
LOCA	LOCA1A	A rupture within the capacity of the D2O transfer system and above the lower LOCA threshold (discharge rate 1-12 kg/s)
	LOCA1A-OC	(discharge rate 1-12 kg/s outside containment)
	LOCA1B	A rupture within the capacity of the D2O feed pump but beyond that of the D2O transfer system (discharge rate 12-40 kg/s)
	LOCA1B-OC	(discharge rate 12-40 kg/s outside containment)
	LOCA1C	A rupture within the capacity of two D2O feed pumps but beyond the capacity of one D2O feed pump (discharge rate 40-70 kg/s)
	LOCA2A	Small breaks within the capacity of the auxiliary moderator heat sink (break discharge rate 70-220 kg/s)
	LOCA2B	Small breaks (discharge rate 220-1000 kg/s)
	LOCA3	Transition breaks. Partial breaks which exhibit system response characteristics in between those of small and large breaks (initial discharge rate 1000-2000 kg/s)
	LOCA4	Large breaks which lead to significant flow degradation in the core (initial discharge rate >2000 kg/s)
	LOCATOP	A LOCA2 size break in HT piping connected to the top of the pressurizer
	LOCA1-SF	Stagnation feeder break in LOCA1 range
	LOCA2-SF	Stagnation feeder break in LOCA2 range
	LOCA2-SDC	A LOCA2 size break in the PHT-SDC interface piping inside an SDC room
Pressure Tube Rupture	PTF	Pressure tube break resulting in a discharge rate in excess of 1 kg/s
Pressure Tube Leak	PTL	Pressure tube break resulting in a discharge rate of less than 1 kg/s
End-fitting Failure	EFL1WAGA	LOCA1A size break inside annulus gas bellows
	EFL1WAGB	LOCA1B size break inside annulus gas bellows
	EFL1WAGC	LOCA1C size break inside annulus gas bellows
	EFL1OAGA	LOCA1A size break outside annulus gas bellows
	EFL1OAGB	LOCA1B size break outside annulus gas bellows
	EFL1OAGC	LOCA1C size break outside annulus gas bellows

Category	Label	Description
	EFL1FMIA	LOCA1A size break involving the fuelling machine
	EFL1FMIB	LOCA1B size break involving the fuelling machine
	EFL1FMIC	LOCA1C size break involving the fuelling machine
	EFL2WAG	LOCA2 size break inside annulus gas bellows
	EFL2OAG	LOCA2 size break outside annulus gas bellows
	EFL2FMI	LOCA2 size break involving the fuelling machine
Steam Generator Tube Rupture	SGTB1	SG single tube break (initial discharge rate 1 kg/s – 12 kg/s)
	SGTB2	SG multiple tube break (>12 kg/s)
Loss of HT Pressure Control (Low)	LRVO	One or more liquid relief valves fail open (base event)
	FVFC	Both D2O feed valves fail closed (base event)
	SBVO	Any pressurizer steam bleed or relief valve fails open
Loss of HT Pressure Control (High)	PHFO	Pressurizer heaters energized spuriously
	BVFC	Both HT bleed valves fail closed
	FVFO	Any D2O feed valve fails open
	FP2S	Inadvertent start-up of inactive feed pump
	BCLCVFC	Bleed condenser level control valves fail closed
	PSBVFC	Pressurizer steam bleed valves fail closed when required open
HT Pressure and Inventory Control Failures	D2OFDL	Pipe break in D2O feed system upstream of check valve NV61
	FBSICL	Feed/bleed system pipe break inside containment
	XSPR	Bleed condenser spray valve CV12 opens spuriously
HT Pump Trip	HTPT1	Pump trip in 2/2 mode
Channel Flow Blockage	LFB	Channel flow reduced by 70% or more
Moderator Failure	LOCOOL	Loss of moderator cooling resulting in setback
	SLOMA	Loss of moderator inventory within capacity of moderator D2O recovery system (discharge rate 1-70 kg/s)
	LLOMA	Loss of moderator inventory beyond capacity of moderator D2O recovery system (discharge rate >70 kg/s)
Loss of End Shield Cooling	LOESHS	Loss of end shield heat sink

