Internal Events Level I PSA Accident Sequence Quantification For Point Lepreau Refurbishment Project

L. Comanescu, M. Wei, S. Sawh, A. Petrescu, G. Banaseanu, A. Nainer, R.K. Jaitly
Atomic Energy of Canada Limited, Mississauga, Ontario, Canada

D.S. Mullin, A.F. Jean, D.F. Basque
NB Power, New Brunswick, Canada

Abstract

A Probabilistic Safety Assessment (PSA) for Point Lepreau Generating Station is planned as part of the plant Refurbishment (PLR) Project. The main objective of this PSA is to provide insights into plant safety design and performance, including the identification of dominant risk contributors and the comparison of options for reducing risk.

A significant component of this PSA was recently completed, the Level I Accident Sequence Quantification (ASQ) for internal events (at full power and shutdown). The objective of Level I ASQ is to determine the overall Severe Core Damage Frequency (SCDF) that results from a system, structure or component failure or human error. This paper describes the major steps in performing Level I ASQ for internal events and discusses the key results of this study. The results presented in this paper are interim as this study has not completed the formal review process.

1. Introduction

The purpose of this ASQ is to estimate the overall Severe Core Damage Frequency (SCDF) as well as the frequency of other plant damage states that result from Level 1 internal events. Level I internal events includes an analysis of plant design and operation with emphasis on the accident sequences that lead to core damage, their basic causes and their frequencies. External events such as fire, floods and earthquakes, are not a part of this analysis. Furthermore, Level I ASQ does not investigate the frequency or mode of containment failure of the consequences of radionuclide releases, which are a part of Level II PSA.

2. Accident Sequence Quantification Inputs

In order to estimate the SCDF, all accident sequences are quantified. Accident sequences are developed using event tree logic and each accident sequence represents a unique series of successes and/or failures of mitigating systems and operator actions following an initiating event. The initiating event frequencies were derived using three different methodologies: a statistical calculation based on site specific operating experience and domestic CANDU® plants; pipe calculation data; or fault tree analysis. For the PLR PSA, event trees were developed for 68 of the 82 initiating events. From these event trees, approximately 3985

accident sequences were developed. The termination of each accident sequence is categorized by plant damage states according to Table 1.

Table 1 - Plant Damage States

PDS	Definition	Type of Accident
0	Early (Rapid) Loss of Core Structural Integrity	Severe Core Damage
1	Late Loss of Core Structural Integrity with High PHT Pressure	Severe Core Damage
2	Late Loss of Core Structural Integrity with Loss PHT Pressure	Severe Core Damage
3	LOCA + LOECC with Moderator Required within Fifteen (15) Minutes	Widespread Fuel Damage
4	LOCA + LOECC with Moderator Required after Fifteen (15) Minutes	Widespread Fuel Damage
5	Large LOCA with Early Flow Stagnation	Limited Fuel Damage
6	Single Channel LOCA with Containment Overpressure	Limited Fuel Damage
7	Single Channel LOCA with No Containment Overpressure (In-Core LOCA)	Limited Fuel Damage
8	Loss of Cooling to Fuelling Machine	Limited Fuel Damage
9	LOCA with No Significant Fuel Failures	No Significant Fuel Damage
10	Deuterium Deflagration (D_2 > 4%) in Cover Gas and/or Release of Moderator into Containment (Fuel Cooling is Maintained)	

An accident sequence is represented by fault tree logic encompassing models for the mitigating and support systems that were credited for this ASQ. In order to develop accident sequence fault tree logic, it is necessary to merge the separate fault trees produced over the course of PLR PSA into a single Master Fault Tree. The list of all FTs that were merged for ASQ are shown in Table 2. In addition, support systems were linked to the mitigating system fault trees. Figure 1 summarizes the creation of the Master Fault Tree.

