ONTARIOPOWER GENERATION

Report

Document Number: NK38-REP-03611-10072	Usage Classification: N/A
Sheet Number: N/A	Revision: R000

Title:
DARLINGTON NGS RISK ASSESSMENT SUMMARY REPORT

Darlington NGS Risk Assessment Summary Report

NK38-REP-03611-10072-R000
2012-05-29

Order Number: P1423
Other Reference Number:
P1423/RP/008 R02

Original Signed

Table of Contents

Page

List of Tables and Figures

Page

Revision Summary

Revision Number	Date	Comments
R000	May 2012	Initial issue.

Executive Summary

The objective of Probabilistic Risk Assessment (PRA) 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 PRAs are required to meet the intent of the corporate Nuclear Safety Policy [R1] and the Canadian Nuclear Safety Commission (CNSC) Standard S-294 [R2].

A nuclear PRA identifies the various sequences that lead to radioactivity releases, and calculates their frequencies of occurrence and consequences. Additionally, the PRA 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 PRA is a comprehensive model of the plant incorporating knowledge about plant design, operation, maintenance, testing and response to abnormal events. To the extent possible, the PRA is intended to be a realistic model of the plant.

The baseline Darlington NGS risk assessments are documented in seven separate reports, and assess risk for the following scenarios:

- The risk of core damage, releases and human health risk 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 risk of 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 covering accidents during outage, including loss of outage heat sinks. The outage assessment also includes a bounding estimate of the large release frequency from internal events while the unit is in the guaranteed shutdown state;
- The risk of severe core damage from seismic events occurring while the reactor is at full power, and an estimate of the risk of large release as a result of seismic events;
- The risk of severe core damage and large release from internal fires occurring while the reactor is at full power; and
- The risk of severe core damage from internal floods occurring while the reactor is at full power.

The risk to the health of the public living or working in the vicinity of Darlington NGS is very low in comparison to other potential risks to which the population is normally exposed. Although the models prepared to meet the requirements of S-294 show that the overall risk is low, the additional modelling to represent some of the design changes planned as part of the Darlington refurbishment show that there are opportunities to further reduce risk as a part of refurbishment.

1.0 INTRODUCTION

The objective of Probabilistic Risk Assessment (PRA) 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 PRAs are required to meet the intent of the corporate Nuclear Safety Policy [R1] and the Canadian Nuclear Safety Commission (CNSC) Standard S-294 [R2].

A nuclear PRA identifies the various sequences that lead to radioactivity releases, and calculates their frequencies of occurrence and consequences. Additionally, the PRA 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 PRA is a comprehensive model of the plant incorporating knowledge about plant design, operation, maintenance, testing and response to abnormal events. To the extent possible, the PRA is intended to be a realistic model of the plant.

The PRA for the Darlington Nuclear Generating Station (NGS) is called the Darlington NGS Risk Assessment (DARA) and has been completed in seven separate studies:

1. A Level-1 internal events at-power probabilistic risk assessment, which studies the risk of fuel damage from events occurring within the station (i.e., loss of coolant accidents, steam line breaks) while the reactor is at full power. This report is referred to as DARA-L1P.

2. A Level-1 internal events outage PRA (DARA-L1O), which studies the risk of fuel damage from internal events occurring at the station while the reactor is in a guaranteed shutdown state (GSS). An outage unit produces decay heat; the outage PRA studies fuel damage due to failure to remove decay heat produced while the unit is in GSS.

3. A seismic PRA (DARA-SEISMIC), which studies the risk of fuel damage and large release from seismic events (i.e., earthquakes).

4. An internal fire PRA (DARA-FIRE), which studies the risk of fuel damage from fires originating in the station (e.g., fires caused by station electrical equipment).

5. An internal flooding PRA (DARA-FLOOD), which studies the risk of fuel damage from floods originating inside the station (i.e., pipe breaks of plant systems).

6. A Level-2 internal events at-power PRA (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 (i.e., loss of coolant accidents, steam line breaks) while the reactor is at full power. This PRA is the extension of the Level-1 PRA described in Item 1.

7. A Level-3 internal events at-power PRA (DARA-L3P), which studies the impact of releases to the environment on the population surrounding Darlington NGS and the overall risk to public health. This PRA is the extension of the Level-2 PRA described in Item 6.

The above seven studies represent the baseline DARA and provide an estimate of the station risk in its current configuration. All but the Level 3 PRA are required for compliance with S-294. The PRA is consistent with the current station design and operation and the OPG PRA methodology. The OPG PRA Methodology has been accepted by the CNSC.

Ontario Power Generation has safety goals for severe core damage, large release frequency and latent effects, Reference [R3], as shown in Table 1. The intent of these goals is to ensure the radiological risks arising from nuclear accidents associated with the operation of Ontario Power Generation's nuclear power reactors is low in comparison to risks to which the public is normally exposed. The baseline DARA studies show that the overall risk from the operation of Darlington NGS is low.

Although the PRA is intended to be a realistic model of the plant, if realistic analysis is not available to support the PRA modelling and assumptions, conservative analysis may be used instead. Once the model is evaluated, if these assumptions result in significantly conservative results, new supporting analysis is typically performed and the PRA model is then revised. Removing significant conservatism from the model is important so that a realistic PRA model is available for PRA applications including operational risk monitoring and benefit-cost assessment studies.

Due to limitations on the available supporting analysis in the Level 1 At-Power PRA, the baseline results include some conservative assumptions. A project was initiated to perform new analysis to support less conservative assumptions, and to consider the benefits of potential design changes (known as Safety Improvement Opportunities or SIOs). This work was performed to support Benefit-Cost Analysis (BCA) used as part of the assessment process for plant changes to be implemented during the Darlington Nuclear Refurbishment and the Environmental Assessment (EA) [R4]. The model with the refined assumptions is called the Enhanced DARA model with SIOs.

The current report summarizes the risk assessments of the Darlington NGS described above and compares the risks associated with the operation of this facility with Ontario Power Generation's Safety Goals, documented in Reference [R3]. Results are presented for both the baseline and enhanced model. This report is intended to provide an introduction to the methods used by Ontario Power Generation for analysing public health risk due to the operation of the Darlington NGS, as well as supplement the information in the Environmental Assessment for the refurbishment of Darlington [R4].

1.1 Objectives

The principal objectives of the Darlington NGS Risk Assessment Studies are:

1. To provide an integrated review of the adequacy of the safety of the current station design and operation;

2. To provide a basis for improvements to the operational surveillance program; and

3. To prepare a risk model in a form that it can be used, in conjunction with ancillary application tools, to assist the safety-related decision making process.

1.2 Scope

The baseline DARA risk assessments are documented in seven separate reports, and assess risk for the following scenarios:

- The risk of core damage, releases and human health risk 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 risk of 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 covering accidents during outage, including loss of outage heat sinks. The outage assessment also includes a bounding estimate of the large release frequency from internal events while the unit is in GSS;

- The risk of severe core damage from seismic events occurring while the reactor is at full power, and an estimate of the risk of large release as a result of seismic events;

- The risk of severe core damage and large release from internal fires occurring while the reactor is at full power; and,

- The risk of severe core damage from internal floods occurring while the reactor is at full power.

The impact of the enhancements on the DARA model was assessed for Level 1, 2 and 3 Internal Events At-Power models (i.e., the first bullet from the list above).

The DARA reports 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, high winds, 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.

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:

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

(b) An overview of risk assessment methods and the three levels of risk assessment (Section 3.0) and the methods used for Level 1 Analysis (Section 4.0), Level 2 Analysis (Section 5.0), and Level 3 Analysis (Section 6.0);

(c) A discussion of the modifications made to the Level 1, 2 and 3 At-Power models for the enhanced DARA model (Section 7.0); and

(d) A discussion of the main results of the DARA studies, including the baseline and enhanced model (Section 8.0).

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

2.0 PLANT DESCRIPTION

The following sections 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, the 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 designed and evaluated for a 30-year lifetime.

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;
(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 system (HT) 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 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

(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. 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.

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

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 the backup supply to Class IV 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 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 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 PRA 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 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.

2.4 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 system is seismically qualified to withstand a design basis earthquake (DBE). The DBE used for the design of Darlington NGS is described in Chapter 6 of the EA [R4]. The Group 2 controls functions are performed from secondary control areas.

3.0 OVERVIEW OF PRA METHODS

Risk assessment is based on the idea that the product of the frequency of occurrence of an event and the consequence of the event represents a useful and meaningful quantity. This product is defined to be the risk from the event and is expressed in units of consequence per unit of time. 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 risk assessment process is that the larger the numerical value of risk for a particular event or combination of events, the more important the event is to safety. Thus, measures to reduce calculated risk improve the level of safety. Probabilistic Risk Assessment, or PRA, 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 and the resultant public dose. Ontario Power Generation uses a three level PRA method to assess the risk from a nuclear generating plant: Level 1 of the PRA assesses the frequency of varying degrees of fuel failures, which lead to release of radioactivity into containment; Level 2 of the PRA assesses the frequency and magnitude of the release of this radioactivity from containment to the outside environment; Level 3 of the PRA assesses the offsite consequences and public health risk as a result of the radioactivity release to the outside environment, together with economic consequences and risks associated with plant damage, offsite countermeasures and health effects. OPG's three safety goals in Table 1 for risk assessment correspond to the three levels of PRA.

Level 1 risk assessments have been prepared for full reactor power operation for the following types of initiating events:

- 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); and,
- Internal flooding (floods originate from water sources internal to the plant).

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

- An outage seismic risk assessment was not performed as the risk from a seismic event is similar if the unit is at-power or in outage; 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.
- An outage internal fire risk assessment 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 risk assessment 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 and Level 3 risk assessments have been prepared for at-power internal events. Limited scope Level 2 assessments have been prepared for seismic events, outage internal events and fire events 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 events reviews the potential for unique containment challenges or bypass pathways in the outage state, and provides a bounding assessment of large release frequency 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.

Level 3 assessment is primarily used in assessing the costs and benefits of design changes to reduce the frequency of accidents and is not required for S-294 compliance. However, Level 3 analysis has been performed for the internal events at-power PRA.

Figure 5 presents an overview of the DARA models and the relationships between the various PRA studies.

In the following sections, the methods used for each of the Levels of PRA are described.

4.0 LEVEL 1 PRA METHODS

The goal of a Level 1 PRA 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, 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 PRA study for a station will be a Level 1 At-Power internal events PRA. 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 PRAs for other types of initiating events, e.g., internal fire, internal flood and seismic, much of the effort is associated with determining the impact these events have on the mitigating systems. The descriptions of the methodology for the various Level 1 studies in the following subsections reflect different requirements for the different studies.

The Level 1 At-Power PRA model was used to aid in the development and quantification of the outage, seismic, fire, and internal flooding PRA.

4.1 Level 1 At-Power Internal Events

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

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

(a) Identification of initiating events based on a review of station operating experience and knowledge gained from previous risk assessment studies. The identification of initiating events is discussed in Section 4.1.1.

(b) Development of a scheme to group sequences into a manageable number of consequence categories based on degree of fuel damage (Section 4.1.2).

(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 4.1.3.

(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 4.1.4.

(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 4.1.4.

(f) Assessment of the affect 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 the DARA. The HRA is discussed in Section 4.1.5.

(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 4.1.6.

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.

4.1.1 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 PRA process.

In the 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 the DARA-L1P is an internal events PRA, 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 risk assessments were reviewed, as were the plant operating experience and station condition records, and other published PRAs. In addition, insight from the fault tree modelling, discussed in Section 4.1.4, identified other initiating events.

The complete list of initiating events considered in DARA-L1P is provided in Table 2.

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.

4.1.2 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 4.1.3. In addition, groupings of the fuel damage categories are used to transition from the Level 1 PRA to the Level 2 PRA (see Section 5.1).

The range of events or event sequences covered by the FDCs is defined by the scope of the DARA. From the event tree analysis described in Section 4.1.3, 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 3 presents the FDCs used in the 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.

4.1.3 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.

4.1.4 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 4.1.3, and for the support systems. Table 4 lists the systems modelled by fault trees in the DARA-L1P. 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 [R5].

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 the 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) [R6], T-book [R7], and Westinghouse Savannah River Company [R8], were used for obtaining generic data. The DARA component reliability database is based on a Bayesian calculation of the equipment failure rates reflecting 1999 to 2008 Darlington operational data.

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.

4.1.5 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 the 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 [R9].

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 [R9].

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 [R9].

4.1.6 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 [R5]. The CAFTA program was developed by Electric Power and Research Institute (EPRI). The FTREX program is used to quantify the results [R10].

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 PRA 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 1E-07 occ/yr range, and a truncation of 1E-11 occ/yr is used.

Following the development of the baseline PRA 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 4.1.1 to 4.1.6 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 5.0. The remaining subsections in Section 4.0 describe the differences in methodology for Level 1 assessment for the outage state, and for fire, internal flood, and seismic initiators.

4.2 Outage Internal Events

The 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 DARA-L1O has been developed following the methodology for preparation of a Level-1 Outage PRA as described in the OPG Outage PRA Guide. The Outage PRA uses many of the same techniques as used in the At-Power PRA. The risk assessment process for outage uses initiating events, event tree analysis and fault tree analysis, like the At-Power PRA. 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 PRA are typically described as plant operational states (POS).

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

4.2.1 Plant Operational State (POS) Identification and Analysis

The purpose of Plant Operational State (POS) 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 PRA. 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 the 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 PRA, including accident sequence analysis using event trees. Table 5 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.

4.2.2 Initiating Event Identification and Quantification

The development of a Level-1 Outage PRA 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 PRA 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 6 presents the list of outage initiating events for the DNGS Level 1 Outage PRA, 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).

4.2.3 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 4.1.3.

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 the DARA-L1O, these are the outage fuel damage categories as shown in Table 7.

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.

4.2.4 Outage System Fault Tree Analysis

The fault tree analysis process for the internal outage PRA is the same as for the at-power PRA. 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 PRA. 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 4 lists the systems modelled by fault trees in DARA-L1O.

4.2.5 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 PRA, 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.

4.2.6 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 PRA is generally the same as in the At-Power model (see Section 4.1.5), the effort required to identify, quantify and model human interactions in Outage PRA 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.

4.2.7 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 [R3].

Following the development of the baseline PRA 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.

4.3 At-Power Internal Fire

The DARA-FIRE assessment has been developed following the methodology for preparation of an Internal Fire PRA as described in the OPG Fire PRA Guide. The OPG Fire PRA Guide has been developed based on NUREG/CR-6850 [R11]. The major activities of the Fire PRA methodology and its application in the development of the DARA-FIRE assessment are summarized in the subsections below.

An internal fire PRA is built from the internal events PRA 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 PRA, 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 Safety Assessment (FSA).

4.3.1 Phased Approach to Fire PRA

The Fire PRA 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 PRA 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 PRA assessment was performed.

The objectives of the Fire PRA 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 PRA logic is based on the internal events PRA logic for the forced shutdown event tree. As the fire PRA is developed based on the internal events PRA, the major tasks in the fire PRA 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 PRA methodology is broken down into 18 tasks:

Task 1 – Plant Boundary Definition and Partitioning
Task 2 – Fire PRA Component Selection
Task 3 – Fire PRA 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 PRA, addressed through alternate methodology)
Task 14 – Fire PRA Level 1 Quantification
Task 15 – Uncertainty and Sensitivity Analysis
Task 16 – Fire PRA Documentation
Task 17 – Fire PRA 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 PRA 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.

4.3.2 Plant Partitioning

This first task in the fire PRA 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 risk assessment 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 PRA to rely on the existing programmatic controls and design requirements for maintaining the integrity of the associated compartment boundaries.

4.3.3 Fire PRA Component and Cable Selection

The development of a fire PRA 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 PRA, 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 Safety Assessment (FSA) with the addition of components associated with the additional heat sink credits relying on IUFT and ESW to the moderator.

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 PRA components potentially affected by postulated fires at different plant locations.

4.3.4 Qualitative Screening

The physical analysis units, described in Section 4.3.2 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.

4.3.5 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 PRA to reflect postulated equipment failures. The scope of the equipment credited in the fire risk model is limited to those components identified in Section 4.3.3.