Category	Label	Description
	LOESF	Total loss of end shield flow
	LOESI1	Non-isolable pressure boundary rupture
	LOESI2A	Rupture upstream of V15/16 where isolation leads to loss of circulation
	LOESI2B	Rupture upstream of V15/16 where isolation does not lead to loss of circulation
Steam Line Break	SSLB1	Small break that requires reactor shutdown but does not cause global harsh environment
	SSLB3	A Feedwater Line Break downstream of the last check valve before the steam generator (assumed to be in SG1 flowpath)
	100SBH-ADJN	100% Steam Balance Header Break in a unit adjacent to the analyzed unit, North of Column Line 11 with potential for in-plant environmental consequences
	100SBH-U2N	Unit 2 100% Steam Balance Header Break, North of Column Line 11 with in-plant environmental consequences
	SRV	Any SRV, ASDV or CSDV opens spuriously
Loss of Feedwater to Steam Generators	LOFWB	LOFW resulting in reactor trip but greater than 3% full flow remains
	LOFWC	LOFW to less than 3% full flow
Feedwater Line Break	SFLB1	Break resulting in reactor shutdown but with sufficient water remaining to remove decay heat
	100LFB-ADJN	100% Feedwater Line Break in an Adjacent Unit, North of Column Line 11
	100FLB-U2N	Unit 2 100% Feedwater Line Break, North Column Line 11, Causing Total Loss of Feedwater
	100FLB-U2S	Unit 2 100% Feedwater Line Break, South of Column Line 11, Causing Total Loss of Feedwater
	FLBSG	Isolable break downstream of LCVs resulting in total loss of feedwater to one steam generator (assumed to be in SG1 flowpath)
	FLBCOND1	Break in condensate system resulting in total loss of feedwater
Turbine Trip	TT	All turbine trips not included in other initiating events
Loss of Condenser Vacuum	LOVAC	Loss of condenser vacuum resulting in turbine trip
High Pressure Reheater Drains Line Break to Steam Generator	RDLB	Break in lines between steam generators and second check valve (assumed to be in SG1 flowpath)

Category	Label	Description
Loss of Condensate Flow	LOCOND	Total loss of condensate flow to deaerator
Unplanned Bulk Increase in Reactivity	UFBIR	Unplanned fast (>0.2 mk/s) bulk increase in reactivity
	USBIR	Unplanned slow (<0.2 mk/s) bulk increase in reactivity
Unplanned Regional Increase in Reactivity	URIR	Local neutron overpower
Loss of Computer Control	WDTOX	Controlling computer stall
	DCCF	Dual computer failure
	DCCUF	Unsafe failure of DCC leading to reactor power increase
	HTPF SGLCF SGPCF MTCF DLCF	Failure 'off' of an individual control program on both computers
Loss of Low Pressure Service Water System	LOLPSW	Total loss of LPSW flow out of header L205
	LOPH	Loss of flow to pumphouse
	LOTH	Loss of flow to turbine hall
Loss of Recirculated Cooling Water System	LORCW	Total loss of RCW flow
Loss of Powerhouse Upper Level Service Water	LOPULSW	Total loss of PULSW flow
Loss of Instrument Air	TLOIA	Total loss of instrument air out of line L17
Loss of Cooling to F/M in Transit	LOFMCIT	Loss of cooling to fuelling machine in transit
Loss of Bulk Electricity Supply	LOBES	Loss of BES
Loss of Switchyard	LOSWYD	Loss of both switchyard buses BU1 and BU2
Loss of Power to Unit Class IV 13.8 kV Bus	LOCL4	Total loss of Unit Class IV 13.8 kV power
	LOBU1 LOBU2 LOBU3 LOBU4	Loss of power to Unit Class IV 13.8 kV bus BU1 Loss of power to Unit Class IV 13.8 kV bus BU2 Loss of power to Unit Class IV 13.8 kV bus BU3 Loss of power to Unit Class IV 13.8 kV bus BU4
Partial Loss of Unit Class IV Power	FS1CB2 FS2CB2	Loss of Unit Class IV 13.8 kV buses BU1 and BU3 due to 1CB2 failing short Loss of Unit Class IV 13.8 kV buses BU2 and BU4 due to 2CB2 failing short

Category	Label	Description
Partial Loss of Unit Class III Power	LOBU7 LOBU8	Loss of power to Unit Class III 4.16 kV bus BU7 Loss of power to Unit Class III 4.16 kV bus BU8
	LOBU13 LOBU14 LOBU15 LOBU16	Loss of power to Unit Class III 600 V bus BU13 Loss of power to Unit Class III 600 V bus BU14 Loss of power to Unit Class III 600 V bus BU15 Loss of power to Unit Class III 600 V bus BU16
Partial Loss of Unit Class II 120 V Power	LOBUA3 LOBUB3 LOBUC3	Loss of Unit Class II 120 V ac bus BUA3 Loss of Unit Class II 120 V ac bus BUB3 Loss of Unit Class II 120 V ac bus BUC3
Partial Loss of Unit Class II 45 V Power	LO45VA LO45VB LO45VC	Loss of Unit Class II 45 V dc at panel 2383-11 Loss of Unit Class II 45 V dc at panel 2859-21 Loss of Unit Class II 45 V dc at panel 3485-C1
Partial Loss of Unit Class I 48 V Power	LOBUA4 LOBUB4 LOBUC4 LOBUA141 LOBUB141	Loss of Unit Class I 48 V dc bus BUA4 Loss of Unit Class I 48 V dc bus BUB4 Loss of Unit Class I 48 V dc bus BUC4 Loss of Unit EPS 48 V dc bus BUA141 Loss of Unit EPS 48 V dc bus BUB141
Loss of Forebay	FOREBAY	Loss of Forebay leading to loss of Circulating Water System; may also lead to loss of Low Pressure Service Water and/or Emergency Service Water
ECI Blowback	BLOWBACK	Blowback of HT system D2O at high pressure outside containment via ECI piping
Powerhouse Freeze	PHFREEZE	Spurious opening of powerhouse venting dampers during extreme cold outside condition.