Table 2 – Fault Tree Systems

Mitigating Systems	
Boiler Feedwater (BFW)	SDS1 & SDS2
Boiler Pressure Control (BPC)	Shutdown Cooling (SDC)
Emergency Core Cooling (ECC)	Secondary Side Pipe Leak Detection (SSPLD)
End Shield Cooling (ESC)	Turbine Protection System (TPS)
Fuelling Handling (FH)	Setback & Stepback
Emergency Water System (EWS)	Turbine Relief Panel (TBRP)
Moderator (MOD)	Emergency Power System
Pressure Inventory and Control (PIC)	Steam Generators Blowdown System
Support Systems	
Electrical Distribution System (EDS)	Service Water System (SWS)
Instrument Air System (IAS)	

Data for each component failure rate is mostly generated based on plant specific operating experience of PLGS, or where there is not enough experience, external data is used. Each fault tree undergoes human reliability and common cause failure analysis. The human error

probabilities (HEPs) modeled in the system fault trees and event trees are assessed covering both pre-accident and post-accident operator errors. The Common Cause Failures (CCF) for redundant components are assessed using Unified Partial Method (UPM) [1]. The CCF events are added to the fault tree to reflect the failure dependency of the components in the group.

Modularisation was performed on modelled systems that are large in size, prior to being merged within the Master Fault Tree, in an effort to reduce the number of cutsets and the time required to evaluate the models. Modularisation is the process of collapsing independent primary events, which cause similar losses of system function, into a single event.

As a result of the support functions being integrated with the mitigation functions under a single master fault tree, circular logic was commonly encountered. For example, EDS includes the Class III Standby Generators, which require cooling from SWS. As well, SWS requires IA for the functionality of some pneumatic valves. The following general guidelines were developed in order to cater to these situations: The EDS branch of a fault tree will be permitted to feed within a branch of IA or a branch of SWS, however an IA branch or an SWS branch will not be permitted to feed within an EDS branch, thereby preventing a circular logic loop.

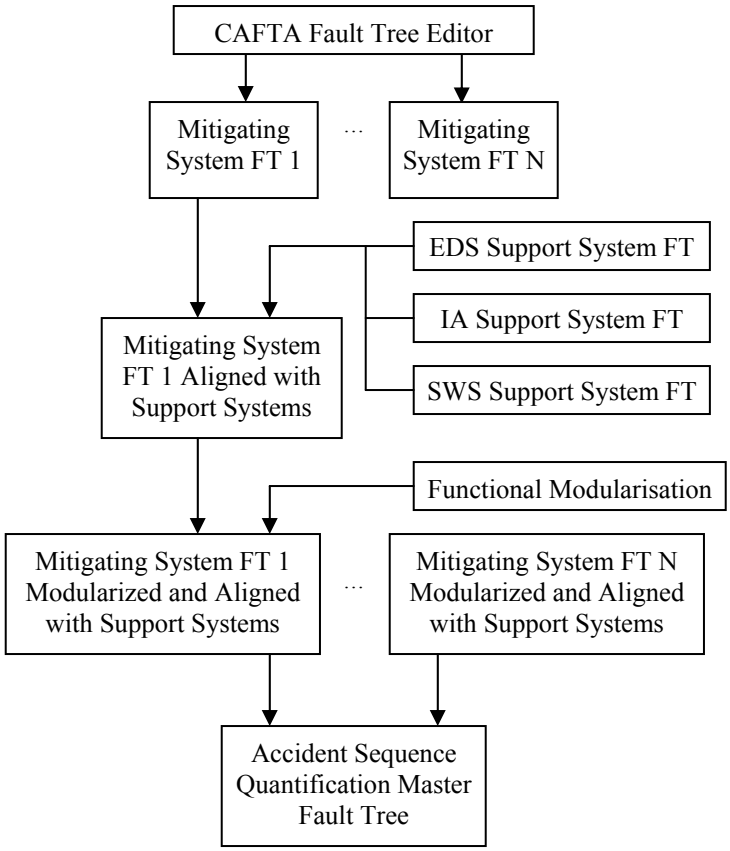


Figure 1 - Flowchart for the creation of the Master Fault Tree

After merging, the Master Fault Tree consists of 635 top events and a single database containing 32408 basic events. It is the only FT used during the ASQ phase, and is associated with every event tree during quantification.