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

4.3.6 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 [R11] and [R12] 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 PRA 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 [R11]. The qualitative review of CANDU operating experience with fire events found Canadian experience sufficiently similar to U. S. experience documented in NUREG/CR-6850 [R11] 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.

4.3.7 Quantitative Screening

The development of a fire PRA 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 4.3.5 and 4.3.6), 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 [R11].

Areas of the plant that are screened during this step still are retained in the fire PRA 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.

4.3.8 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.

4.3.9 Detailed Circuit Failure and Failure Mode Likelihood Analysis

The development of a fire PRA 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 PRA. 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 risk assessment, see Section 4.3.3. 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.

4.3.10 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 4.3.8 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 [R13].

4.3.11 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 PRA 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 PRA 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 credit was taken for potential post-fire shutdown actions that were not already modeled in the internal events at power PRA.

4.3.12 Fire Level 1 PRA Quantification

The development of a fire PRA 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 PRA model, described in Section 4.3.5, to quantify SCD frequency for each of the fire PRA scenarios.

The scoping fire modeling (Section 4.3.8) provided a conservative and simplified means to develop an initial refinement to the bounding treatment in the quantitative screening (Section 4.3.7). The scope of work for detailed fire PRA quantification involves the use of the fire PRA model with the modified post-fire HEPs (Section 4.3.11) 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 4.3.8) 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 4.3.7). 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.

4.3.13 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.

4.4 At-Power Internal Flood

The OPG Internal Flooding PRA Guide describes the methodology used to quantify the risk due to internal flooding. Similar to the Fire PRA, 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 PRA was not required.

Like the fire PRA described in Section 4.3, 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 PRA is the At-Power Internal Events PRA (DARA-L1P). The At-Power Internal Events PRA 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 PRA 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 PRA Quantification.
9. Sensitivity and Uncertainty Analysis.
10. Support Task – Plant Walkdowns.

Figure 11 shows the tasks for the flooding PRA.

The flooding PRA 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 13) 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.

4.4.1 Identification of Flood Areas, SSC and Flood Sources

Like the fire PRA, the first step of the flooding PRA 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 PRA 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 PRA, and the possible flood sources in the area.

4.4.2 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 4.3.4);
- 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.

4.4.3 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 PRA.

4.4.4 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 [R14].

4.4.5 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 PRA. 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).

4.4.6 Internal Flooding Accident Sequence and Level 1 PRA Quantification

This step includes the finalization of flood scenario development and completing internal flood accident sequence models based on modifying the internal events PRA 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 4.4.5. 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 PRA, 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 sensitive and uncertainly analysis were included as part of the quantification of the DARA-FLOOD model.

4.5 At-Power Seismic

The DARA-SEISMIC assessment has been developed following the methodology for preparation of a seismic PRA as described in the OPG Seismic PRA Guide. The major activities of the Seismic PRA 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 PRA 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 PRA was created based on the internal events At-Power PRA, DARA-L1P.

The DARA-SEISMIC model considers sequences that result in severe core damage (FDC1 and FDC2). Like the fire PRA, 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 PRA Guide also outlines a Phased approach with two phases defined:

- **Phase 1 - PRA-Based Seismic Margin Assessment (SMA)** - In Phase 1, a Probabilistic Risk Assessment-based Seismic Margin Assessment (PRA based SMA) is performed based on the methodology described in Reference [R15]. 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 PRA (SPRA)** – 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 SPRA. 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 PRA study was performed.

Major elements of the DNGS SPRA 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 PRA Quantification
- Alternate Unit Analysis (excluded from DARA-SEISMIC assessment)

- Seismic PRA Documentation

The integration of these tasks is shown in Figure 12.

4.5.1 Seismic Hazard Characterization

The first step in the seismic PRA 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 PRA analysis.

4.5.2 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 PRA. This task relies upon the internal events PRA 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). 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 and PAWCS).

4.5.3 Seismic Response Characterization

The next step in the seismic PRA 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 PRA 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.

4.5.4 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 SPRA. The plant walkdowns included reviews of the SEL items in one unit and the items in the systems common to all four units.

4.5.5 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 [R16]. In some cases more refined fragilities were derived using the Separation-of-Variable method [R17] and [R18], for risk contributing equipment. This method includes estimates of median seismic capacity and uncertainty.

4.5.6 Seismic Level 1 PRA Quantification

To build the seismic PRA 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 PRA.

This task involves the integration of the seismic fragility information described in Sections 4.5.3 to 4.5.5 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 8 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.

5.0 LEVEL 2 PRA METHODS

Section 4.0 described the methods used for the Level 1 PRA assessments of Darlington NGS. In the Level 1 PRA, 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 PRA 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 PRA as described in the Level 2 PRA Guide. The major activities of the Level-2 PRA methodology and its application in the development of the DARA-L2P are summarized in the subsections below.

5.1 Interface with Level 1 PRA

The Darlington At-Power Risk Assessment Level 1 PRA (DARA-L1P) generates results in the form of frequencies of nine Fuel Damage Categories, described in Section 4.1.2, 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 15) 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 PRA Study. In order to develop the logic for PDS3, conservative assumptions were made to partition the FDC2 logic in to 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 PRA 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 9.

5.2 Containment Event Tree Analysis

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

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

5.3 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 15, 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

The fault tree models used in the quantification of the Level 2 PRA are listed in Table 4. 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.

5.4 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 such as Level 3 PRA 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),

- 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 10 presents the release categories used in the DARA-L2P analysis. Large release frequency (LRF) is defined to be the sum of RC1 through RC3.

5.5 MAAP-CANDU Analysis

MAAP-CANDU (Modular Accident Analysis Program – CANDU) is a severe accident simulation code for CANDU nuclear stations [R19]. 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 risk 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 PRA. 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.

5.6 Integration of the Level 1 and 2 PRA

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.

5.7 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 GSS.

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.

5.8 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).
- Screening of remaining scenarios based on potential multi-unit impact, or potential to impact Level 2 functions.
- The unscreened sequences were then assessed to determine the number of units impacted by a scenario. Based on this assessment, the SCD frequency was adjusted to take credit for containment availability, or contributed directly to the estimate of large release frequency.

5.9 Level 2 Seismic Assessment

The Level 2 seismic PRA was limited to two main tasks:

- To estimate the seismic fragility of containment components;

- To estimate the potential contribution of non-consequential containment failures (i.e., seismic fragility of containment) to LRF.

Additional walkdowns and fragility calculations, using the same techniques as those described in Section 4.5.5, were used to assess the possible failure of containment due to seismic events.

6.0 LEVEL 3 PRA METHODS

Level 3 PRA addresses estimation of offsite consequences and risks arising from such releases. The offsite consequences of a release are a function of the magnitude and timing of the release, together with societal response to the release in the form of immediate and long-term offsite emergency response measures. The consequences are expressed in terms of the radiation dose received by members of the public and the economic costs of mitigation measures taken to minimize the exposure. Ontario Power Generation's safety goals for public health risk are documented in Reference [R3]. Economic risk is used for Benefit Cost Studies.

6.1 Public Health Risk

The assessment of public health risk considers the increased risk of serious irreversible injury to an individual living near the Darlington site. Exposure of the public to radiation can increase the risk of immediate ("early") health effects and delayed ("latent") effects due to increased rates of cancer induction at all dose levels. Early health effects are deterministic in nature in the sense that only specific individuals exposed to high doses at high dose rates above certain dose thresholds are at risk, whereas the delayed effects are assumed stochastic, linearly related to exposure and can occur remote in distance and time from the point of release.

The range of possible accident sequences which can result in releases from the station to atmosphere of potential significance to public risk is represented in the Level 2 PRA by a set of Release Categories, defined in Section 5.4. The Darlington Release Categories are labelled RC1 to RC7, representing accidents involving severe core damage, plus two Plant Damage States addressing the consequences of limited core damage accidents. Impacts of the releases were estimated in terms of individual dose and risk, and societal dose and risk. The release characteristics (or source term) for each category are determined by the Level 2 analysis and are the input to the Level 3 analysis. The offsite radiological consequences are evaluated using atmospheric dispersion and environmental pathway models to estimate doses to most exposed individuals at various distances from the point of release and to the population within 100 km of a station, with various countermeasures expected to be implemented according to the Ontario Provincial Nuclear Emergency Plan [R20].

In order to calculate the consequences of such releases, information is required describing the general geographic characteristics of the region around the point of release, distribution of population, and the costs associated with measures taken to mitigate the public exposure to radiation.

6.2 Consequence Analysis Method

Offsite health and offsite economic consequences were calculated using the MACCS2 v1.13.1.0 computer code [R21]. Sandia National Laboratories (SNLs) developed MACCS2 for the US Nuclear Regulatory Commission (NRC) to evaluate the potential impacts of severe accidents at nuclear power plants on the surrounding public.

The radioactive materials released are modelled as being dispersed in the atmosphere while being transported by the prevailing wind. During transport, depending on weather conditions and the presence of precipitation, particulate material can be deposited on the ground. In estimating human exposure to radioactive plume, dispersion, deposition and a number of environmental and exposure pathways are considered. The MACCS2 code calculates the radiological dose that is not avoided by mitigation measures.

In MACCS2, the time period after the accident is divided into three phases: Emergency, Intermediate and Long-term. The emergency phase begins immediately after the arrival of the first plume and can last up to seven days. In this period, the exposure of the population to both the radioactive plume and contaminated ground is modelled. Effective whole body dose is calculated for:

- Acute doses for calculating early fatalities and injuries, and
- Lifetime committed dose used for calculating delayed fatalities (i.e., cancers) resulting from the early exposure.

The calculation of radiation doses in the emergency phase considers five pathways: direct external exposure to radioactive material in the plume (cloudshine), exposure from inhalation of radionuclides in the cloud (cloud inhalation), exposure to radioactive material deposited on the ground (groundshine), inhalation of resuspended material (resuspension inhalation), and skin dose from material deposited on the skin. The release is represented as a series of discrete plumes. Various mitigation measures can be specified for this phase, including evacuation, sheltering and dose-dependent relocation. In the emergency phase, two countermeasures are considered: sheltering and evacuation.

Following the emergency phase, four long-term exposure pathways are addressed; groundshine and resuspension inhalation in the intermediate and long-term phases, and ingestion of contaminated food and drinking water only in the long-term phase.

The intermediate phase is used to represent a period in which post-accident hazard evaluation is performed and planning decisions are made regarding the type of long-term mitigation measures that need to be taken. In this period, the radioactive plume is not present and the only exposure pathways are those from the contaminated ground. For DARA, the duration of the intermediate phase was set to zero and treated as part of the long term phase. The justification for this was that the early phase lasts a relatively long time (7 days) during which there is time for post-accident hazard evaluation and planning decisions. Thus in order to simplify the model, it was not necessary to credit the intermediate phase and report any intermediate results.

The long-term phase represents the time period subsequent to the intermediate phase and can last many years. Mitigation measures can be credited to reduce doses to acceptable levels. These include decontamination, interdiction or condemnation of property, disposal of milk and crops. MACCS2 performs detailed analysis using user-supplied intervention criteria to determine the need for and scope of long-term actions, using some simplified cost-benefit analysis to optimize the process.

The analysis takes into account early (evacuation and/or sheltering) and late countermeasures as required. The timing and nature of offsite emergency response depend on the nature and rate of progression of the accident. In general, evacuation would be initiated if a General Emergency were declared by the station or the Province. A General Emergency is defined as an ongoing atmospheric emission of radioactive material, or one likely within a short time frame (typically 12 hours), as a result of a more severe accident. Response plans and organizations are fully activated and, if necessary, appropriate protective measures are taken.

If time is available, the need for offsite action would be determined by projections of the potential for dose exposure and comparison against the Ontario Protective Action Levels (PALs). The PALs are expressed in terms of the highest projected dose likely to be received by the most exposed individual in the relevant critical group and consider sheltering, evaluation and thyroid blocking. In most cases where radiation exposure is already occurring, it would neither be possible nor desirable to base protective action decisions on calculations involving PALs; instead, they would be based on pre-planned responses and conservative estimates [R20].

6.3 Health Effects

Two types of doses are calculated by the code. They are referred to as "acute" and "lifetime doses". Acute doses are calculated for the purpose of estimating the "deterministic" health effects that can result from high doses delivered at high dose rates. Such conditions may occur in the immediate vicinity of a nuclear power plant following hypothetical severe accidents where containment failure has been postulated to occur.

Lifetime doses are the conventional measure of detriment used for radiological protection. These are the 50-year dose commitments to either specific tissues (e.g., red marrow and lungs), or a weighted sum of tissue doses defined by the International Commission on Radiological Protection (ICRP) [R22], and referred to as "committed effective dose" or just “effective dose”. Lifetime doses are used to calculate the stochastic health effect risk resulting from exposure to radiation.

7.0 ENHANCED DARA MODELLING

While the results of baseline DARA studies show that the overall risks from the operation of Darlington NGS are low, review of the final results identified several areas of the model as conservative. OPG’s PRA process requires the PRA to be updated every 3 years, and conservative assumptions would typically be assessed and modified, if required, during this update. However, two PRA applications necessitated an early update to remove major sources of conservatism:

- The Environmental Assessment of the Darlington Refurbishment;
- Cost benefit studies for Safety Improvement Opportunities (design or operational changes) considered as part of the Darlington Refurbishment.

To support the required model changes, new thermalhydraulic and MAAP-CANDU studies were completed.

In addition to crediting new analysis, the Enhanced DARA model assessed the benefit of four safety improvement opportunities for which OPG has initiated the conceptual design [R4]. It is expected that these SIOs will be implemented as part of the refurbishment of Darlington NGS and address opportunities to further improve safety as a result of Refurbishment Project Studies, as well as address post-Fukushima follow-up commitments and activities. Four SIOs are considered in the Enhanced DARA 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 heat transport system.
- Containment Filtered Venting System (CFVS) and shield tank over pressure relief. CFVS is a new system to prevent failure of containment due to over pressure following severe accidents at multiple units.

The modelling changes and SIOs changes were used to create two new models:

- The Enhanced DARA model, which reflects the current plant configuration and takes credits for the new thermalhydraulic and MAAP-CANDU studies.
- The Enhanced DARA model with SIOs, which reflects post-refurbishment configuration and takes credits for both the new analysis as well as four design changes.

The following sections outline the changes made to the Level 1, 2 and 3 At-Power Internal Events models for the enhanced DARA assessment.

7.1 Enhanced Level 1 At-Power Modelling

In the DARA-L1P study, the analysis to support environmental impacts on equipment and steam protected rooms in the powerhouse was based on some conservative assumptions used in traditional thermalhydraulic safety analysis. To reduce conservatism in the PRA model due to these assumptions, new focused thermalhydraulic analysis was performed to determine the environmental conditions in the powerhouse to support more realistic modelling for these scenarios.

In addition to the above enhancement, additional assessment was done for the following three SIOs anticipated for the refurbished Darlington NGS:

- 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 heat transport system.

The fourth SIO only impacts the Level 2 analysis and is discussed in the next section.

7.2 Enhanced Level 2 At-Power Modelling

The baseline DARA-L1P model assesses severe core damage at a single unit. The Level 2 model considers the consequences of severe core damage at multiple units in plant damage state PDS3. As described in Section 5.1, in the baseline DARA-L2P model, any sequences that might result in severe core damage at two or more units is conservatively assigned the consequence of a four unit scenario. In the enhanced DARA model, PDS3 is split into two new plant damage states:

- PDS3A: sequences with severe core damage at two units. New MAAP-CANDU analysis was performed to assess the consequences of two unit sequences.
- PDS3B: sequences with severe core damage at three or four units. The existing PDS3 MAAP-CANDU analysis for the consequences of a four unit scenario was used for these sequences.

More detailed modelling is used to assess the number of units impacted using information from the Level 1 model on availability of support systems (electrical and service water) at Units 1,3 and 4, and the severe core damage model developed for Unit 2.

In addition to the above modelling enhancement, additional assessment was done for the following containment SIO anticipated for the refurbished Darlington NGS:

- Containment Filtered Venting System (CFVS) and shield tank over pressure relief. CFVS is a new system to prevent failure of containment due to over pressure following severe accidents at multiple units.