Table 5: DARA Fuel Damage Categories

FDC	Definition	Typical Events in FDC
1	Rapid loss of core structural integrity.	Positive reactivity transient and failure to shutdown.
2	Slow loss of core structural integrity.	Loss of coolant accident (LOCA) with failure of emergency coolant injection system (ECIS) and failure of moderator heat sink.
3	Moderator required as heat sink in the short-term (< 1 hr after reactor trip).	LOCAs of LOCA2B size or greater and failures of ECIS on demand or during mission.
4	Moderator required as heat sink in the intermediate term (1 to 24 hr after reactor trip).	LOCAs of LOCA2A size or greater and failure of emergency coolant recovery (ECR). Total loss of secondary side heat sink with ECI successful.
5	Moderator required as heat sink in the long-term (> 24 hr after reactor trip).	LOCA1 and failures of D2O make up and ECR.
6	Temporary loss of cooling to fuel in many channels.	LOCA4.
7	Single channel fuel failure with sufficient release of steam or radioactivity to initiate automatic containment button-up.	In-core LOCA with end-fitting release End-fitting LOCA2B and fuel ejection. LOCA2A stagnation feeder break.
8	Single channel fuel failure with insufficient release of steam or radiation activity to initiate automatic containment button-up.	Large flow blockage (no end-fitting release). LOCA1 stagnation feeder break. Loss of F/M cooling in transit.
9	LOCAs with no fuel failure (ECIS successful); potential for significant economic impact.	LOCA2A, LOCA2B and LOCA3. LOCA1 with no D2O makeup.

Table 6: List of Systems Modelled by Fault Trees

System Name	L1 At-Power	L1 Outage	Level 2 At-Power
Heat Transport Liquid Relief, Pressure and Inventory Control and D_2O Storage Systems	Y	Y	*
Heat Transport Circulation System And Heat Transport Pump Gland Seal LOCA	Y	Y	*
Shutdown Cooling System	Y	Y	*
Moderator System	Y	Y	*
Boiler Feedwater System	Y	Y	*
Condensate and Makeup Systems	Y	Y	*
Steam Relief and Bypass System	Y	Y	*
Digital Control Computer System	Y	Y	*
OH180 Programmable Controller and PK Buffer System	Y	Y	*
Class IV Power Distribution System	Y	Y	*
Class III Power Distribution System	Y	Y	*
Class II Power System	Y	Y	*
Class I Power System	Y	Y	*
Emergency Power Supply System	Y	Y	*
Standby Generators	Y	Y	*
Emergency Power Generators System	Y	Y	*
Low Pressure Service Water System	Y	Y	*
Recirculated Cooling Water System	Y	Y	*
Powerhouse Upper Level Service Water System	Y	Y	*
Emergency Service Water System	Y	Y	*
Unit Instrument Air System	Y	Y	*
Common Instrument Air System	Y	Y	*
Reactivity Control System	Y	N	*
Shutdown System No. 1	Y	N	*
Shutdown System No. 2	Y	N	*
Emergency Coolant Injection System	Y	Y	*
Emergency Coolant Injection System: Blowback	Y	N	*
Inter-Unit Feedwater Tie System	Y	Y	*
D_2O Recovery and Transfer Systems	Y	Y	*
Room Air Conditioning System	Y	Y	*
Hostile Environment Events (including Powerhouse Emergency Venting System)	Y	Y	*
Annulus Gas System	Y	N	*
Emergency Mitigating Equipment	Y	N	*

System Name	L1 At-Power	L1 Outage	Level 2 At-Power
Containment Envelope Integrity System	N	N	Y
Reactor Vault Atmosphere Cooling System	N	N	Y
Post-Accident Hydrogen Ignition System	N	N	Y
Emergency Filtered Air Discharge System	N	N	Y

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

Note: Fire, seismic, flooding, and high wind risk is calculated through modifications or interrogations based on the integrated severe core damage model from the Internal Events At-Power Level 1 PSA, and do not include specific fault tree models for the individual plant systems.