3. Accident Sequence Quantification

The computer code PRAQuant 4.0a generates the fault tree logic to represent the accident sequences using the Master Fault Tree and the event trees as inputs. FORTE was used as the primary quantification engine but was found to be very memory intensive thus limited in its ability to solve all sequences. For the sequences in which FORTE encountered memory limitations, the FTREX quantification engine was used. Mutually exclusive events are removed from the resulting cutsets, followed by the application of recovery factors using QRecover. Figure 2 below is a flowchart outlining the steps of ASQ.

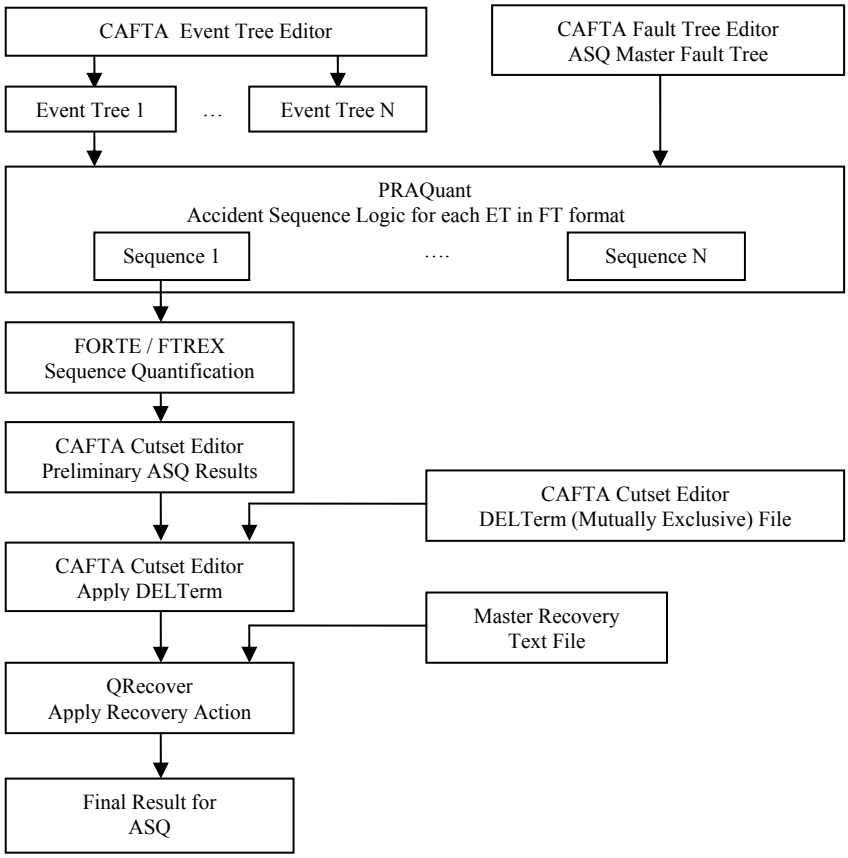


Figure 2 - ASQ Computer Codes and Functions

As seen in the figure above, the results obtained after applying recovery are the final results that provide a realistic estimate of the plant damage frequency. There are various types of recovery factors that were credited. If a common cause failure (CCF) is found to be a dominant contributor to Severe Core Damage, the CCF, previously calculated using the Unified Partial Method, is reviewed for conservatism or recalculated via the Alpha factor

methodology [2] using the latest alpha factor distribution presented in the 2003 USNRC database [3]. Sequences that include more than one human action are required to be re-evaluated in order to account for the dependencies between the operators and their location. The methodology used for this re-quantification is based on the SPAR-H method (Standardized Plant Analysis Risk Human Reliability Analysis) [4] and the new value is incorporated within the overall PSA result as a recovery action. In addition, if an operator action is found to be a dominant contributor to Severe Core Damage, the operator action, previously calculated using the Accident Sequence Evaluation Program Human Reliability Analysis Procedure (ASEP) [5], is recalculated using Technique for Human Error Rate Prediction (THERP) methodology, as per [6]. Recovery actions taken by the operator to recover from a sequence of events can also be identified and credited. The results obtained after applying recovery are the final results that provide a realistic estimate of the plant damage frequency.