7.3 Enhanced Level 3 At-Power Modelling

One of the applications of the Enhanced Level 3 modelling was as input into the Environmental Assessment for the Refurbishment and Continued Operation of the Darlington NGS [R4]. Based on the CNSC October 2011 EA Scoping Information Document, Appendix A [R4], accident sequences that have a frequency of occurrences equal to or greater than 1E-06 (one in a million years) must be studied in the EA. For purposes of the Darlington Refurbishment EA, the selection of a bounding nuclear accident scenario was based on a review of event frequencies from the Enhanced DARA Level 2 models. Of those categories with a mean frequency greater than 1E-06 occ/yr, the highest release is selected as the most limiting. For the enhanced DARA model, this is release category RC7. The enhanced Level 3 model focused on assessment of the consequences of this release category.

Dose consequence estimates were carried out for the bounding event (RC7) following the methodology described in Section 6.0. In the baseline DARA-L3P, this analysis was performed assuming constant wind direction for all plumes. This approach generates conservative results for RC7 compared to a methodology that would allow for a realistic wind-variant calculation. For the other RCs the release is over a shorter time period and using a wind-varient calculation has a lesser impact on the results. For the Enhanced Level 3 DARA model, the RC7 individual dose calculation was performed allowing variation in wind direction from plume to plume as determined from the site meteorological data file.

8.0 SUMMARY OF RESULTS

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

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

Table 11 compares the results of the internal events PRA studies described in Sections 4.0, 5.0, 6.0 and 7.0, with the OPG safety goals.

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. The results in Table 11 show that the large release frequency for the Internal Events At-Power model is above the OPG Safety Goal Target, and the Latent Effects are at the target. When risk results are above the target, action is taken to reduce risk, when cost effective. The first step was to assess the assumptions made when modelling.

An enhancement of the Level 1 At-Power PRA was undertaken, and new analysis was performed to support less conservative assumptions. The major changes in this model are that the modeling of the consequences of steam and feedwater line breaks was revised, and the identification of multi-unit severe core damage sequences (for interface with the Level 2 PRA) was reassessed.

With these major assumptions changed, and some other minor model changes, the calculated severe core damage frequency for the existing plant configuration from at-power internal events was reduced approximately 60%. The large release frequency was reduced by 75%. Despite this significant reduction, the large release frequency is still slightly above the target. OPG is planning to make changes to reduce risk; the four SIOs described in Section 7.0, reflecting the post-refurbishment plant configuration, reduce the internal events risk to well below the safety target.

The internal event PRAs assess the full range of fuel damage and release categories defined in Table 3. These categories are required as input to the Level 3 PRA. The frequency of fuel damage for the at-power internal events PRA (DARA-L1P) is presented in Table 13, as well as the Level 1 enhanced model results with the three SIOs described above that impact Level 1. The results in Table 13 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) is presented in Table 14.

As described in Section 5.1, the fuel damage categories used as end states in the Level 1 PRA are partitioned into Plant Damage States (PDSs) to use as inputs into the Level 2 PRA. Table 15 presents the frequencies of the plant damage states, and Table 16 presents the results of DARA-L2P as well as the Level 2 enhanced model results crediting the four SIOs described above (3 that impact Level 1, plus CFVS that impacts Level 2). Table 17 and Table 18 present the results of DARA-L3P. Table 19 presents the enhanced DARA crediting the four SIOs.

The fire, seismic and flooding results are presented in Table 12. The seismic results present 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 [R24] require use of the 1E-04 per frequency for design of new nuclear power plants and for evaluation of the seismic capacity of existing plants. The fire, seismic results up to the 1E-04 earthquake and flood results are below all the safety goal targets for severe core damage. The seismic results up to the 1E-04 seismic event for large release frequency are above the safety target, but the SIOs described in Section 7.0 are expected to significantly reduce this frequency.

While the large release frequency due to a seismic event is bounded by the severe core damage frequency, the assessment of the containment fragility concluded that containment is robust to seismically induced failure modes.

8.1 Conclusions

The DARA models meet the intent of the corporate Nuclear Safety Policy [R1] and the Canadian Nuclear Safety Commission (CNSC) Standard S-294 [R2]. This comprehensive model assesses risk from internal events, internal floods, internal fires and seismic events.

When the Ontario Provincial Emergency Plan countermeasures are followed, the public health risk meets the OPG risk-based safety goals. Meeting the risk-based safety goal for public health ensures that radiological risks arising from nuclear accidents associated with operation of nuclear reactors are low in comparison to risks to which the public is normally exposed [R3].

As described in Section 8.0, the results of models prepared to meet the requirements of S-294 are below the OPG Safety Goal Limits, demonstrating that the overall risk is low. A small number of release frequency results are above the OPG Safety Goal Targets. The planned changes during refurbishment are expected to reduce these results below the targets, further enhancing safety at the plant.

9.0 REFERENCES

[R1] Ontario Power Generation Inc., Nuclear Safety Policy, N-POL-0001 R001, March 5, 2010.

[R2] Canadian Nuclear Safety Commission, Probabilistic Safety Assessments (PSA) for Nuclear Power Plants, Regulatory Standard S-294, April 2005.

[R3] Ontario Power Generation Inc, Risk and Reliability Program, N-PROG-RA-0016, R06, September 2010.

[R4] Ontario Power Generation Inc., Environmental Impact Statement: Darlington Nuclear Generation Station Refurbishment and Continued Operation, NK38-REP-07730-10002 R000, December 2011.

[R5] CAFTA, Software Manual Version 5.4, EPRI, Palo Alto, CA: 2009. Software Product ID #1018460.

[R6] 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.

[R7] The TUD Office, T-Book - Reliability Data of Components in Nordic Nuclear Power Plants, 6th Edition, ISBN 91-631-7232-1, 2005.

[R8] Westinghouse Savannah River Company, Savannah River Site Generic Data Base Development, File # WSRC-TR-93-262, Rev. 1, May 1998.

[R9] 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.

[R10] FTREX User Manual Version 1.4, EPRI, Palo Alto, CA and KAERI, Daejeon, South Korea: 2008. Software Product ID #: 1016858.

[R11] 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.

[R12] 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.

[R13] Generic Fire Modeling Treatments, Hughes Associates Project Number 1SPH02902.030, Revision 0, January 15, 2008.

[R14] Pipe Rupture Frequencies For Internal Flood Probabilistic Risk Assessments (PRAs), EPRI, Palo Alto, CA: 2009, 1021086 R01.

[R15] 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.

[R16] 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.

[R17] Electric Power Research Institute, Seismic Fragility Application Guide, EPRI TR-1002988, Palo Alto, CA, 2002.

[R18] Electric Power Research Institute, Methodology for Developing Seismic Fragilities, EPRI TR-103959, Palo Alto, CA, June 1994.

[R19] MAAP4-CANDU - Modular Accident Analysis Program for Candu Power Plant Volume 1: User Guidance, Fauske & Associates, Inc, Burr Ridge, Illinois, 1998.

[R20] Emergency Management Ontario, Ontario Provincial Nuclear Emergency Plan, 2009.

[R21] Chanin, D. and Young, M.L., Code Manual for MACCS2, NUREG/CR-6613, Vol. 1 and Vol. 2 (SAND97-0594), May 1998.

[R22] ICRP Publication 60: 1990 Recommendations of the International Commission on Radiological Protection, 1991.

[R23] Draft Regulatory Document RD-152; Guidance on the Use of Deterministic and Probabilistic Criteria in Decision-making for Class I Nuclear Facilities, Canadian Nuclear Safety Commission, May 2009.

[R24] General Requirements for Seismic Design and Qualification of CANDU Nuclear Power Plants, CSA N289.1-08, September 2008.