Table 7: DARA-L1O Plant Operational State Definition

<table>
<tr><th rowspan="2">Input Parameter</th><th colspan="5">Plant Operational State (POS)</th></tr>
<tr><th>A</th><th>B</th><th>C</th><th>D</th><th>E</th></tr>
<tr><td>GSS</td><td>OPGSS</td><td>OPGSS</td><td>OPGSS</td><td>DGSS</td><td>OPGSS</td></tr>
<tr><td>HTS Inventory Level</td><td>Full</td><td>GFS</td><td>LLDS</td><td>LLDS</td><td>Full</td></tr>
<tr><td>HTS Boundary Configuration</td><td>Closed</td><td>Closed</td><td>Open</td><td>Open</td><td>Closed</td></tr>
<tr><td>HTS Temp (Nominal)</td><td><60°C</td><td>30°C</td><td>30°C</td><td>30°C</td><td>55°C</td></tr>
<tr><td>HTS Pressure</td><td>Pressurized 4.3-7.5 MPa</td><td>Depressurized < 1.0 MPa</td><td>Depressurized ~0 kPa(g)</td><td>Depressurized ~0 kPa(g)</td><td>Pressurized 4.3-7.5 MPa</td></tr>
<tr><td>Primary Heat Sink (Circulation)</td><td>HTS Pumps or SDC Pumps</td><td>SDC Pumps</td><td>SDC Pumps</td><td>SDC Pumps</td><td>HTS Pumps or SDC Pumps</td></tr>
<tr><td>Primary Heat Sink (Heat Removal)</td><td>SDC HXs</td><td>SDC HXs</td><td>SDC HXs</td><td>SDC HXs</td><td>SDC HXs</td></tr>
<tr><td>Backup Heat Sink (Circulation)</td><td>SDC Pumps or HTS Pumps [Note1]</td><td rowspan="2">Various (SDC, NC, HTS Pumps and Steam Generators)</td><td rowspan="2">Various (SDC, NC, HTS Pumps and Steam Generators)</td><td rowspan="2">Various (SDC, NC)</td><td>SDC Pumps or HTS Pumps [Note1]</td></tr>
<tr><td>Backup Heat Sink (Heat Removal)</td><td>Steam Generators</td><td>Steam Generators</td></tr>
<tr><td>Outage Day Number (Average Duration)</td><td>1-4 (4.0 days)</td><td>37-48 (11.8 days)</td><td>5-30 (25.9 days)</td><td>31-36 (6.5 days)</td><td>49-53 (4.8 days)</td></tr>
</table>

Note 1: If HTS pumps are the primary shutdown heat sink circulation method, then SDC pumps are the backup (and vice versa).

Table 8: Initiating Events (IEs) for Darlington Level 1 Outage PSA

Outage IE Label	IE Definition	POS Applicability				
		A	B	C	D	E
Loss of Moderator Inventory						
LOMA	Loss of moderator inventory leading to a drained moderator when initially in OPGSS	Y	N	N	N	Y
Failures of the HT or SDC System Boundaries						
LOCA1	Small non-isolatable breaks inside containment from a pressurized HTS, within the capacity of two D_2O feed pumps	Y	N	N	N	Y
LK1A	Small non-isolatable leak inside containment from a depressurized HTS, within the capacity of D_2O transfer	N	Y	Y	Y	N
LK1B	Small non-isolatable leak inside containment from a depressurized HTS, within the capacity of one D_2O feed pump	N	Y	Y	Y	N
LK1C	Small non-isolatable leak inside containment from a depressurized HTS, within the capacity of two D_2O feed pumps	N	Y	Y	Y	N
LLOCA	Non-isolatable breaks inside containment from a pressurized HTS, beyond the capacity of two D_2O feed pumps	Y	N	N	N	Y
LOCA2-OUTAGE	Non-isolatable breaks inside containment from a depressurized HTS, beyond the capacity of two D_2O feed pumps	N	Y	Y	Y	N
LOCA1-OC	Small breaks outside containment from a pressurized HTS, within the capacity of one D_2O feed pump	Y	N	N	N	Y
LK1-OC	Small leak outside containment from a depressurized HTS, within the capacity of one D_2O feed pump	N	Y	Y	Y	N
LK1-SDCIS	Leak in piping within the SDC system when in service, within the capacity of two D_2O feed pumps	Y	Y	Y	Y	Y
LLOCA-SDCIS	Large break in piping within the SDC system when in service, beyond the capacity of two D_2O feed pumps	Y	Y	Y	Y	Y
PTF	Pressure tube failure	Y	N	N	N	Y
PTL	Pressure tube leak (initial discharge rate less than 1 L/s)	Y	Y	Y	Y	Y
SGTB1	Steam generator tube break within the capacity of two D_2O feed pumps	Y	N	N	N	Y
SGTB2	Steam generator tube break beyond the capacity of two D_2O feed pumps	Y	N	N	N	Y
SDCHXTB1	SDC HX tube break within the capacity of two D_2O feed pumps	Y	Y	Y	Y	Y
SDCHXTB2	SDC HX tube break beyond the capacity of two D_2O feed pumps	Y	N	N	N	Y
ICEPLUGS	Failure of liquid nitrogen supply to all ice plugs	N	Y	Y	Y	N
Intrinsic System Failures for Primary Heat Sink						
SDC-COOL	Failure of SDC HXs to remove heat	Y	Y	Y	Y	Y
SDC-FLOW	Loss of HTS forced circulation using the SDC pumps	Y	Y	Y	Y	Y
2HTPT	2 or more heat transport pumps trip (2 in one loop)	Y	N	N	N	Y