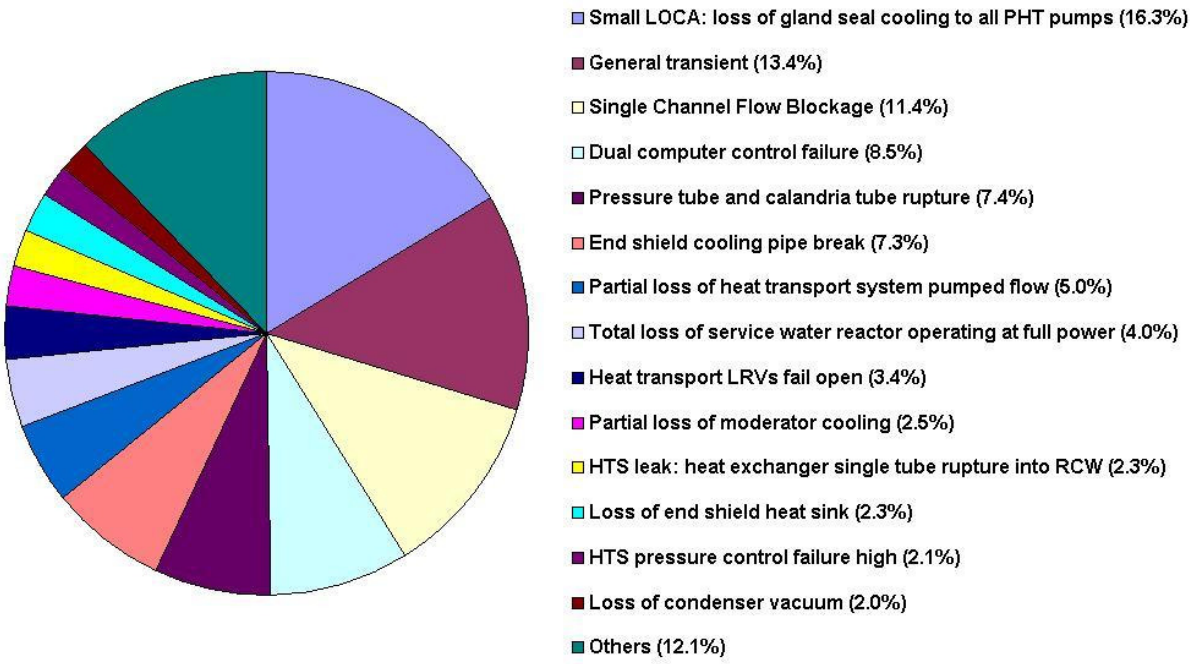
4. Accident Sequence Quantification Results

Severe core damage accidents are beyond-design-basis accidents in which a rapid or late loss of the structural integrity of the reactor core occurs. Severe core damage accidents are characterized by plant damage states PDS0, PDS1 and PDS2. A loss of core structural integrity results from a loss of heat sinks leading to core damage involving multiple fuel channels failures and core disassembly. The core structure is defined as the calandria/end shield assembly. Widespread fuel damage accidents are design basis accidents in which core structural integrity is maintained and are characterized by plant damage states PDS3 and PDS4. For widespread fuel damage accidents, the fuel heat is not removed by coolant flow in the Heat Transport System and the moderator is the heat sink.