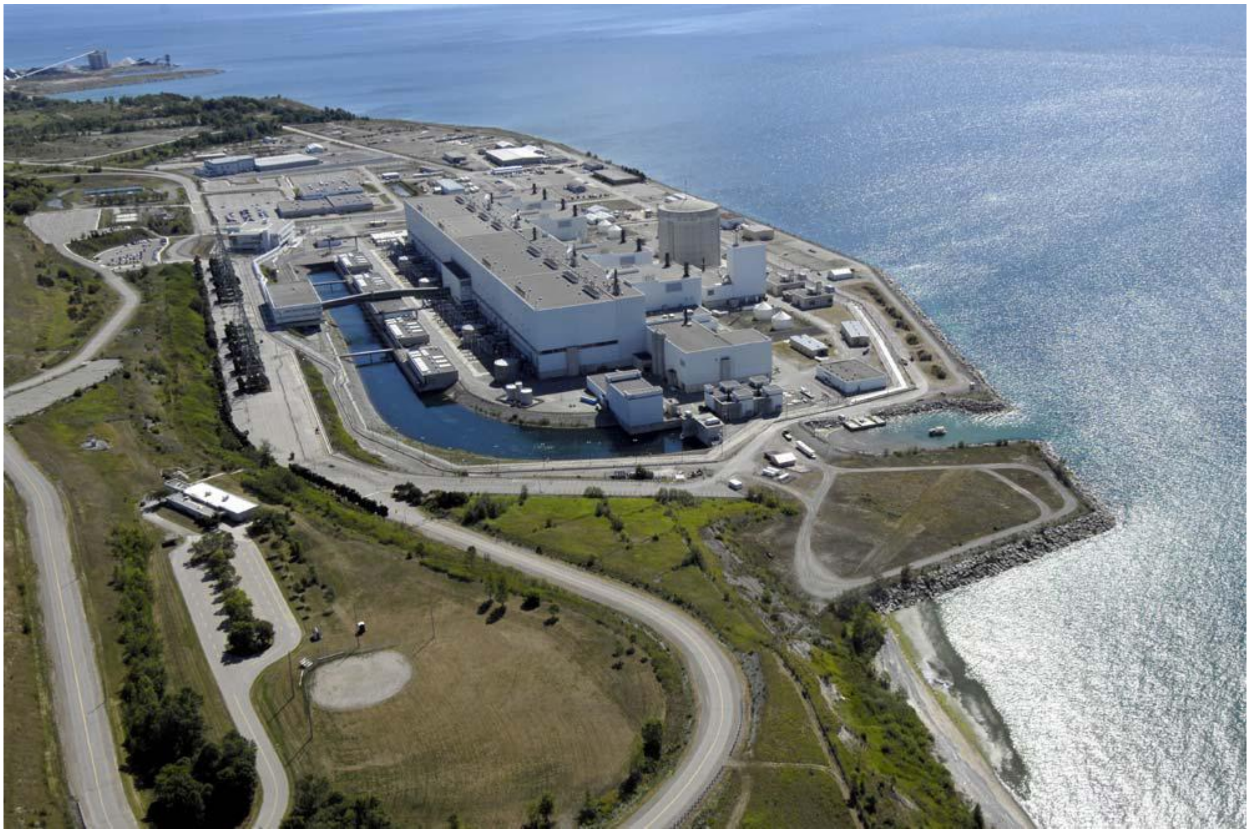


Figure 1: Site Area

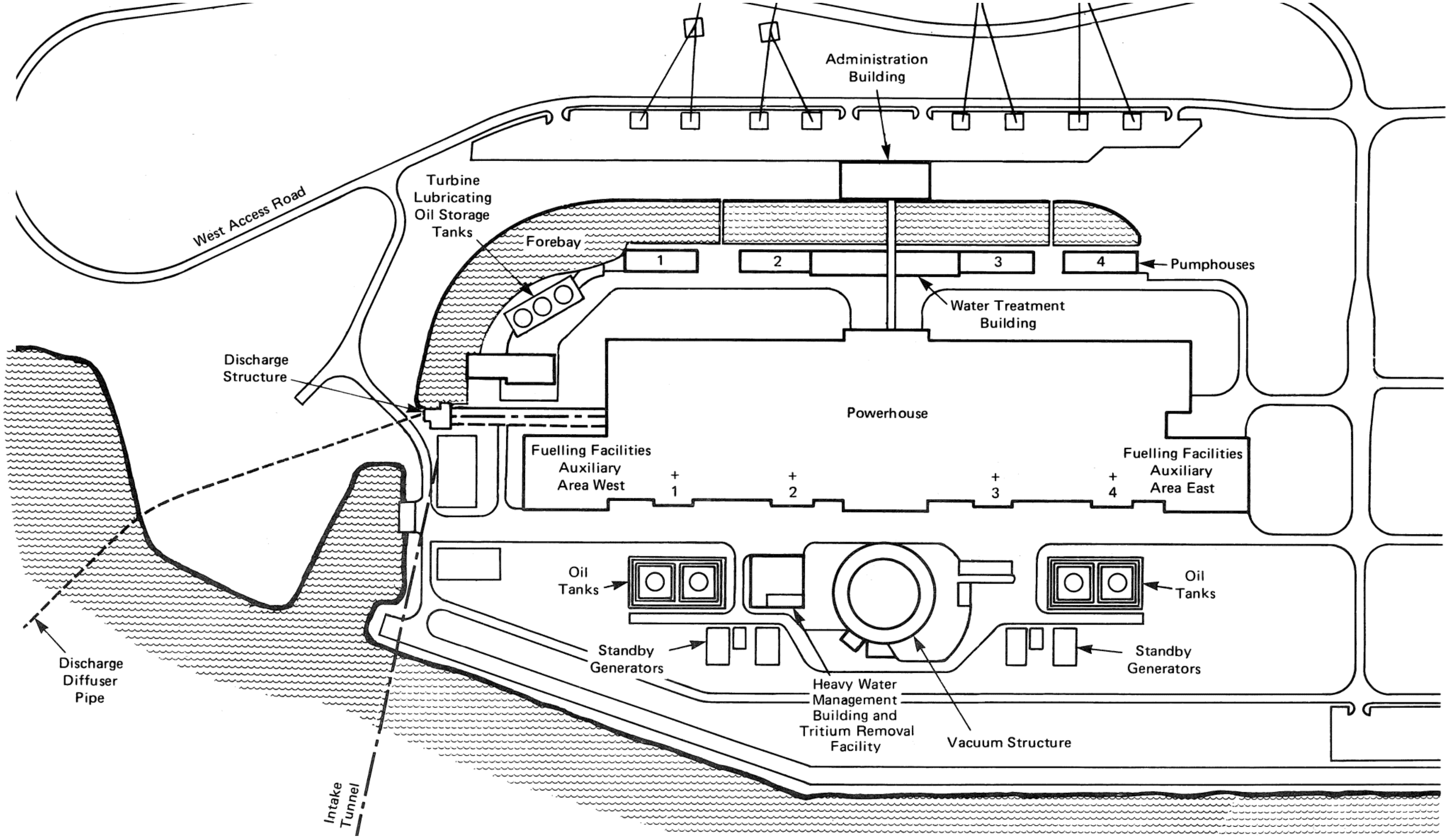
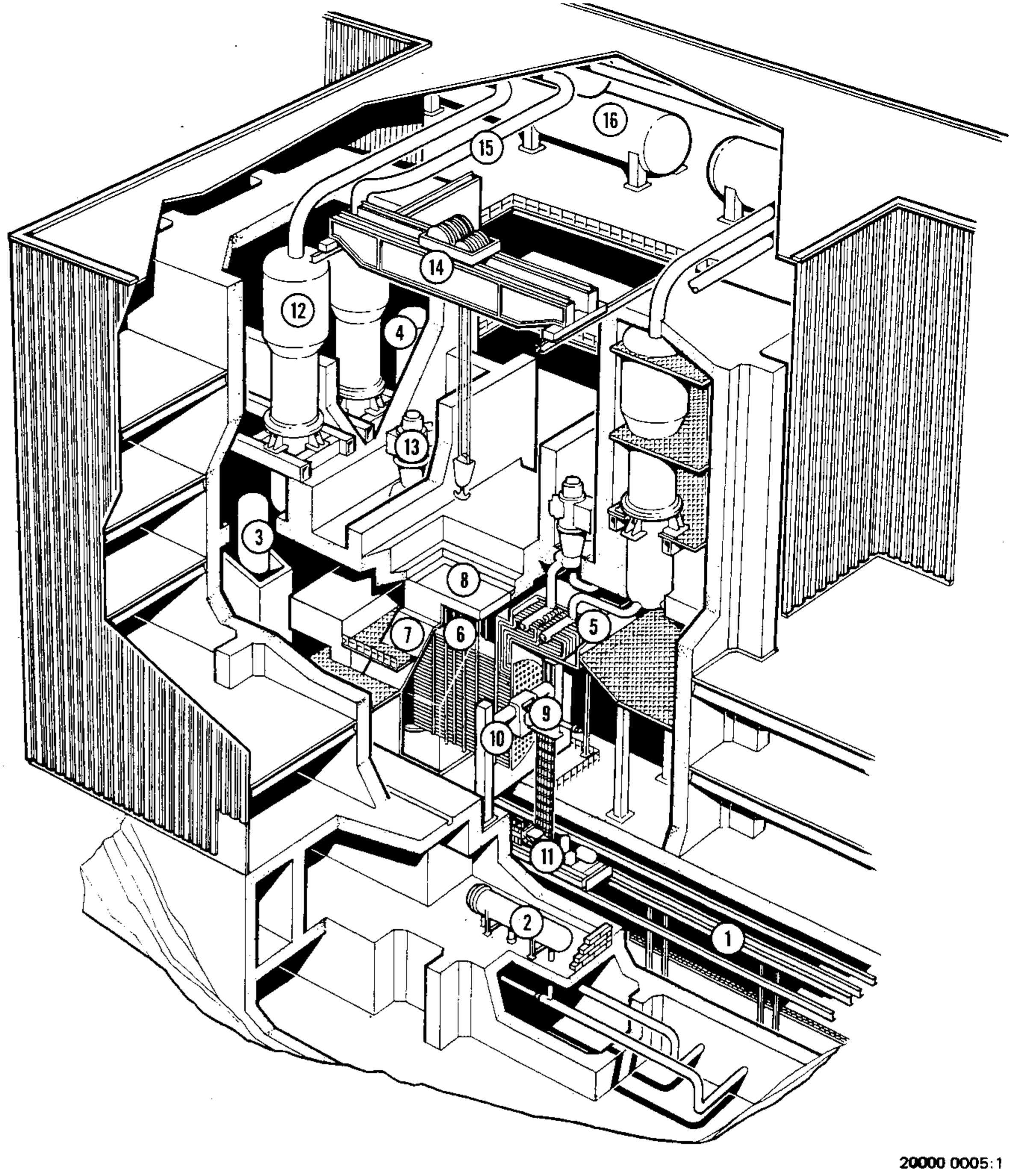
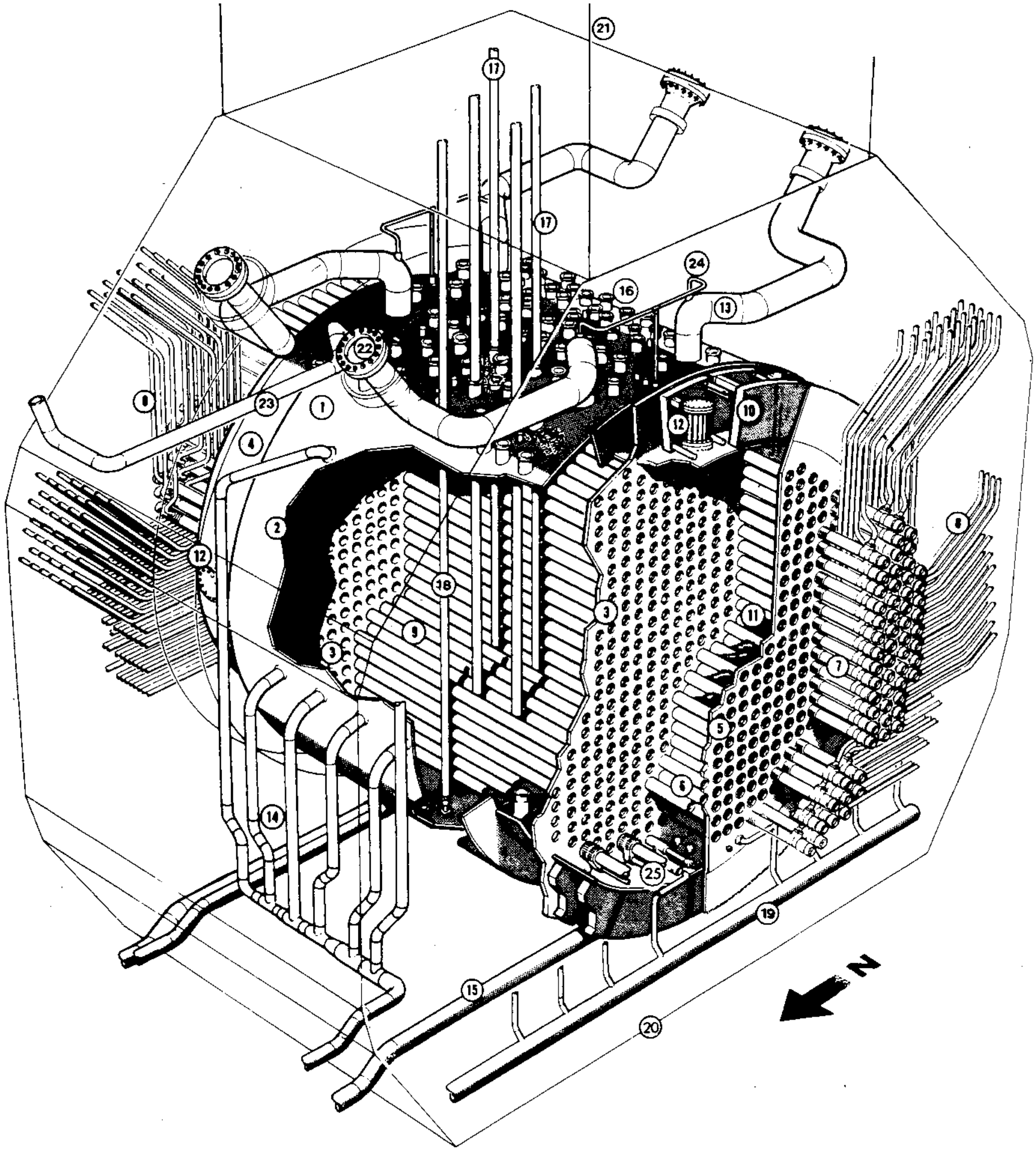


Figure 2: Darlington Station General Arrangement



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

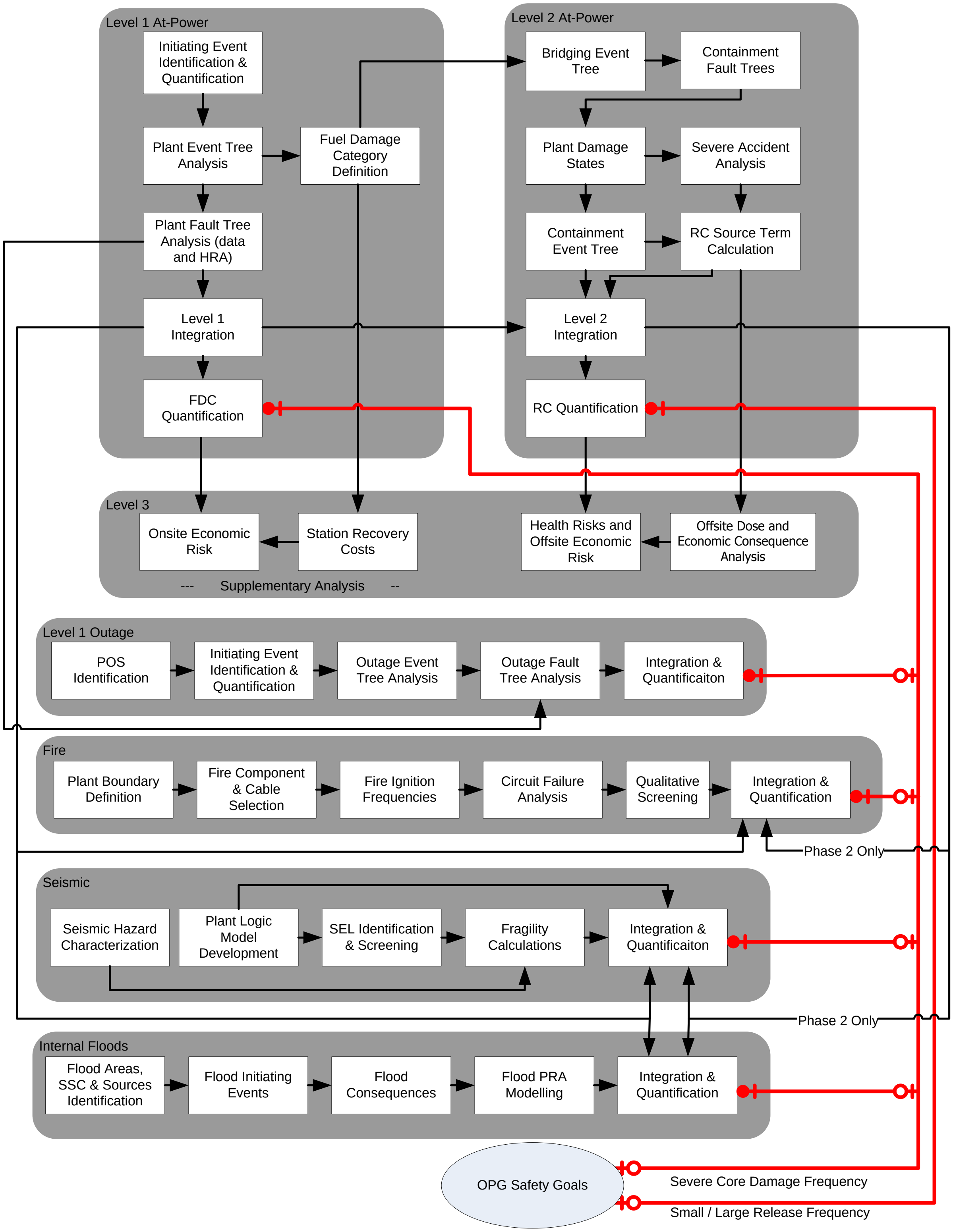

Level 1 At-Power
Initiating Event Identification & Quantification
Plant Event Tree Analysis
Fuel Damage Category Definition
Plant Fault Tree Analysis (data and HRA)
Level 1 Integration
FDC Quantification
Level 2 At-Power
Bridging Event Tree
Containment Fault Trees
Plant Damage States
Severe Accident Analysis
Containment Event Tree
RC Source Term Calculation
Level 2 Integration
RC Quantification
Level 3
Onsite Economic Risk
Station Recovery Costs
Health Risks and Offsite Economic Risk
Offsite Dose and Economic Consequence Analysis
--- Supplementary Analysis --
Level 1 Outage
POS Identification
Initiating Event Identification & Quantification
Outage Event Tree Analysis
Outage Fault Tree Analysis
Integration & Quantificaiton
Fire
Plant Boundary Definition
Fire Component & Cable Selection
Fire Ignition Frequencies
Circuit Failure Analysis
Qualitative Screening
Integration & Quantification
Phase 2 Only
Seismic
Seismic Hazard Characterization
Plant Logic Model Development
SEL Identification & Screening
Fragility Calculations
Integration & Quantificaiton
Phase 2 Only
Internal Floods
Flood Areas, SSC & Sources Identification
Flood Initiating Events
Flood Consequences
Flood PRA Modelling
Integration & Quantification
OPG Safety Goals
Severe Core Damage Frequency
Small / Large Release Frequency

Figure 5: Overview of DARA Models

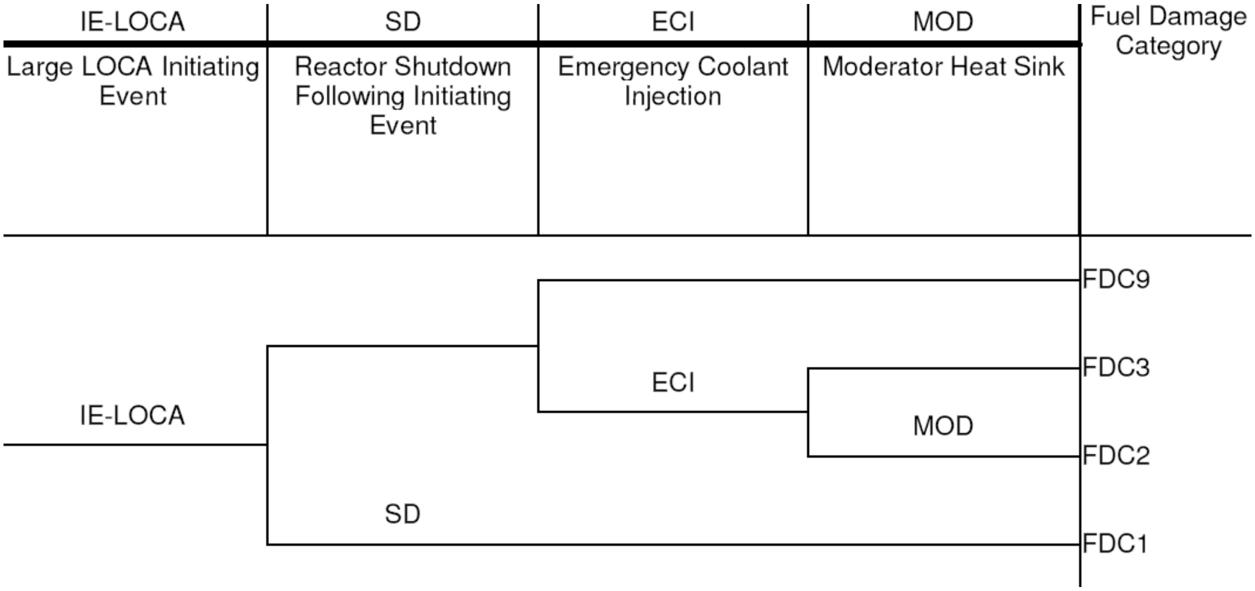

IE-LOCA
Large LOCA Initiating Event
SD
Reactor Shutdown Following Initiating Event
ECI
Emergency Coolant Injection
MOD
Moderator Heat Sink
Fuel Damage Category
FDC9
ECI
FDC3
IE-LOCA
MOD
FDC2
SD
FDC1