Outage IE Label	IE Definition	POS Applicability				
		A	B	C	D	E
SDC-INV	Loss of HTS inventory (not in LLDS; no rupture) leads to failure of forced circulation using SDC pumps.	N	Y	N	N	N
SDC-INV-LLDS	Loss of HTS inventory in LLDS (no rupture) leads to failure of forced circulation using SDC pumps	N	N	Y	Y	N
SDC-MV	Spurious closure of SDC isolating MV	Y	Y	Y	Y	Y
Pressure and Inventory Control System Failures						
LOPIC	Failure of HTS pressure and inventory control (no pressure boundary failure) while HTS is pressurized in solid mode	Y	N	N	N	Y
PIC-LOC	Loss of HTS inventory through HTS P&IC pressure boundary while pressurized in solid mode	Y	N	N	N	Y
Large Pipe Breaks or Other Events in Operating Units with Effects on Outage Unit						
LSLB1	Large steam line break at adjacent unit (Unit 1)	Y	Y	Y	Y	Y
LFLB1	Large FW line break at adjacent unit (Unit 1)	Y	Y	Y	Y	Y
LSLB34	Large steam or FW line break at remote unit (Units 3 or 4)	Y	Y	Y	Y	Y
EVAC-CNMT	Internal event, not originating from U2, that leads to an evacuation of the outage unit work areas inside containment	Y	Y	Y	Y	Y
Electrical System Failures						
LOBES	Loss of Bulk Electricity System	Y	Y	Y	Y	Y
LOSWYD	Loss of Switchyard	Y	Y	Y	Y	Y
LOCL4	Loss of Class IV	Y	Y	Y	Y	Y
LOBU1	Loss of power to Unit Class IV 13.8 kV bus BU1	Y	Y	Y	Y	Y
LOBU2	Loss of power to Unit Class IV 13.8 kV bus BU2	Y	Y	Y	Y	Y
LOBU3	Loss of power to Unit Class IV 13.8 kV bus BU3	Y	Y	Y	Y	Y
LOBU4	Loss of power to Unit Class IV 13.8 kV bus BU4	Y	Y	Y	Y	Y
LOBU5	Loss of power to Unit Class IV 13.8 kV bus BU5	Y	Y	Y	Y	Y
LOBU6	Loss of power to Unit Class IV 13.8 kV bus BU6	Y	Y	Y	Y	Y
FS1CB2	Loss of Unit Class IV 13.8 kV buses BU1 and BU3 due to 1CB2 failing short	Y	Y	Y	Y	Y
FS2CB2	Loss of Unit Class IV 13.8 kV buses BU2 and BU4 due to 2CB2 failing short	Y	Y	Y	Y	Y
LOBU7	Loss of power to Unit Class III 4.16 kV bus BU7	Y	Y	Y	Y	Y
LOBU8	Loss of power to Unit Class III 4.16 kV bus BU8	Y	Y	Y	Y	Y
LOBU13	Loss of power to Unit Class III 600 V bus BU13	Y	Y	Y	Y	Y
LOBU14	Loss of power to Unit Class III 600 V bus BU14	Y	Y	Y	Y	Y
LOBU15	Loss of power to Unit Class III 600 V bus BU15	Y	Y	Y	Y	Y
LOBU16	Loss of power to Unit Class III 600 V bus BU16	Y	Y	Y	Y	Y
LOBUA3	Loss of Unit Class II 120 V ac bus BUA3	Y	Y	Y	Y	Y
LOBUB3	Loss of Unit Class II 120 V ac bus BUB3	Y	Y	Y	Y	Y
LOBUC3	Loss of Unit Class II 120 V ac bus BUC3	Y	Y	Y	Y	Y
LO45VA	Loss of Unit Class II 45 V dc at panel 2383-11	Y	Y	Y	Y	Y
LO45VB	Loss of Unit Class II 45 V dc at panel 2859-21	Y	Y	Y	Y	Y
LO45VC	Loss of Unit Class II 45 V dc at panel 3485-C1	Y	Y	Y	Y	Y

Outage IE Label	IE Definition	POS Applicability				
		A	B	C	D	E
LOBUA4	Loss of Unit Class I 48 V dc BUA4	Y	Y	Y	Y	Y
LOBUB4	Loss of Unit Class I 48 V dc BUB4	Y	Y	Y	Y	Y
LOBUC4	Loss of Unit Class I 48 V dc BUC4	Y	Y	Y	Y	Y
LOBUA141	Loss of EPS 48 V dc bus BUA141	Y	Y	Y	Y	Y
LOBUB141	Loss of EPS 48 V dc bus BUB141	Y	Y	Y	Y	Y
Failures of Other Support Systems						
LOLPSW	Total loss of low pressure service water	Y	Y	Y	Y	Y
LOPULSW	Total loss of powerhouse upper level service water	Y	Y	Y	Y	Y
LORCW	Total loss of recirculated water flow	Y	N	N	N	Y
TLOIA	Total loss of instrument air	Y	Y	Y	Y	Y
FOREBAY	Forebay severe condition	Y	Y	Y	Y	Y