In order to estimate a Severe Core Damage Frequency (SCDF), the accident sequences leading to PDS0, PDS1 and PDS2 are summed together. The frequency for severe core damage for Level I internal events during full power operation and shutdown is 2.10E-05 events/year. The SCDF during full power operation is 1.19E-05 events/year and the SCDF during shutdown is 9.16E-06 events/year.

Each accident sequence that contributes to the SCDF can be grouped according to the initiating event from which the sequence propagated. As a result, the initiating events that dominate the severe core damage frequency during full power operation for internal events are shown in Figure 2. The six most dominant initiators during full power operation are Loss of Gland Seal Cooling to PHT Pumps (LOCA2.2), General Transient (GENT), Single Channel Fuel Blockage (LOFA2.1), Dual Computer Control Failure (DCC), Pressure Tube and Calandria Tube Rupture (LOCA2.6), and End Shield Cooling Pipe Break (END1.3). Together, the accident sequences following these initiating events account for 64% of the SCDF at full power.

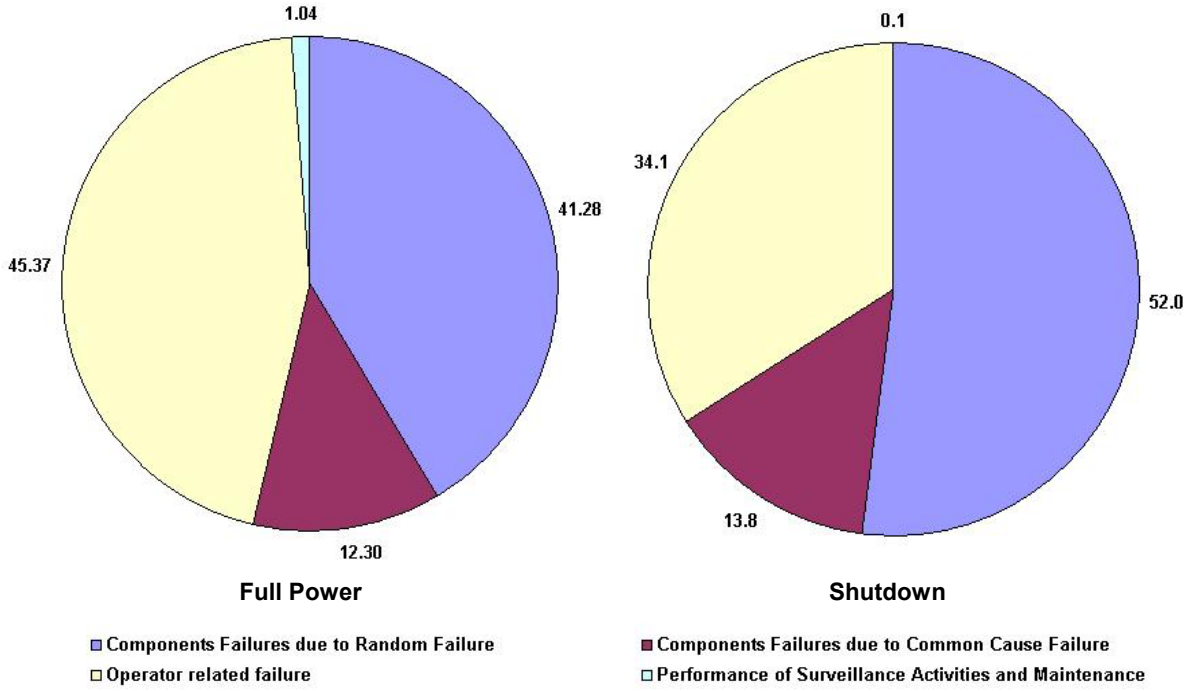
Figure 2 - Initiator Distribution of SCD during Full Power Operation



The most dominant initiator during shutdown is Shutdown LOCA: HTS pipe leaks with HTS full and depressurised (SDLOCA1.1), followed by Total loss of Class IV power with reactor shutdown, HTS cold depressurised and drained to the header level (XEL4.3). The accident sequences following the SDLOCA1.1 initiating event accounts for 97.5% of the SCDF during shutdown while XEL4.3 accounts for 1.8%.