Figure 6: Example LOCA Event Tree

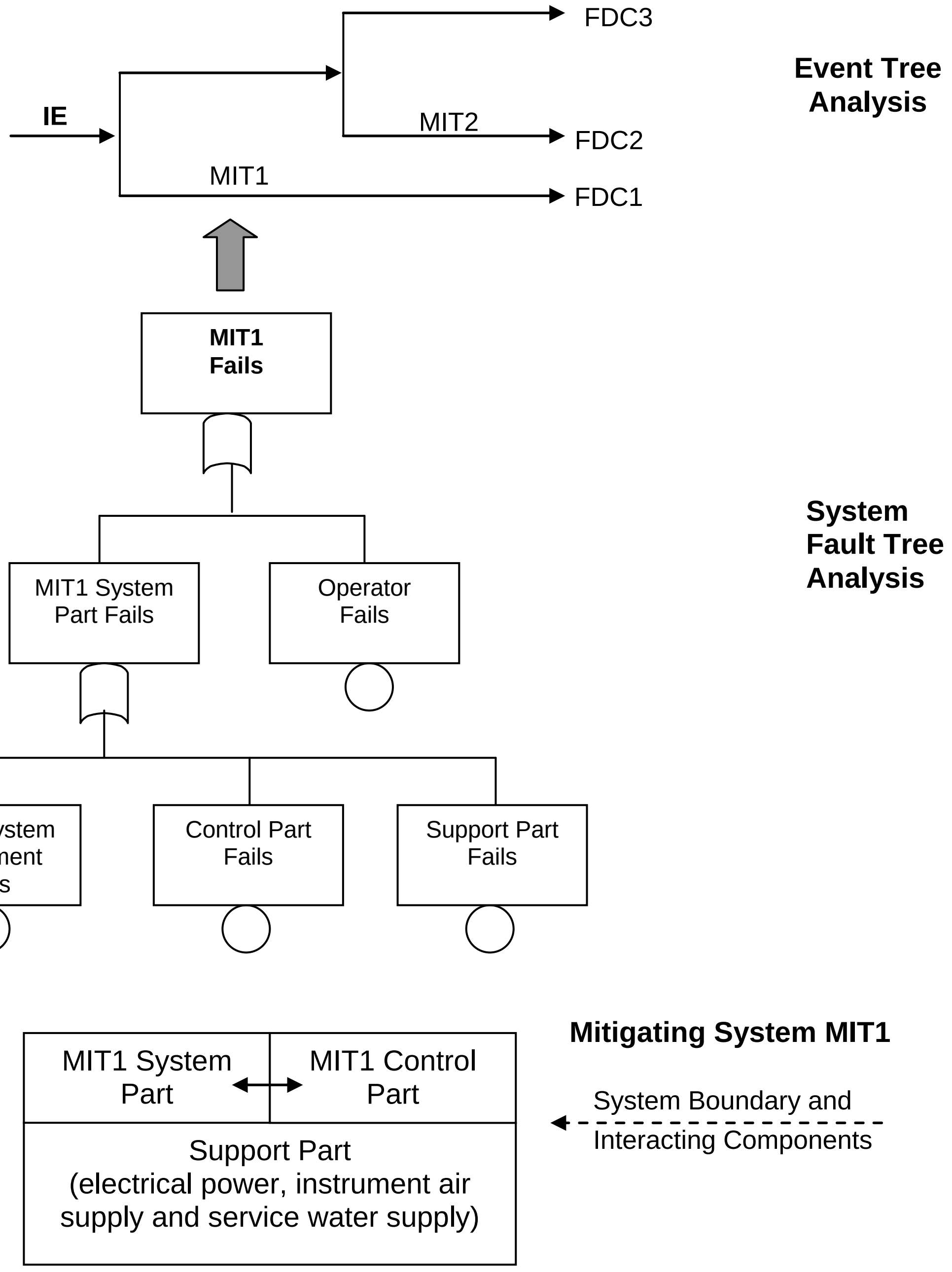


Figure 7: Fault Tree and Event Tree Integration

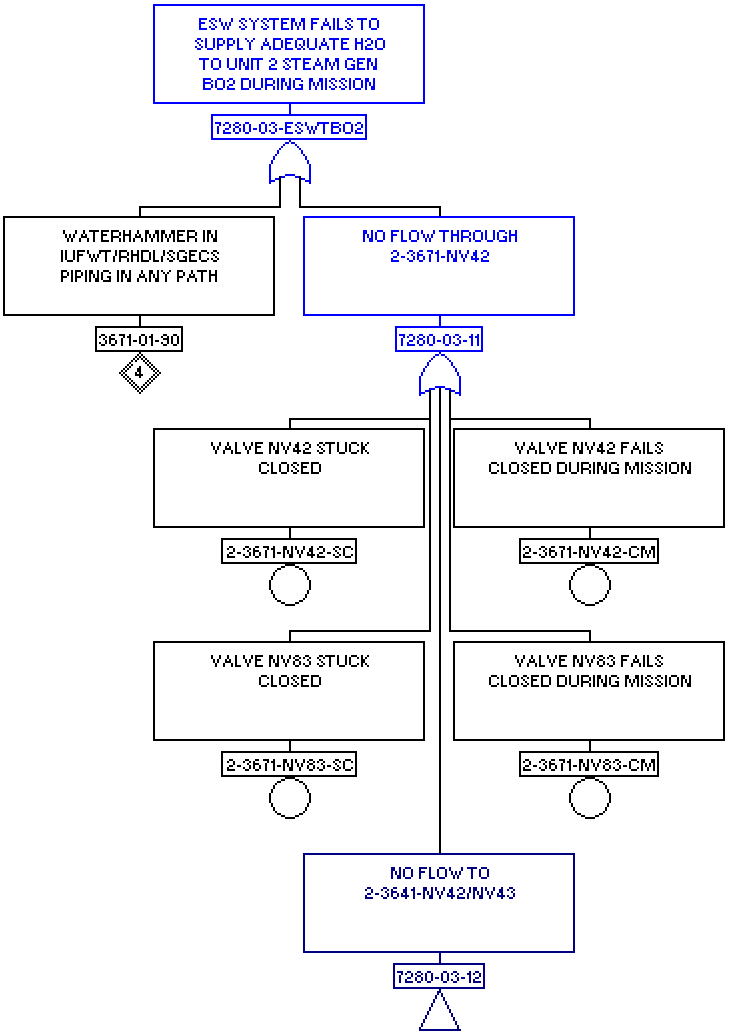

ESW SYSTEM FAILS TO SUPPLY ADEQUATE H2O TO UNIT 2 STEAM GEN BO2 DURING MISSION
7280-03-ESWTBO2
WATERHAMMER IN IUFWT/RHDL/SGECS PIPING IN ANY PATH
3671-01-90
4
NO FLOW THROUGH 2-3671-NV42
7280-03-11
VALVE NV42 STUCK CLOSED
2-3671-NV42-SC
VALVE NV42 FAILS CLOSED DURING MISSION
2-3671-NV42-CM
VALVE NV83 STUCK CLOSED
2-3671-NV83-SC
VALVE NV83 FAILS CLOSED DURING MISSION
2-3671-NV83-CM
NO FLOW TO 2-3641-NV42/NV43
7280-03-12

Figure 8: Example Fault Tree

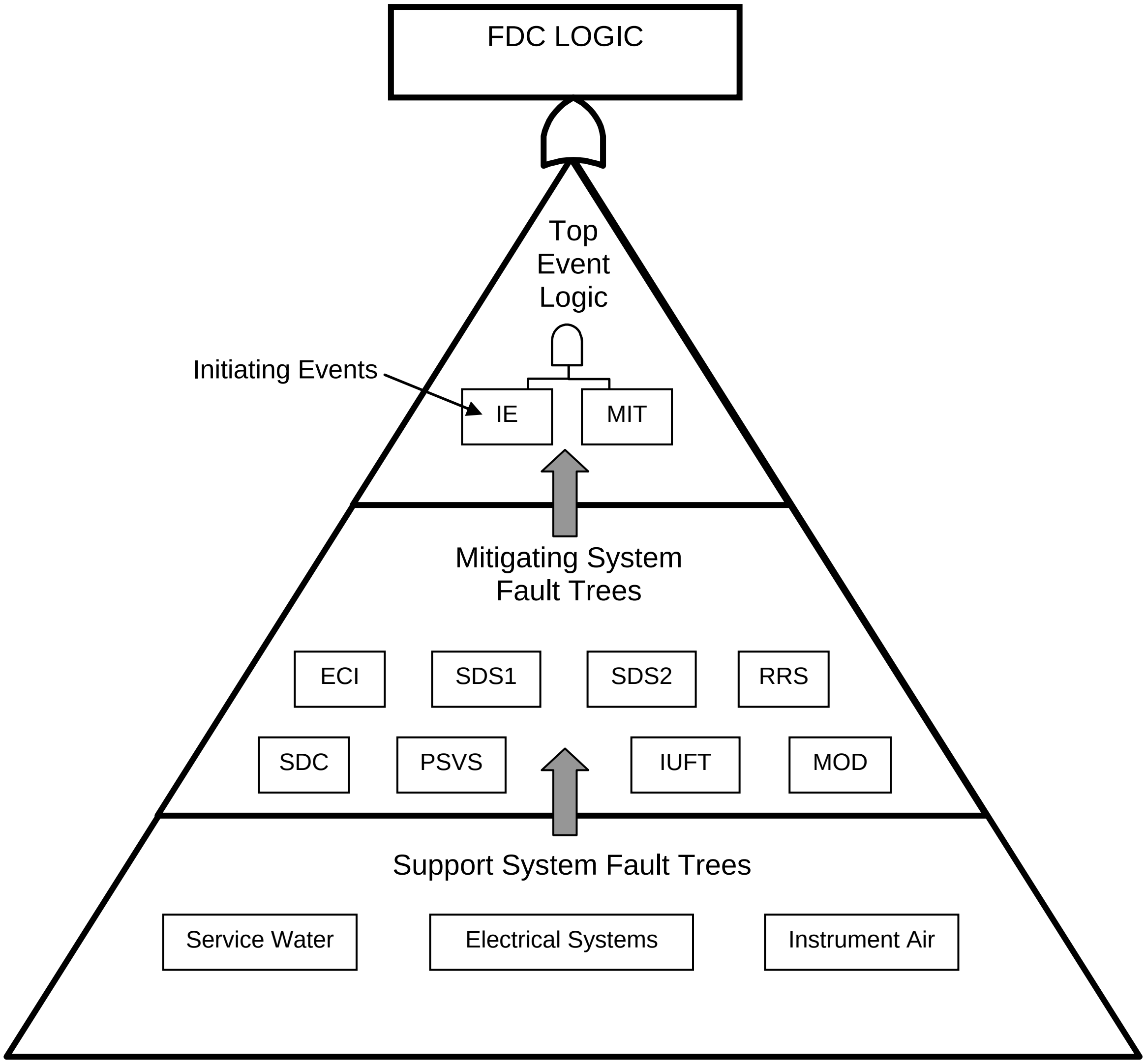


Figure 9: Fault Tree Integration

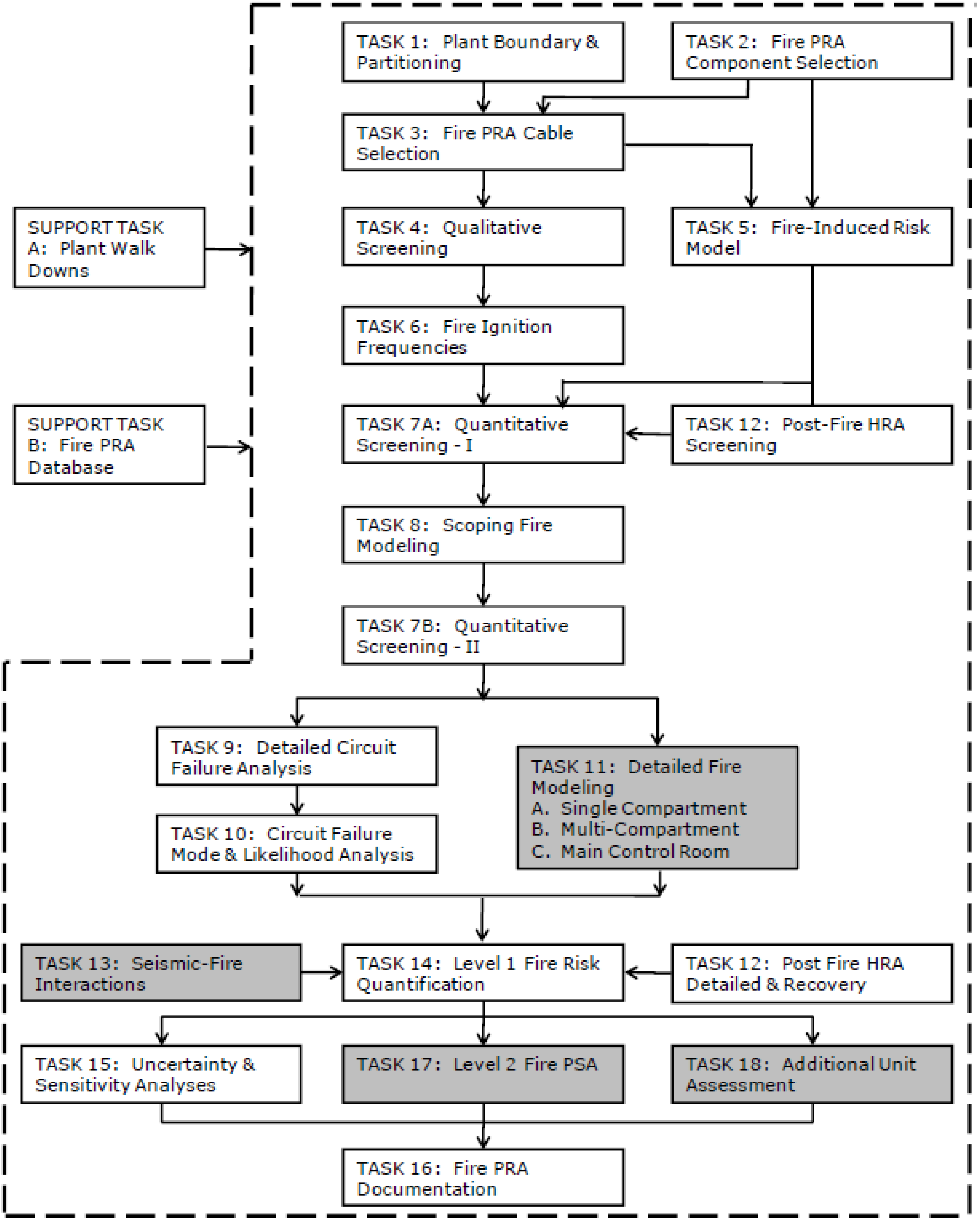

TASK 1: Plant Boundary & Partitioning
TASK 2: Fire PRA Component Selection
TASK 3: Fire PRA Cable Selection
SUPPORT TASK A: Plant Walk Downs
TASK 4: Qualitative Screening
TASK 5: Fire-Induced Risk Model
TASK 6: Fire Ignition Frequencies
SUPPORT TASK B: Fire PRA Database
TASK 7A: Quantitative Screening - I
TASK 12: Post-Fire HRA Screening
TASK 8: Scoping Fire Modeling
TASK 7B: Quantitative Screening - II
TASK 9: Detailed Circuit Failure Analysis
TASK 11: Detailed Fire Modeling
A. Single Compartment
B. Multi-Compartment
C. Main Control Room
TASK 10: Circuit Failure Mode & Likelihood Analysis
TASK 13: Seismic-Fire Interactions
TASK 14: Level 1 Fire Risk Quantification
TASK 12: Post Fire HRA Detailed & Recovery
TASK 15: Uncertainty & Sensitivity Analyses
TASK 17: Level 2 Fire PSA
TASK 18: Additional Unit Assessment
TASK 16: Fire PRA Documentation

Figure 10: Fire PRA Tasks

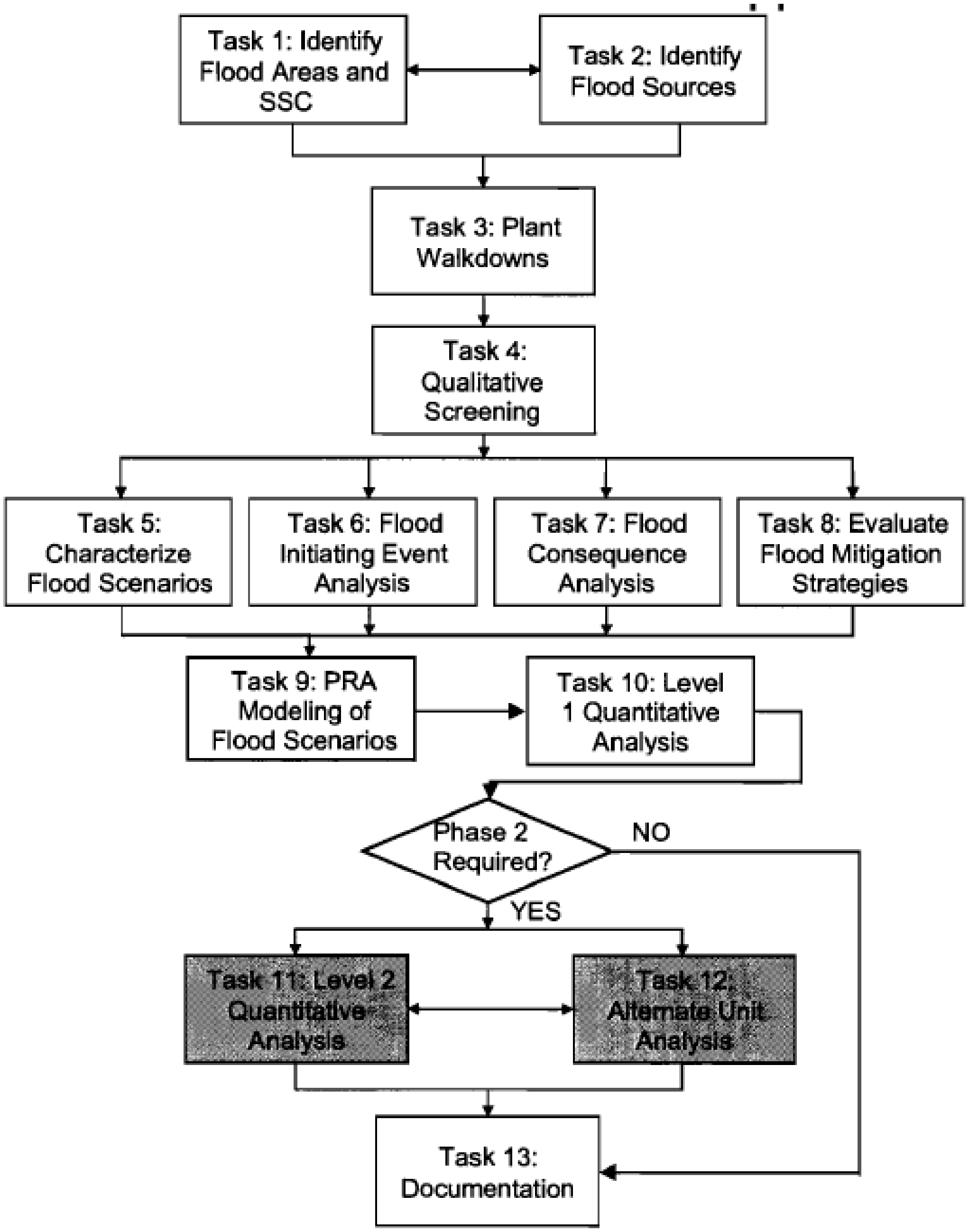

Task 1: Identify Flood Areas and SSC
Task 2: Identify Flood Sources
Task 3: Plant Walkdowns
Task 4: Qualitative Screening
Task 5: Characterize Flood Scenarios
Task 6: Flood Initiating Event Analysis
Task 7: Flood Consequence Analysis
Task 8: Evaluate Flood Mitigation Strategies
Task 9: PRA Modeling of Flood Scenarios
Task 10: Level 1 Quantitative Analysis
Phase 2 Required?
NO
YES
Task 11: Level 2 Quantitative Analysis
Task 12: Alternate Unit Analysis
Task 13: Documentation