Table 9: Summary of Fuel Damage Categories for DARA-L1O

FDC	Definition	Typical Outage Events in FDC
1-SD	**Rapid loss of core structural integrity.**	**Inadvertent criticality during outage and failure to terminate the event.** [Note 1]
2-SD	**Slow loss of core structural integrity.**	**HTS leak with failure of HTS make-up and failure of the moderator heat sink.**
3	Moderator required as heat sink in the short term (< 1 hr after reactor shutdown).	Not applicable to Outage PSA. Unit has been shutdown for greater than 1 hour and therefore the short term moderator heat sink is not required.
4	Moderator required as heat sink in the intermediate term (1 to 24 hr after reactor shutdown).	Not applicable to Outage PSA. Unit has been shutdown for >24 hours and therefore the intermediate term moderator heat sink not required.
5-SD	**Moderator required as heat sink in the long term (> 24 hr after reactor shutdown).**	**HTS leak with failure of HTS make-up but with successful use of the moderator heat sink.**
6	Temporary loss of cooling to fuel in many channels.	Represents stylized conditions of specific at-power accidents. Not applicable to Outage PSA.
7-SD	**Single channel fuel failure with sufficient release of steam or radioactivity to initiate automatic containment button-up.**	**Failure to cool fuel contained within the fuelling machines. Large flow blockage with fuel ejection. LOCA1 stagnation feeder break.** [Notes 2,3,4]
8	Single channel fuel failure with insufficient release of steam or radiation activity to initiate automatic containment button-up.	Single channel events for Outage are adequately covered by FDC7-SD.
9-SD	**HTS leaks with no fuel failure (ECIS successful); potential for significant economic impact.**	**HTS leak with failure of D_2O make-up but with successful use of ECI.**

Note 1: Potential initiating events representing inadvertent criticality during an outage have been screened out of DARA-L1O on the basis that they have an extremely low frequency. Similarly, the likelihood of an inadvertent criticality during the mission is assumed to be negligible when compared to the other causes of severe core damage during an outage. Therefore, no DARA-L1O event tree sequences are assigned to the FDC1-SD end state.

Note 2: Initiating events representing a loss of cooling to the fuelling machines while in transit are screened out from DARA-L1O since the DARA Level-1 At-Power PSA includes the exposure time for fuelling machine failures that occur during unit outages.

Note 3: Large flow blockages with fuel ejection and stagnation feeder breaks are stylized at-power accidents representing conditions that are not applicable during outage, so these initiating events have been screened out of DARA-L1O.

Note 4: Given the specific IEs that were screened out, there were no DARA-L1O ET sequences that were identified as proceeding to the FDC7-SD end state.

Table 10: Seismic Hazard Bins

Bin #	Seismic Interval (g)	Magnitude For Fragility Calculation (g)	Seismic Interval Frequency (1/yr)*
1	0.03 - 0.08	0.05	1.3E-05
2	0.08 - 0.2	0.13	4.1E-05
3	0.2 - 0.3	0.24	1.2E-05
4	0.3 - 0.5	0.39	9.3E-06
5	0.5 - 0.7	0.59	3.4E-06
6	0.7 - 1	0.84	2.0E-06
7	1 - 2	1.41	1.4E-06
8	>2	2	3.0E-07

* Occurrence of seismic event per year with potential to impact the station.

Table 11: Summary of Selected Accident Sequence

PDS	Representative Accident Sequence
PDS1	No representative sequence defined.
PDS2A	LOCA2A, with loss of moderator cooling and failure of ECI.
PDS2B	LOCA2A, with loss of moderator cooling and failure of ECI, combined with EFADS system failed.
PDS2C	LOCA2A, with loss of moderator cooling and failure of ECI, combined with failure of hydrogen igniters.
PDS2D	LOCA2A, with loss of moderator cooling and failure of ECI, combined with failure of reactor vault ACUs.
PDS2E	LOCA2A, with loss of moderator cooling and failure of ECI, combined with failure of reactor vault ACUs and failure of EFADS.
PDS2F	LOCA2A, with loss of moderator cooling and failure of ECI, combined with containment envelope impairment.
PDS2G	LOCA2A, with loss of moderator cooling and failure of ECI, combined with containment envelope impairment and failure of reactor vault ACUs.
PDS3-2U	2-Unit blackout with failure of FW, IUFT, IA, SDC, ESW, ECI.
PDS3-4U	100% steam line break in Unit 2, loss of Class IV and III power and EPS affecting all 4 units.
PDS4	Multiple steam generator tube rupture, failure of ECI and moderator cooling.
PDS5	LOCA2 end fitting failure plus failure of ECI, with the moderator providing a long term heat sink, and failure of containment isolation.
PDS6	Multiple steam generator tube rupture with failure of ECI, with the moderator providing a long term heat sink.