The Basic Event Importance Measure Report with Risk Reduction Worth is performed for the SCD cutsets. The conditioning events are not considered in the risk reduction worth analysis and in the following discussion. The remaining events, other than initiators are categorized in the following main grouping categories: component failures due to random failures, component failures due to common cause failures, operator related failures, and performance of surveillance activities and maintenance resulting in a degradation of a mitigation function. Figure 3 shows the mitigation main contributors to SCD according to the four groups for full power and shutdown. The two main contribution groups, accounting for over 80% of both full power and shutdown operation are random component failures and operator related failures.

Figure 3 - Main Contribution Groups to Full Power and Shutdown SCD



5. Summary

A summary of the plant damage state frequencies estimated from this ASQ is provided in Table 3 and Table 4. The total severe core damage frequency for internal events full power and shutdown is under the proposed risk limit of 1E-04/y [7] for severe core damage frequency and is in line with the international results for the refurbished plants.

Table 3 - Summary of Plant Damage State Frequencies

Plant Damage State	Frequency Total	Frequency at Power	Frequency Shutdown
PDS0	1.66E-07	8.31E-08	8.25E-08
PDS1	5.34E-07	5.34E-07	0
PDS2	2.03E-05	1.12E-05	9.07E-06
PDS3	1.72E-05	1.72E-05	0
PDS4	4.34E-05	2.73E-05	1.61E-05
PDS5	1.02E-05	1.02E-05	0
PDS6	2.50E-04	2.50E-04	0
PDS7	7.38E-04	7.38E-04	0
PDS8	0	0	0
PDS9	3.08E-02	3.05E-02	3.19E-04
PDS10	1.31E-05	1.31E-05	0
NDF	1.23E-07	1.23E-07	0

Table 4 - Summary of Reporting Category Frequencies

Plant Damage Category	Frequency
SCDF Total (PDS0 + PDS1 + PDS2)	2.10E-05
SCDF at Power (PDS0 + PDS1 + PDS2)	1.18E-05
SCDF Shutdown (PDS0 + PDS1 + PDS2)	9.16E-06
Early SCDF Total (PDS0)	1.66E-07
Early SCDF at Power (PDS0)	8.31E-08
Early SCDF Shutdown (PDS0)	8.25E-08
Late SCDF Total (PDS1 + PDS2)	2.08E-05
Late SCDF at Power (PDS1 + PDS2)	1.17E-05
Late SCDF Shutdown (PDS1 + PDS2)	9.07E-06
Widespread Fuel Damage Frequency Total (PDS3 + PDS4)	6.06E-05
Widespread Fuel Damage Frequency at Power (PDS3 + PDS4)	4.45E-05
Widespread Fuel Damage Frequency Shutdown (PDS3 + PDS4)	1.61E-05

5. References

[1] UPM 3.1: A Pragmatic Approach to Dependent Failures Assessment for Standard Systems, SRDA-R13, SRD Association, AEA Technology PLC, Cheshire, UK, 1996.

[2] U.S. NRC, CCF Parameter Estimations, 2003 Update, http://nrcoe.inl.gov/results/CCF/ParamEst2003/ccfparamest.htm, 2006 May (accessed May 2007).

[3] U.S. NRC, Reliability Study: Babcock & Wilcox Reactor Protection System, 1984-1998, NUREG/CR-5500, 2001 November.

[4] U.S. NRC, The SPAR-H Human Reliability Analysis Method, NUREG/CR-6883, 2005 August.

[5] U.S. NRC, Accident Sequence Evaluation Program Human Reliability Analysis Procedure, NUREG/CR-4772, 1987 February.

[6] U.S. NRC, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, 1983 August.

[7] IAEA, Basic Safety Principles for Nuclear Power Plants, Safety Series Document No. 75-INSAG 3, 1988.