Figure 11: Internal Flood Phase 1 Tasks

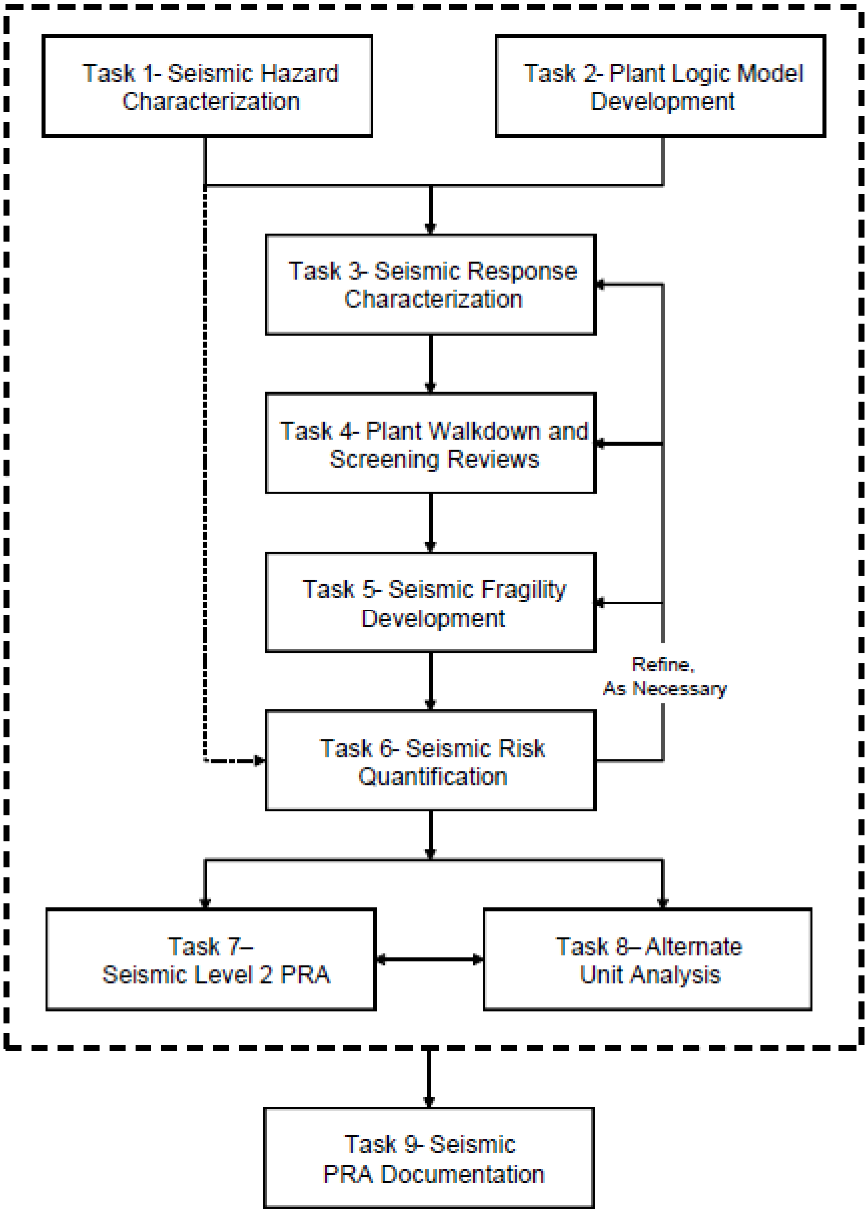

Task 1- Seismic Hazard Characterization
Task 2- Plant Logic Model Development
Task 3- Seismic Response Characterization
Task 4- Plant Walkdown and Screening Reviews
Task 5- Seismic Fragility Development
Refine, As Necessary
Task 6- Seismic Risk Quantification
Task 7– Seismic Level 2 PRA
Task 8– Alternate Unit Analysis
Task 9- Seismic PRA Documentation

Figure 12: Seismic PRA Tasks

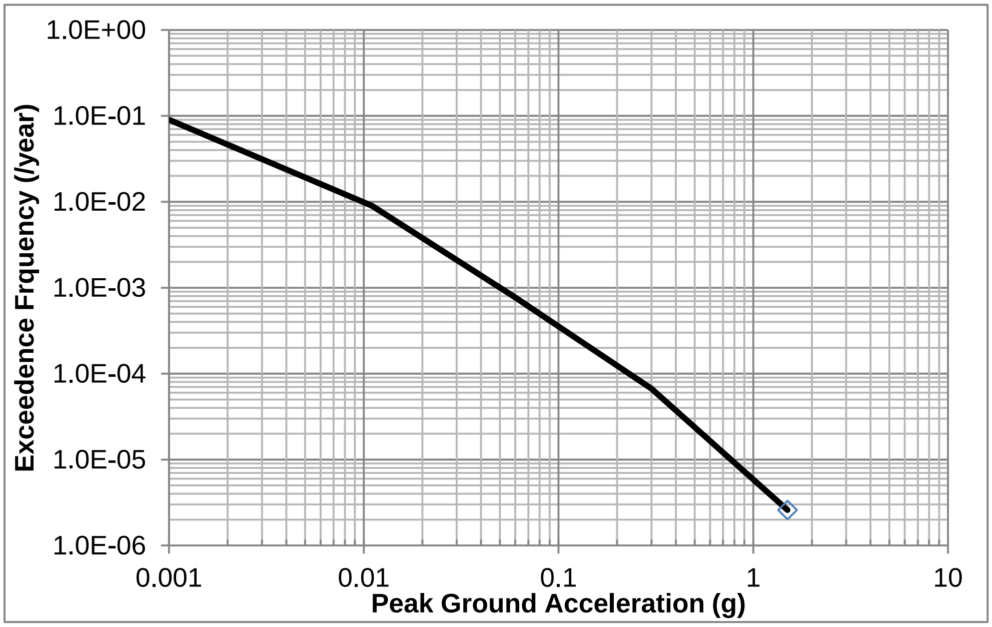


Figure 13: Example Seismic Hazard Curve

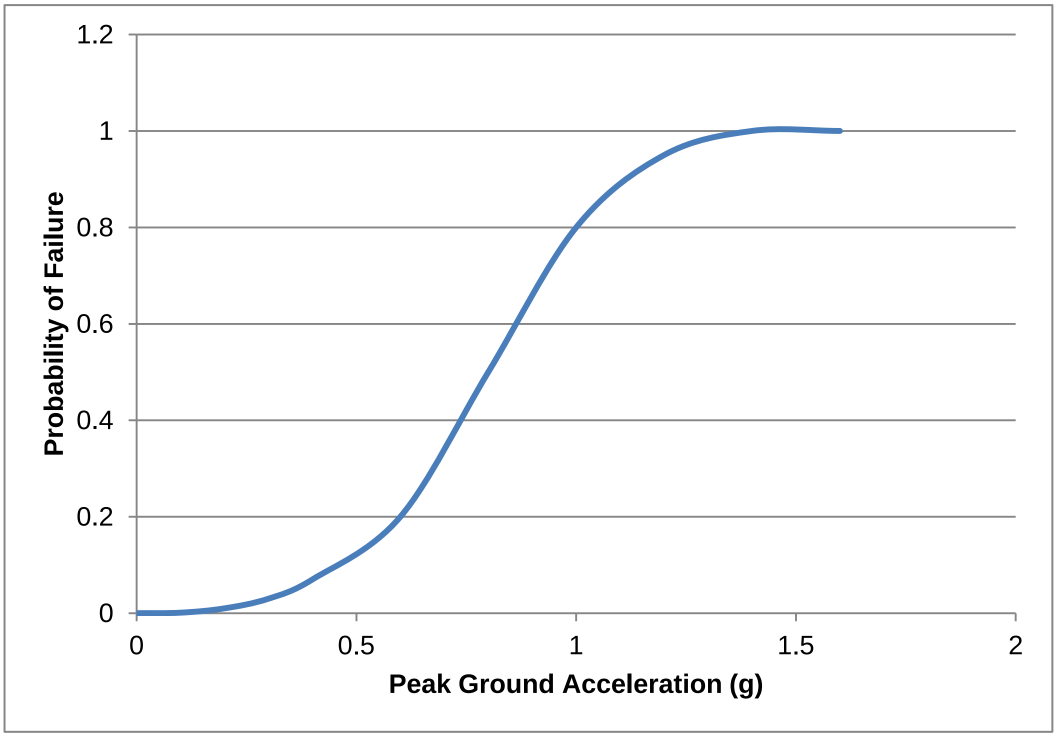


Figure 14: Example Fragility Curve

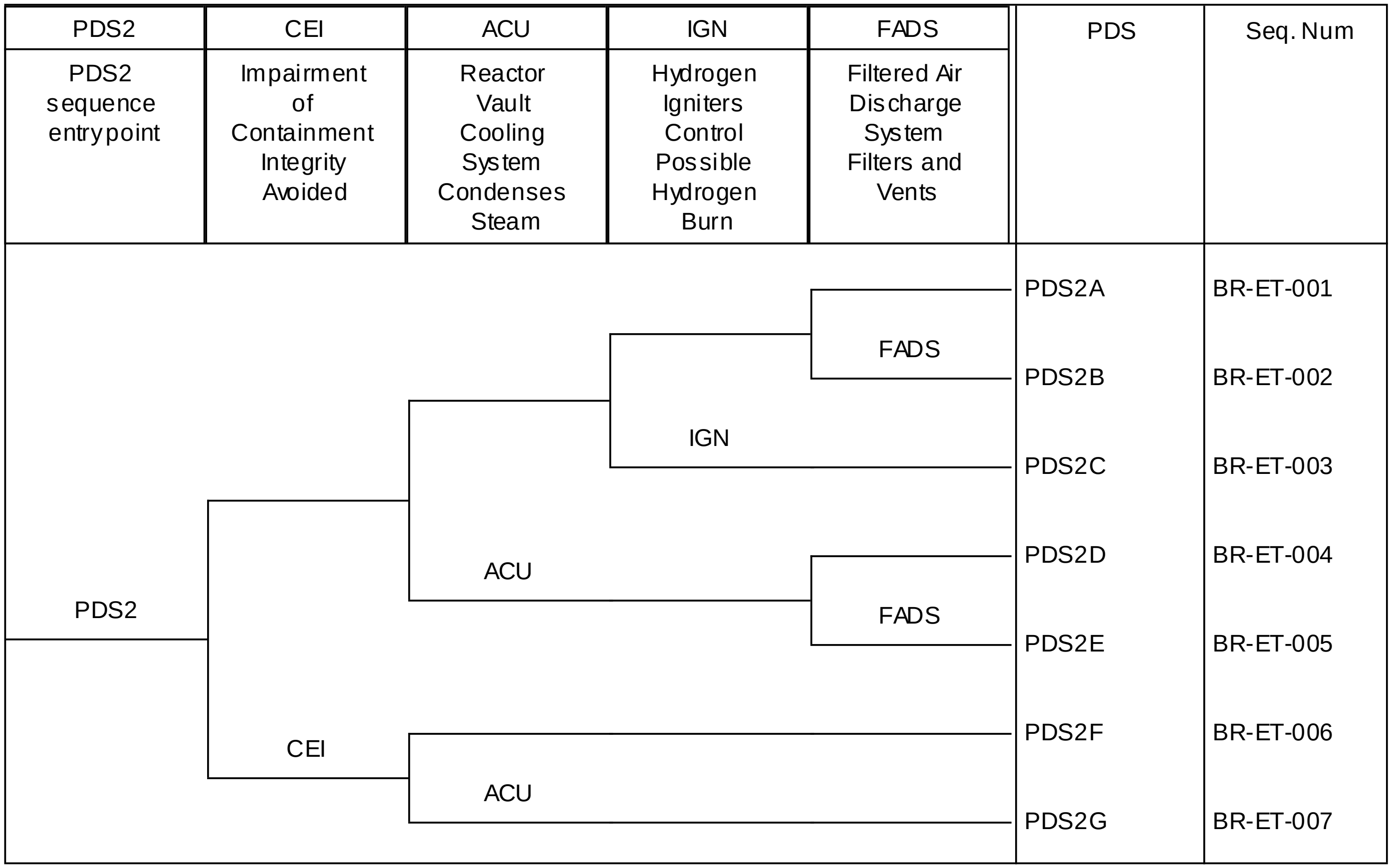
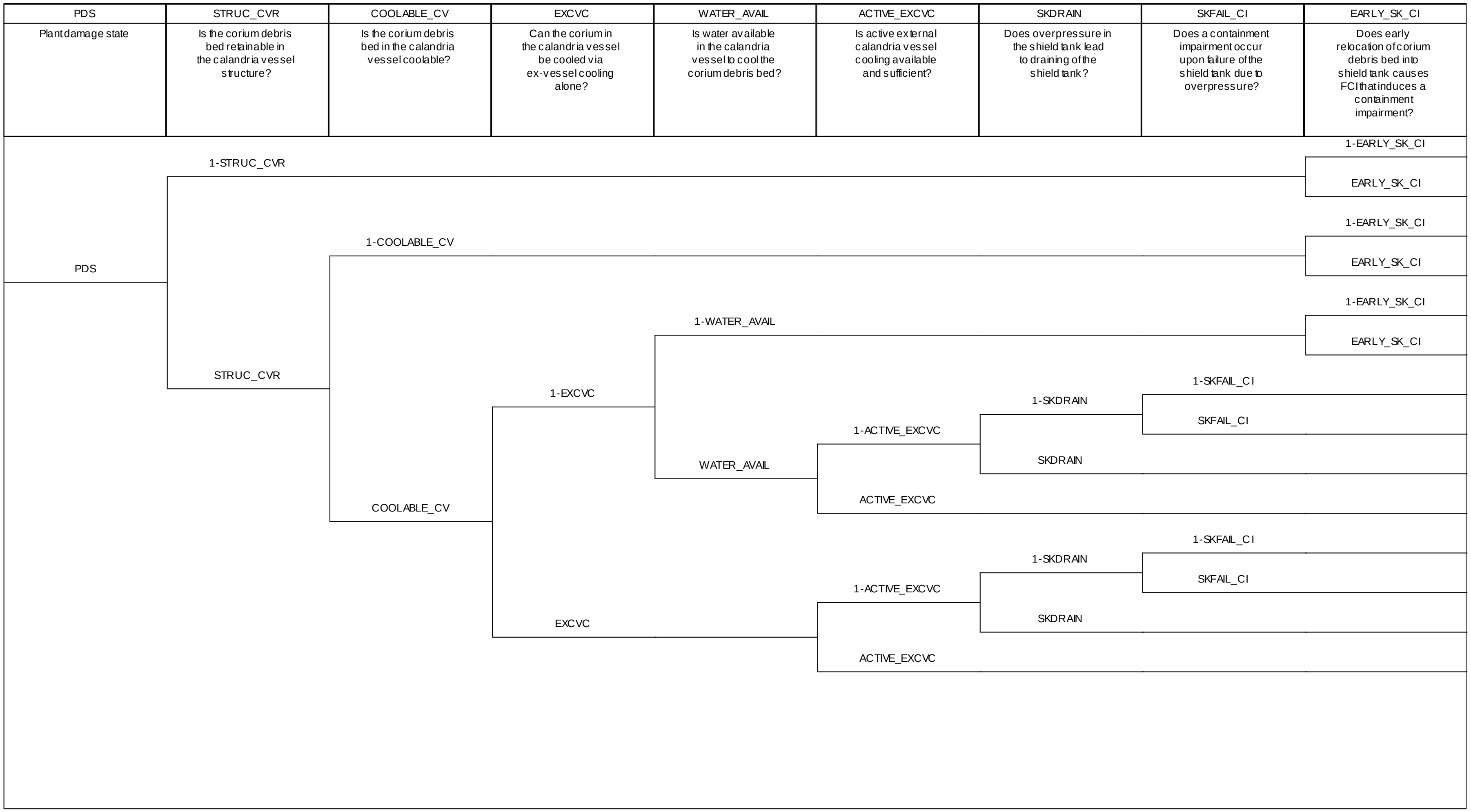