Table 12: Darlington NGS Release Categorization Scheme

Release Category #	Description
D-RC1	Very large release (> ~3% core inventory of I-131) with potential for acute offsite radiation effects and/or widespread contamination
D-RC2	Mixture of fission products containing > 1E14 Bq of Cs-137 but less than D-RC1 occurring mainly within 24 hours
D-RC3	Mixture of fission products containing > 1E14 Bq of Cs-137 but less than D-RC1 occurring mainly after 24 hours
D-RC4	Mixture of fission products containing > 1E15 Bq of I-131 but < 1E14 Bq of Cs-137 occurring mainly within 24 hours
D-RC5	Mixture of fission products containing > 1E15 Bq of I-131 but < 1E14 Bq of Cs-137 occurring mainly after 24 hours
D-RC6	Mixture of fission products containing > 1E14 Bq of I-131 but < 1E15 Bq of I-131 occurring mainly after 24 hours
D-RC7	Normal containment leakage. Leakage across an intact containment envelope or long-term filtered release.
D-RC8	Basemat Melt-through. No release to atmosphere.

Table 13: Summary of DARA Severe Core Damage and Large Release Frequency Results

Model	Severe Core Damage Frequency (x 10^{-5} occurrences per reactor year) [4]		Large Release Frequency (x 10^{-5} occurrences per reactor year) [4]	
	2015 DARA Baseline (with EME)	2015 DARA with EME and SIOs [1]	2015 DARA Baseline (with EME)	2015 DARA with EME and SIOs [1]
Internal Events At-Power	0.23	0.14	0.10	0.04
Internal Events Outage	0.10	0.05	<0.10 [2]	<0.05 [2]
Fire At-Power	0.09	<0.09	0.08	<0.08 [2]
Seismic At-Power	0.37	0.14	0.28	<0.14 [2]
Flooding At-Power	0.02	<0.02	0.02 [2]	<0.02 [2]
High Wind At-Power	0.22	0.08	0.10	0.05
Unit Aggregate Risk Across All Hazards	0.93 [3]	0.47 [3]	0.58 [3]	0.33 [3]
OPG Safety Goal Target	1		0.1	
OPG Safety Goal Limit	10		1	

[1] The SIOs are described in Section 7.0.

[2] For some models, LRF is not assessed in detail as LRF is bounded by SCDF.

[3] The aggregated SCDF and LRF results exclude Internal Events during outage as the internal events at-power model assumes that the unit is at full power operation 100% of the time. The aggregated results are calculated by simple addition. No widely accepted methodology exists for risk aggregation and simple addition may lead to overly-conservative and biased results.

[4] To facilitate comparison between different hazards, the results in this table are all presented as values of 10^{-5} occurrences per reactor year and are rounded as appropriate. Elsewhere in this summary report and in the individual DARA reports, standard scientific notation is used.

Table 14: DARA Level 1 At-Power Internal Events Fuel Damage Results

Fuel Damage Category	**Baseline Predicted Frequency (/yr)**
FDC1	<<1E-09
FDC2	2.3E-06
FDC3	1.6E-05
FDC4	2.6E-04
FDC5	8.6E-06
FDC6	4.0E-06
FDC7	1.0E-03
FDC8	4.3E-03
FDC9	2.5E-02
Severe Core Damage Frequency FDC1 + FDC2	2.3E-06

Table 15: Frequencies of Fuel Damage Categories for DARA-L1O

Fuel Damage Category	Plant Operating State	Frequency (/yr)	
		Time-Average Note 1	Non-Time-Average
FDC2-SD	(all)	9.8E-07	
	POS A	3.4E-09	9.4E-07
	POS B	1.0E-08	9.3E-07
	POS C	3.0E-08	1.3E-06
	POS D	9.4E-07	1.6E-04
	POS E	4.6E-09	1.0E-06
Severe Core Damage Note 2	(all)	9.8E-07	

Note 1: Time-average FDC results are on a reactor-year basis, using the weighted duration and outage frequency from the POS analysis.

Note 2: FDC2-SD represents Severe Core Damage for the DARA-L1O model.

Table 16: Plant Damage State Frequency

PDS	Predicted Frequency (occ/yr)
PDS1	1.0E-11
PDS2	1.5E-06
PDS3-2U	9.7E-07
PDS3-4U	4.2E-07
PDS4	4.0E-07
PDS5*	1.2E-03
PDS6*	1.5E-04

*PDS5 and PDS6 sequences are limited core damage sequences.

Table 17: Release Category Frequency

Release Category	Baseline Predicted Frequency (occ/yr)
D-RC1	5.0E-07
D-RC2	5.2E-07
D-RC3*	0
D-RC4*	0
D-RC5	4.8E-8
D-RC6	3.2E-7
D-RC7	1.9E-06
D-RC8	4.2E-7

* No sequences above the truncation limit were identified in which a release was predicted in the range of magnitude and timing corresponding to the definitions of RC3 and RC4.