PDS2
PDS2 sequence entry point
CEI
Impairment of Containment Integrity Avoided
ACU
Reactor Vault Cooling System Condenses Steam
IGN
Hydrogen Igniters Control Possible Hydrogen Burn
FADS
Filtered Air Discharge System Filters and Vents
PDS
Seq. Num
FADS
IGN
ACU
FADS
PDS2
CEI
ACU
PDS2A
PDS2B
PDS2C
PDS2D
PDS2E
PDS2F
PDS2G
BR-ET-001
BR-ET-002
BR-ET-003
BR-ET-004
BR-ET-005
BR-ET-006
BR-ET-007

Figure 15: Darlington NGS Bridging Event Tree



PDS	STRUC_CVR	COOLABLE_CV	EXCVC	WATER_AVAIL	ACTIVE_EXCVC	SKDRAIN	SKFAIL_CI	EARLY_SK_CI
Plant damage state	Is the corium debris bed retainable in the calandria vessel structure?	Is the corium debris bed in the calandria vessel coolable?	Can the corium in the calandria vessel be cooled via ex-vessel cooling alone?	Is water available in the calandria vessel to cool the corium debris bed?	Is active external calandria vessel cooling available and sufficient?	Does overpressure in the shield tank lead to draining of the shield tank?	Does a containment impairment occur upon failure of the shield tank due to overpressure?	Does early relocation of corium debris bed into shield tank causes FCI that induces a containment impairment?

Figure 16: Simplified Containment Event Tree

Table 1: OPG Risk Based Safety Goals

SAFETY GOAL	AVERAGE RISK (PER YEAR)	
	Target	Limit
9.1 Severe Core Damage (per unit)[1]	10^{-5}	10^{-4}
9.2 Large Release (per unit)[2]	10^{-6}	10^{-5}
Latent Effects (per site)[3]	10^{-5}	10^{-4}

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

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

[3] Latent effects are defined to be serious irreversible injury to a hypothetical individual at a fixed location near the site boundary arising from the release of radiation to the environment due to operation of a nuclear generating station when averaged over one year

OPG's Risk Based Safety Goals are described in Reference [R3].

Table 2: Darlington At-Power Internal Events PRA Initiating Events

Category	Label	Description
Forced Shutdown	IE-38-FSD	All reactor trips not included in other initiating events
LOCA	IE-38-LOCA1A	A rupture within the capacity of the D_2O transfer system and above the lower LOCA threshold (discharge rate 1-12 kg/s)
	IE-38-LOCA1A-OC	A rupture within the capacity of the D_2O transfer system and above the lower LOCA threshold (discharge rate 1-12 kg/s outside containment).
	IE-38-LOCA1B	A rupture within the capacity of the D_2O feed pump but beyond that of the D_2O transfer system (discharge rate 12-40 kg/s)
	IE-38-LOCA1B-OC	A rupture within the capacity of the D_2O feed pump but beyond that of the D_2O transfer system (discharge rate 12-40 kg/s outside containment)
	IE-38-LOCA1C	A rupture within the capacity of two D_2O feed pumps but beyond the capacity of one D_2O feed pump (discharge rate 40-70 kg/s)
	IE-38-LOCA2A	Small breaks (discharge rate 70-220 kg/s)
	IE-38-LOCA2B	Small breaks (discharge rate 220-1000 kg/s)
	IE-38-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)
	IE-38-LOCA4	Large breaks which lead to significant flow degradation in the core (initial discharge rate >2000 kg/s)
	IE-38-LOCATOP	A LOCA2 size break in HT piping connected to the top of the pressurizer
	IE-38-LOCA1-SF	Stagnation feeder break in LOCA1 range
	IE-38-LOCA2-SF	Stagnation feeder break in LOCA2 range
	IE-38-LOCA2-SDC	A LOCA2 size break in the PHT-SDC interface piping inside a SDC room
Pressure Tube Rupture	IE-38-PTF	Pressure tube break resulting in a discharge rate in excess of 1 kg/s
Pressure Tube Leak	IE-38-PTL	Pressure tube break resulting in a discharge rate of less than 1 kg/s
End-fitting Failure	IE-38-EFL1WAGA	LOCA1A size break inside annulus gas bellows
	IE-38-EFL1WAGB	LOCA1B size break inside annulus gas bellows
	IE-38-EFL1WAGC	LOCA1C size break inside annulus gas bellows
	IE-38-EFL1OAGA	LOCA1A size break outside annulus gas bellows
	IE-38-EFL1OAGB	LOCA1B size break outside annual gas bellows

Category	Label	Description
	IE-38-EFL1OAGC	LOCA1C size break outside annulus gas bellows
	IE-38-EFL1FMIA	LOCA1A size break involving the fuelling machine
	IE-38-EFL1FMIB	LOCA1B size break involving the fuelling machine
	IE-38-EFL1FMIC	LOCA1C size break involving the fuelling machine
	IE-38-EFL2WAG	LOCA2 size break inside annulus gas bellows
	IE-38-EFL2OAG	LOCA2 size break outside annulus gas bellows
	IE-38-EFL2FMI	LOCA2 size break involving the fuelling machine
Steam Generator Tube Rupture	IE-38-SGTB1	Steam generator tube break with discharge rate within the capacity of the D_2O feed system (< 70 kg/s)
	IE-38-SGTB2	Steam generator tube break with discharge rate beyond the capacity of the D_2O feed system (> 70 kg/s)
Loss of HT Pressure Control (Low)	IE-38-LRVO	One or more liquid relief valves fail open
	IE-38-FVFC	Both D_2O feed valves fail closed
	IE-38-SBVO	Any pressurizer steam bleed or relief valve fails open
Loss of HT Pressure Control (High)	IE-38-PHFO	Pressurizer heaters energized spuriously
	IE-38-BVFC	Both HT bleed valves fail closed
	IE-38-FVFO	Any D_2O feed valve fails open
	IE-38-FP2S	Inadvertent start-up of inactive feed pump
	IE-38-BCLCVFC	Bleed condenser level control valves fail closed
	IE-38-PSBVFC	Pressurizer steam bleed valves fail closed when required open
HT Pressure and Inventory Control Failure	IE-38-D2OFDL	Pipe break in D_2O feed system upstream of check valve NV61
	IE-38-FBSICL	Feed/bleed system pipe break inside containment
	IE-38-XSPR	Bleed condenser spray valve CV12 opens spuriously
HT Pump Trip	IE-38-HTPT1	Pump trip in 2/2 mode
Channel Flow Blockage	IE-38-LFB	Channel flow reduced by 70% or more
Moderator Failure	IE-38-LOCOOL	Loss of moderator cooling resulting in setback
	IE-38-SLOMA	Loss of moderator inventory within capacity of moderator D_2O recovery system (discharge rate 1-70 kg/s)
	IE-38-LLOMA	Loss of moderator inventory beyond capacity of moderator D_2O recovery system (discharge rate > 70 kg/s)

Category	Label	Description
Loss of End Shield Cooling	IE-38-LOESHS	Loss of end shield heat sink
	IE-38-LOESF	Total loss of end shield flow
	IE-38-LOESI1	Non-isolable pressure boundary rupture
	IE-38-LOESI2A	Rupture upstream of V15/V16 where isolation leads to loss of circulation
	IE-38-LOESI2B	Rupture upstream of V15/V16 where isolation does not lead to loss of circulation
Steam Line Break	IE-38-SSLB1	Small break that requires reactor shutdown but does not cause global harsh environment
	IE-38-SSLB3	A feedwater line break downstream of the last check valve before the steam generator (assumed to be in SG1 flowpath)
	IE-38-LSLB1	Large break in the unit adjacent to the analyzed unit, with potential for in-plant environmental consequences
	IE-38-LSLB2	Large break with in-plant environmental consequences
	IE-38-SRV	Any SRV, ASDV, or CSDV opens spuriously
Loss of Feedwater to Steam Generators	IE-38-LOFWB	LOFW resulting in a reactor trip but greater than 3% full flow remains
	IE-38-LOFWC	LOFW to less than 3% full flow
Feedwater Line Break	IE-38-SFLB1	Break resulting in reactor shutdown but with sufficient feedwater available to remove decay heat
	IE-38-LFLB1	Large FW Line Break in Adjacent Unit 1
	IE-38-LFLB2	Large FW Line Break in Unit 2 Causing Total Loss of Feedwater
	IE-38-FLBSG	Isolable break downstream of LCVs resulting in total loss of feedwater to one steam generator (assumed to be in SG1 flowpath)
	IE-38-FLBCOND1	Break in condensate system resulting in total loss of feedwater
Turbine Trip	IE-38-TT	All turbine trips not included in other initiating events
Loss of Condenser Vacuum	IE-38-LOVAC	Loss of condenser vacuum resulting in a turbine trip
High Pressure Reheater Drains Line Break to SG	IE-38-RDLB	Break in lines between steam generators and second check valve (assumed to be in SG1 flowpath)

Category	Label	Description
Loss of Condensate Flow	IE-38-LOCOND	Total loss of condensate flow to deaerator
Unplanned Bulk Increase in Reactivity	IE-38-UFBIR	Unplanned fast (> 0.2 mk/s) bulk increase in reactivity
	IE-38-USBIR	Unplanned slow (< 0.2 mk/s) bulk increase in reactivity
Unplanned Regional Increase in Reactivity	IE-38-URIR	Local neutron overpower
Loss of Computer Control	IE-38-WDTOX	Controlling computer stall
	IE-38-DCCF	Dual computer failure
	IE-38-DCCUF	Unsafe failure of DCC leading to reactor power increase
	IE-38-HTPF	Failure "off" of an individual control program on both computers
	IE-38-SGLCF	
	IE-38-SGPCF	
	IE-38-MTCF	
	IE-38-DLCF	
Loss of LPSW System	IE-38-LOLPSW	Total loss of LPSW flow out of header L205
	IE-38-LOPH	Loss of flow to the pumphouse
	IE-38-LOTH	Loss of flow to the turbine hall
Loss of RCW System	IE-38-LORCW	Total loss of RCW flow
Loss of Powerhouse Upper Level Service Water	IE-38-LOPULSW	Total loss of PULSW flow
Loss of Instrument Air	IE-38-TLOIA	Total loss of instrument air out of line L17
Loss of Cooling to F/M in Transit	IE-38-LOFMCIT	Loss of cooling to fuelling machine in transit
Loss of Bulk Electricity Supply	IE-38-LOBES	Loss of BES

Category	Label	Description
Loss of Switchyard	IE-38-LOSWYD	Loss of both switchyard buses BU1 and BU2
Loss of Unit Class IV 13.8 kV Bus	IE-38-LOCL4	Total loss of Unit Class IV 13.8 kV power
	IE-38-LOBU1	Loss of power to Unit Class IV 13.8 kV bus BU1
	IE-38-LOBU2	Loss of power to Unit Class IV 13.8 kV bus BU2
	IE-38-LOBU3	Loss of power to Unit Class IV 13.8 kV bus BU3
	IE-38-LOBU4	Loss of power to Unit Class IV 13.8 kV bus BU4
Partial Loss of Unit Class IV Power	IE-38-FS1CB2	Loss of Unit Class IV 13.8 kV buses BU1 and BU3 due to 1CB2 failing short
	IE-38-FS2CB2	Loss of Unit Class IV 13.8 kV buses BU2 and BU4 due to 2CB2 failing short
Partial Loss of Unit Class III Power	IE-38-LOBU7	Loss of power to Unit Class III 4.16 kV bus BU7
	IE-38-LOBU8	Loss of power to Unit Class III 4.16 kV bus BU8
	IE-38-LOBU13	Loss of power to Unit Class III 600 V bus BU13
	IE-38-LOBU14	Loss of power to Unit Class III 600 V bus BU14
	IE-38-LOBU15	Loss of power to Unit Class III 600 V bus BU15
	IE-38-LOBU16	Loss of power to Unit Class III 600 V bus BU16
Partial Loss of Unit Class II 120 V Power	IE-38-LOBUA3	Loss of Unit Class II 120 V ac bus BUA3
	IE-38-LOBUB3	Loss of Unit Class II 120 V ac bus BUB3
	IE-38-LOBUC3	Loss of Unit Class II 120 V ac bus BUC3
Partial Loss of Unit Class II 45 V Power	IE-38-LO45VA	Loss of Unit Class II 45 V dc at panel 2383-11
	IE-38-LO45VB	Loss of Unit Class II 45 V dc at panel 2859-21
	IE-38-LO45VC	Loss of Unit Class II 45 V dc at panel 3485-C1
Partial Loss of Unit Class I 48 V Power	IE-38-LOBUA4	Loss of Unit Class I 48 V dc BUA4
	IE-38-LOBUB4	Loss of Unit Class I 48 V dc BUB4
	IE-38-LOBUC4	Loss of Unit Class I 48 V dc BUC4
	IE-38-LOBUA141	Loss of EPS 48 V dc bus BUA141
	IE-38-LOBUB141	Loss of EPS 48 V dc bus BUB141
Loss of Forebay	IE-38-FOREBAY	Loss of forebay leading to loss of Circulating Water System and/or Low Pressure Service Water, in one or more units, and/or Emergency Service Water
ECI Blowback	IE-38-BLOWBACK	Emergency Coolant Injection Blowback
Powerhouse Freeze	IE-38-PHFREEZE	Spurious opening of powerhouse venting dampers during extreme cold outside conditions

Table 3: 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.	LOCA with failure of ECIS and failure of moderator heat sink.
3	Moderator required as heat sink in the short term (< 1 hr after reactor trip).	LOCAs of LOCA2 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 LOCA2 size or greater and failure of ECI Recovery before 24 hours. Total loss of steam generator and SDC heat sink (LHS) with ECI successful.
5	Moderator required as heat sink in the long term (> 24 hr after reactor trip).	LOCA1 and failures of D_2O makeup and ECI Recovery. LOCAs of LOCA2 size or greater and failure of ECI Recovery after 24 hours.
6	Temporary loss of cooling to fuel in many channels.	LOCA4. LOCA2 and failure to cooldown
7	Single channel fuel failure with sufficient release of steam or radioactivity to initiate automatic containment button-up.	End-fitting LOCA2 and fuel ejection. LOCA2 stagnation feeder break.
8	Single channel fuel failure with insufficient release of steam or radiation activity to initiate automatic containment button-up.	In-core LOCA and fuel ejection. Large flow blockage. LOCA1 stagnation feeder break. Loss of F/M cooling in transit.
9	LOCAs with no fuel failure (ECIS successful); potential for significant economic impact.	LOCA2 and LOCA3. LOCA1 with no D_2O makeup.