Appendix A: Acronyms

Acronym	Definition
ACU	Air Conditioning Unit
AIM	Abnormal Incident Manual
ASDV	Atmospheric Steam Discharge Valve
BCA	Benefit-Cost Assessment
BES	Bulk Electrical System
BWR	Boiling Water Reactor
CANDU	CANadian Deuterium Uranium
CCDP	Conditional Core Damage Probability
CDFM	Conservative Deterministic Failure Margin
CEI	Containment Envelope Integrity
CET	Containment Event Tree
CFVS	Containment Filtered Venting System
CNSC	Canadian Nuclear Safety Commission
COG	CANDU Owners Group
CSA	Central Service Area
CSDV	Condenser Steam Discharge Valve
D_2O	Deuterium Oxide (Heavy Water)
DARA	Darlington NGS Probabilistic Safety Assessment
DARA-FIRE	Internal Fire Darlington Probabilistic Safety Assessment
DARA-FLOOD	Internal Flooding Darlington Probabilistic Safety Assessment
DARA-L1O	Level 1 Outage Internal Events Darlington Probabilistic Safety Assessment
DARA-L1P	Level 1 At-Power Internal Events Darlington Probabilistic Safety Assessment
DARA-L2P	Level 2 At-Power Internal Events Darlington Probabilistic Safety Assessment
DARA-SEISMIC	Seismic Darlington Probabilistic Safety Assessment
DARA-WIND	Darlington High Wind Probabilistic Safety Assessment
DBE	Design Basis Earthquake
DCC	Digital Control Computer
DGSS	Drained Guaranteed Shutdown State
DNGS	Darlington Nuclear Generating Station
ECI	Emergency Coolant Injection

Acronym	Definition
ECIS	Emergency Coolant Injection System
ECR	Emergency Coolant Recovery
EFADS	Emergency Filtered Air Discharge System
EME	Emergency Mitigating Equipment
EPG	Emergency Power Generator
EPRI	Electric Power Research Institute
EPS	Emergency Power System
ESW	Emergency Service Water
ET	Event Tree
FADS	Filtered Air Discharge System
FAI	Fauske and Associates
FDC	Fuel Damage Category
FHA	Fire Hazard Assessment
FIF	Fire Ignition Frequency
FIS	Fixed Ignition Source
FP	Full Power
FSSA	Fire Safe Shutdown Analysis
FT	Fault Tree
FTREX	Fault Tree Reliability Evaluation eXpert
FW	Feedwater
GFS	Gravity Filled State
GSS	Guaranteed Shutdown State
HEP	Human Error Probability
HRA	Human Reliability Analysis
HT	Heat Transport
HTS	Heat Transport System
HX	Heat Exchanger
IAEA	International Atomic Energy Association
ICRP	International Commission on Radiological Protection
IE	Initiating Event
IGN	Hydrogen Igniters
ISRV	Instrumented Steam Relief Valve
IST	Industry Standard Toolset
IUFT	Interunit Feedwater Tie

Acronym	Definition
LHS	Loss of Heat Sink
LLDS	Low Level Drained State
LOCA	Loss-of-Coolant Accident
LPSW	Low Pressure Service Water
LRF	Large Release Frequency
MAAP	Modular Accident Analysis Program
MCR	Main Control Room
MW	Megawatt
NC	Natural Circulation
NGS	Nuclear Generating Station
NPC	Negative Pressure Containment
NRC	Nuclear Regulatory Commission (U.S.)
NUREG	Nuclear Regulation
OPG	Ontario Power Generation
OPGSS	Over Poisoned Guaranteed Shutdown State
OSR	Operational Safety Requirements
PAU	Physical Analysis Unit
PAWCS	Post-Accident Water Cooling System
PDS	Plant Damage State
PHT	Primary Heat Transport
PK	Programmable Controller
PMF	Probable Maximum Flood
POS	Plant Operational State
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor
PSVS	Powerhouse Steam Venting System
PULSW	Powerhouse Upper Level Service Water
PUPS	Portable Uninterruptable Power Supply
PWR	Pressurized Water Reactor
RC	Release Category
RCW	Recirculating Cooling Water
RLC	Review Level Condition
RRS	Reactor Regulating System
SCD	Severe Core Damage

Acronym	Definition
SCDF	Severe Core Damage Frequency
SDC	Shutdown Cooling
SDS	Shutdown System
SDV	Screening Distance Value
SEL	Seismic Equipment List
SFL	Screening Frequency Level
SGECS	Steam Generator Emergency Cooling System
SIO	Safety Improvement Opportunity
SMA	Seismic Margin Assessment
SNL	Sandia National Laboratories
SPSA	Seismic Probabilistic Safety Assessment
SRV	Steam Relief Valve
SSC	Systems Structures and Components
STOP	Shield Tank Over Pressure
THERP	Technique for Human Error Rate Prediction
USA	United States of America
USCA	Unit Secondary Control Area