Table 4: 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 D2O 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	*
D2O Recovery and Transfer Systems	Y	Y	*
Room Air Conditioning System	Y	Y	*
Hostile Environment Events (including Powerhouse Emergency Venting System)	Y	Y	*
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 and flooding risk is calculated through modifications or interrogations based on the integrated severe core damage model from the Internal Events At-Power Level 1 PRA, and do not include specific fault tree models for the individual plant systems.

Table 5: DARA-L1O Plant Operational State Definition

Input Parameter	Plant Operational State (POS)				
	A	B	C	D	E
GSS	OPGSS	OPGSS	OPGSS	DGSS	OPGSS
HTS Inventory Level	Full	GFS	LLDS	LLDS	Full
HTS Boundary Configuration	Closed	Closed	Open	Open	Closed
HTS Temp (Nominal)	<60°C	30°C	30°C	30°C	55°C
HTS Pressure	Pressurized 4.3-7.5 MPa	Depressurized < 1.0 MPa	Depressurized ~0 kPa(g)	Depressurized ~0 kPa(g)	Pressurized 4.3-7.5 MPa
Primary Heat Sink (Circulation)	HTS Pumps or SDC Pumps	SDC Pumps	SDC Pumps	SDC Pumps	HTS Pumps or SDC Pumps
Primary Heat Sink (Heat Removal)	SDC HXs	SDC HXs	SDC HXs	SDC HXs	SDC HXs
Backup Heat Sink (Circulation)	SDC Pumps or HTS Pumps[Note1]	Various (SDC, NC, HTS Pumps and Steam Generators)	Various (SDC, NC, HTS Pumps and Steam Generators)	Various (SDC, NC)	SDC Pumps or HTS Pumps[Note1]
Backup Heat Sink (Heat Removal)	Steam Generators				Steam Generators
Decay Power	0.541 %FP	0.100 %FP	0.316 %FP	0.113 %FP	0.084 %FP
Outage Day Number (Typical Planned Duration)	1-3 (3 days)	32-41 (10 days)	4-26.5 (22.5 days)	26.5-31 (5.5 days)	42-44 (3 days)
Weighted Duration (Accounting for Unplanned Outage Contributions)	3.5 days	10.5 days	22 days	5 days	3 days

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

Table 6: Initiating Events (IEs) for Darlington Level 1 Outage PRA

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
LOBUA4	Loss of Unit Class I 48 V dc BUA4	Y	Y	Y	Y	Y

Outage IE Label	IE Definition	POS Applicability				
		A	B	C	D	E
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 7: 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 PRA. 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 PRA. 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 PRA.
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 the 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 the DARA-L1O since the DARA Level-1 At-Power PRA 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 the 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 8: Seismic Hazard Bins

Bin #	Seismic Interval (g)	Magnitude For Fragility Calculation (g)	Seismic Interval Frequency (1/yr)*
1	0.03 - 0.08	0.05	1.21E-05
2	0.08 - 0.2	0.13	4.24E-05
3	0.2 - 0.3	0.24	1.22E-05
4	0.3 - 0.5	0.39	9.26E-06
5	0.5 - 0.7	0.59	3.41E-06
6	0.7 - 1	0.84	2.02E-06
7	1 - 2	1.41	1.41E-06
8	>2	2	3.04E-07

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

Table 9: Summary of Selected Accident Sequence

PDS	Representative Accident Sequence
PDS1	No representative sequence defined.
PDS2A	LOCA2A, with loss of moderator cooling and failure of ECIS injection.
PDS2B	LOCA2A, with loss of moderator cooling and failure of ECIS injection, combined with EFADS system failed.
PDS2C	LOCA2A, with loss of moderator cooling and failure of ECIS injection, combined with failure of hydrogen igniters.
PDS2D	LOCA2A, with loss of moderator cooling and failure of ECIS injection, combined with failure of reactor vault ACUs.
PDS2E	LOCA2A, with loss of moderator cooling and failure of ECIS injection, combined with failure of reactor vault ACUs and failure of EFADS.
PDS2F	LOCA2A, with loss of moderator cooling and failure of ECIS injection, combined with containment envelope impairment.
PDS2G	LOCA2A, with loss of moderator cooling and failure of ECIS injection, combined with containment envelope impairment and failure of reactor vault ACUs.
PDS3	Common mode failure, combined with failures causing station blackout, leading to a loss of heat sink and failure of ECIS and moderator cooling at four units simultaneously.
PDS4	Multiple steam generator tube rupture, failure of ECIS and moderator cooling.
PDS5	LOCA2 plus failure of ECIS, with the moderator providing a long term heat sink, and failure of containment isolation.
PDS6	Multiple steam generator tube rupture with failure of ECIS, with the moderator providing a long term heat sink.

Table 10: Darlington NGS Release Categorization Scheme

Release Category #	Description
D-RC1	Very large release with potential for acute offsite radiation effects and/or widespread contamination
D-RC2	Early release in excess of safety goal “Large Release” definition from Reference [R23].
D-RC3	Late release in excess of safety goal “Large Release” definition from Reference [R23].
D-RC4	Early release in excess of safety goal “Small Release” definition from Reference [R23].
D-RC5	Late release in excess of safety goal “Small Release” definition from Reference [R23].
D-RC6	Greater than normal containment leakage below Small Release limit.
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 11: Summary of DARA Severe Core Damage and Large Release Frequency Results for Internal Events

Model	Severe Core Damage Frequency (occurrences per reactor year)	Large Release Frequency (occurrences per reactor year)	Latent Effects (effects per station year)
Internal Events At-Power	7.9E-06	5.2E-06	1.0E-05
Internal Events At-Power – Enhanced Model	3.3E-06	1.3E-06	Not Required[1]
Internal Events At-Power – Enhanced Model with limited number of SIO[2]	2.1E-06	4.1E-07	3.8E-06
Internal Events Outage	8.8E-07	8.8E-07[3]	Not Required
OPG Safety Goal Target	1E-05	1E-06	1E-05
OPG Safety Goal Limit	1E-04	1E-05	1E-04

[1] Items denoted “Not Required” were not assessed as they are not required to support S-294 compliance.

[2] Includes four Safety Improvement Opportunities (SIOs) described in Section 8.1.

[3] LRF for internal outage events bounded by the frequency of SCD.

Table 12: Summary of DARA Severe Core Damage and Large Release Frequency Results for Fire, Seismic and Flooding Events

Model	Severe Core Damage Frequency (occurrences per reactor year)	Large Release Frequency (occurrences per reactor year)
Fire At-Power	1.9E-06	9.7E-08
Seismic At-Power[1]	3.7E-06	3.7E-06
Flooding At-Power	4.8E-07	<4.8E-07[2]

[1] Seimic results reported for events with a frequency of occurrence up to 1E-04/yr (recurrence interval of 10,000 years)

[2] LRF for at-power internal flooding was not assessed due to the low frequency of severe core damage. LRF is bounded by SCD frequency.

Table 13: DARA Level 1 At-Power Internal Events Fuel Damage Results

Fuel Damage Category	Baseline Predicted Frequency (/yr)	Enhanced Model with SIOs (/yr)	Enhanced Model without SIOs (/yr)
FDC1	1.4E-11	1.5E-11	1.5E-11
FDC2	7.9E-06	2.1E-06	3.3E-06
FDC3	1.8E-05	1.7E-05	1.8E-05
FDC4	1.7E-04	4.6E-05	1.4E-04
FDC5	1.3E-05	9.6E-06	9.6E-06
FDC6	2.0E-06	2.0E-06	2.0E-06
FDC7	2.8E-03	2.8E-03	2.8E-03
FDC8	4.6E-03	4.6E-03	4.6E-03
FDC9	2.6E-02	2.3E-02	2.3E-02
Severe Core Damage Frequency FDC1 + FDC2	7.9E-06	2.1E-06	3.3E-06

Table 14: 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)	8.8E-07	
	POS A	8.3E-09	2.6E-06
	POS B	1.2E-08	1.3E-06
	POS C	3.2E-08	1.6E-06
	POS D	8.2E-07	1.8E-04
	POS E	6.7E-09	2.4E-06
FDC5-SD	(all)	6.4E-06	
	POS A	2.0E-07	6.3E-05
	POS B	1.5E-06	1.5E-04
	POS C	4.6E-06	2.3E-04
	POS D	0.0E+00	0.0E+00
	POS E	9.0E-08	3.3E-05
FDC9-SD	(all)	3.0E-03	
	POS A	1.3E-04	4.0E-02
	POS B	8.4E-04	8.7E-02
	POS C	1.8E-03	9.0E-02
	POS D	2.2E-04	4.8E-02
	POS E	5.3E-05	1.9E-02
Severe Core Damage [Note 2]	(all)	8.8E-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 15: Plant Damage State Frequency

PDS	Predicted Frequency (/reactor-yr)
PDS1	1.5E-11
PDS2	1.7E-06
PDS2A	1.7E-06
PDS2B	1.9E-07
PDS2C	2.8E-07
PDS2D	2.1E-07
PDS2E	1.1E-07
PDS2F	2.8E-08
PDS2G	1.4E-08
PDS3	4.9E-06
PDS4	4.3E-07
PDS5*	2.9E-03
PDS6*	4.2E-05

*PDS5 and PDS6 sequences are limited core damage sequences.

Table 16: Release Category Frequency

Release Category	Baseline Predicted Frequency (/reactor-yr)	Enhanced Model with SIOs Predicted Frequency (/reactor-yr)	Enhanced Model without SIOs Predicted Frequency (/reactor-yr)
D-RC1	4.9E-06	5.1E-08	7.8E-07
D-RC2	3.7E-07	3.6E-07	5.2E-07
D-RC3	0	0	0
D-RC4	2.0E-09	5.7E-08	2.9E-07
D-RC5	NA*	NA*	NA*
D-RC6	NA*	NA*	NA*
D-RC7	1.5E-06	1.7E-06	2.4E-06
D-RC8	4.9E-06	~0	< 7.8E-07**

* No sequences were assigned to D-RC5 and D-RC6 in the Level 2 CET analysis.

** RC8 in the enhanced model is reported with a frequency being less than the frequency of RC1 because there are two-unit accident sequences (PDS3A) that contribute to RC1 which do not result in basemat melt-through. The severe accident simulations for two-unit accidents demonstrate that although core-concrete interaction occurs, it does not completely penetrate through the basemat.

Table 17: Individual Risk and Societal Risk - Late Countermeasures

Release[1] Category	Mean Frequency (/R-Yr)	Individual Dose[2] (Sv)	Population Dose (person-Sv)	Individual Risk (effect/R-Yr)	Societal Risk (effect/R-Yr)
D-RC1	4.9E-06	2.0E+01	5.5E+04	3.4E-06	1.6E-02
D-RC2	3.7E-07	4.1E-01	1.1E+03	1.3E-08	2.0E-05
D-RC4	2.0E-09	5.5E-01	9.6E+02	1.0E-10	9.7E-08
D-RC7	1.5E-06	4.3E-02	4.9E+01	3.4E-09	3.6E-06
PDS5	2.9E-03	6.2E-03	7.1E+00	9.0E-07	1.0E-03
PDS6	4.2E-05	6.6E-03	1.2E+01	1.4E-08	2.6E-05

[1] This table uses baseline numbers. For Enhanced DARA RC frequencies, see Table 16.

[2] At 1km from the point of release after accounting for long-term countermeasures

Table 18: Individual Risk at 1 km – Early and Late Countermeasures

Release[1] Category	Mean Frequency (/R-Yr)	Individual Dose[2] (Sv)	Population Dose (person-Sv)	Individual Risk (effect/R-Yr)	Societal Risk (effect/R-Yr)
D-RC1	4.9E-06	1.9E-02	4.8E+04	4.6E-09	1.3E-02
D-RC2	3.7E-07	4.6E-02	9.6E+02	8.6E-10	1.8E-05
D-RC4	2.0E-09	1.4E-02	7.3E+02	1.4E-12	7.2E-08
D-RC7	1.5E-06	4.1E-05	3.4E+01	3.0E-12	2.5E-06
PDS5	2.9E-03	1.6E-04	5.2E+00	2.2E-08	7.5E-04
PDS6	4.2E-05	4.5E-03	1.1E+01	9.6E-09	2.4E-05

[1] This table uses baseline numbers. For Enhanced DARA RC frequencies, see Table 16.

[2] At 1km from the point of release after accounting for early and long-term countermeasures

Table 19: Individual Risk and Societal Risk - Late Countermeasures (Enhanced DARA with SIO model)

Release Category	Mean Frequency (/R-Yr)	Individual Dose[a] (Sv)	Population Dose (person-Sv)[b]	Individual Risk (effect/R-Yr)	Societal Risk (effect/R-Yr)
D-RC1	5.1E-08	2.0E+01	6.0E+04	5.1E-08	1.5E-04
D-RC2	3.6E-07	4.1E-01	1.2E+03	7.4E-09	2.2E-05
D-RC4	5.7E-08	5.5E-01	1.1E+03	1.6E-09	3.2E-06
D-RC7	1.7E-06	5.7E-03[c]	5.4E+01	4.8E-10	4.6E-06
PDS5	2.8E-03	6.2E-03	7.9E+00	8.7E-07	1.1E-03
PDS6	2.4E-05	6.6E-03	1.3E+01	8.0E-09	1.6E-05

[a] At 1 km from the point of release after accounting for long-term countermeasures as provided for in provincial and federal emergency response plans.
[b] Projected 2013 population to a radius of 100km from the point of release.
[c] Calculated using variable wind direction.

Appendix A: Acronyms

Acronym	Definition
ACU	Air Conditioning Unit
ASDV	Atmospheric Steam Discharge Valve
BCA	Benefit-Cost Assessment
BWR	Boiling Water Reactor
CANDU	CANadian Deuterium Uranium
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 Risk Assessment
DARA-FIRE	Internal Fire Darlington Risk Assessment
DARA-FLOOD	Internal Flooding Darlington Risk Assessment
DARA-L1O	Level 1 Outage Internal Events Darlington Risk Assessment
DARA-L1P	Level 1 At-Power Internal Events Darlington Risk Assessment
DARA-L2P	Level 2 At-Power Internal Events Darlington Risk Assessment
DARA-L3P	Level 3 At-Power Internal Events Darlington Risk Assessment
DARA-SEISMIC	Seismic Darlington Risk Assessment
DBE	Design Basis Earthquake
DGSS	Drained Guaranteed Shutdown State
DNGS	Darlington Nuclear Generating Station
ECI	Emergency Coolant Injection
ECIS	Emergency Coolant Injection System
EFADS	Emergency Filtered Air Discharge System
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
FSA	Fire Safety Assessment

Acronym	Definition
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
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
MACCS	MELCOR Accident Consequence Code System
MCR	Main Control Room
MELCOR	Computer Code for Modelling Severe Accidents
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
PAL	Protective Action Level
PAU	Physical Analysis Unit
PAWCS	Post-Accident Water Cooling System
PDS	Plant Damage State
PK	Programmable Controller
POS	Plant Operational State
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor
PSVS	Powerhouse Steam Venting System
PULSW	Powerhouse Upper Level Service Water
PWR	Pressurized Water Reactor

Acronym	Definition
RC	Release Category
RCW	Recirculating Cooling Water
RRS	Reactor Regulating System
SCD	Severe Core Damage
SCDF	Severe Core Damage Frequency
SDC	Shutdown Cooling
SDS	Shutdown System
SEL	Seismic Equipment List
SGECS	Steam Generator Emergency Cooling System
SIO	Safety Improvement Opportunity
SMA	Seismic Margin Assessment
SNL	Sandia National Laboratories
SPRA	Seismic Probabilistic Risk Assessment
SR	Safety Report
SRV	Steam Relief Valve
SSC	Systems Structures and Components
THERP	Technique for Human Error Rate Prediction
USA	United States of America
USCA	Unit Secondary Control Area