



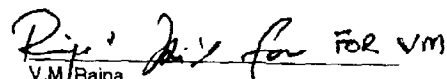
Assessment Document

Design Assist Role of ACR Probabilistic Safety Assessment (PSA)


ACR

108-03660-ASD-008
Revision 0

Prepared by
Rédigé par


V.M. Raina
VMR Consulting Inc.

Reviewed by
Examiné par


P. Santamura
ACR PSA and Safety Design

Approved by
Approuvé par


R.K. Jaitly, Manager
ACR PSA and Safety Design

Approved by
Approuvé par


M. Bonechi, Manager
ACR Safety Engineering

2004 February

Février 2004

CONTROLLED -
Licensing

CONTRÔLÉ -
Permis

© Atomic Energy of
Canada Limited

© Énergie atomique du
Canada limitée

2251 Speakman Drive
Mississauga, Ontario
Canada L5K 1B2

2251, rue Speakman
Mississauga (Ontario)
Canada L5K 1B2



Assessment Document

Design Assist Role of ACR Probabilistic Safety Assessment (PSA)

ACR

108-03660-ASD-008
Revision 0

2004 February

Février 2004

**CONTROLLED -
Licensing**

**CONTRÔLÉ -
Permis**

This document and the information contained in it is made available for licensing review. All rights reserved by Atomic Energy of Canada Limited. No part of this document may be reproduced or transmitted in any form or by any means, including photocopying and recording, without the written permission of the copyright holder, application for which should be addressed to Atomic Energy of Canada Limited. Such written permission must also be obtained before any part of this document is stored in a retrieval system of any nature.

Le présent document et l'information qu'il contient sont disponibles pour examen en vue de l'obtention des permis. Tous droits réservés par Énergie atomique du Canada limitée. Il est interdit de reproduire ou de transmettre, par quelque procédé que ce soit, y compris de photocopier ou d'enregistrer, toute partie du présent document, sans une autorisation écrite du propriétaire du copyright obtenue auprès d'Énergie atomique du Canada limitée. De plus, on doit obtenir une telle autorisation avant qu'une partie du présent document ne soit intégrée dans un système de recherche documentaire de quelque nature que ce soit.

© Atomic Energy of
Canada Limited

© Énergie atomique du
Canada limitée

2251 Speakman Drive
Mississauga, Ontario
Canada L5K 1B2

2251, rue Speakman
Mississauga (Ontario)
Canada L5K 1B2



Release and Revision History

Liste des documents et des révisions

0939B Rev. 13

Document Details / Détails sur le document

Title
Titre

Total no. of pages
N^{bre} total de pages

Design Assist Role of ACR Probabilistic Safety Assessment (PSA)

CONTROLLED – Licensing / CONTRÔLÉ – Permis

Release and Revision History / Liste des documents et des révisions

Release Document		Revision Révision		Purpose of Release; Details of Rev./Amendement Objet du document; détails des rév. ou des modif.	Prepared by Rédigé par	Reviewed by Examiné par	Approved by Approuvé par
No./N ^o	Date	No./N ^o	Date				
1		D1	2004/02/09	Issued for Review and Comment.	V.M. Raina	P. Santamaura V.G. Snell V. Langman K. Hau A. Josefowicz L. Comanescu P. Iliescu	R.K. Jaitly
2		0	2004/02/27	Issued as “Approved for Use.” This document replaces 108-00580-ASD-009.	V.M. Raina	P. Santamaura	R.K. Jaitly M. Bonechi

DCS/RMS Input / Données SCD ou SGD

Rel. Proj. Proj. conn.	Project Projet	SI	Section	Serial Série	No. N ^o	Sheet Feuille	Of De	Unit No.(s) Tranche n ^o
	108		ASD	008		1	1	

ABSTRACT

This report addresses the application of the Probabilistic Safety Assessment (PSA) discipline to the design of the Advanced CANDU Reactor™ (ACR™)*. It first discusses the influence of risk concepts and techniques on the evolution of CANDU®** reactor safety design over the years. The insights and lessons learned from a number of previous CANDU risk-based assessments are presented. Enhanced safety design features of the proposed ACR are discussed in the light of these assessments.

The report also reviews the scope of the ACR PSA, highlighting the “design assist” role of the PSA in developing the detailed design of the ACR. It concludes with a review of the preliminary PSA analyses completed to date and a discussion of how they are being utilized in the detailed design and licensing of the ACR.

* ACR™ (Advanced CANDU Reactor™) is a trademark of Atomic Energy of Canada Limited (AECL).

** CANDU® (CANada Deuterium Uranium®) is a registered trademark of Atomic Energy of Canada Limited (AECL).

ACRONYMS

ACND	Auxiliary Condensate Extraction (system)
ACR	Advanced CANDU Reactor
ACU	Air Cooling Unit
AECB	Atomic Energy Control Board
AECL	Atomic Energy of Canada Ltd.
AFW	Auxiliary Feed Water (subsystem)
AFW-IS	Auxiliary Feed Water – Isolation (failure)
ALWR	Advanced Light Water Reactor
ASDV	Atmospheric Steam Discharge Valve
ADW	Auto De-pressurization Water (function)
ASEP	Accident Sequence Evaluation Program (Human Reliability Analysis Procedure)
BBRA	Bruce B Risk Assessment
BCLCV	Bleed Condenser Level Control Valve
BPCC	Boiler Pressure Control Cool-down (subsystem)
CAFTA	Computer Aided Fault Tree Analysis
CANDU	CANada Deuterium Uranium
CC	Crash Cool-down (of steam generators)
CCF	Common Cause Failure
CCW	Condenser Cooling Water
CDF	Core Damage Frequency
CDS	Core Damage State
CL4	No Consequential loss of class IV electrical power supply
CLPRV	Consequential LOCA via Pressure Relief Valves
CLPS	Consequential LOCA via pump seals
CND	Condensate (system)
CNSC	Canadian Nuclear Safety Commission
CSDV	Condenser Steam Dump Valve
D1SW	Division I Service Water
DCC	Digital Control Computer
DECC	Dormant Emergency (Core) Cooling (injection system - this is an obsolete term for ECI system)
DG	Diesel Generator

DG-AV=1	1 Diesel Generator Set Available
DG-AV=2	2 Diesel Generator Set Available
DG-AV=3	3 Diesel Generator Set Available
DG-AV=4	4 Diesel Generator Set Available
DPSE	Darlington Probabilistic Safety Evaluation
ECC	Emergency Core Cooling (function; carried out by the ECI and LTC systems)
ECI	Emergency Coolant Injection (system)
ECR	Emergency Coolant Recovery
EFW	Emergency Feed Water (supply from RWS to SG)
EOOS	Equipment Out OF Service
EOP	Emergency Operating Procedures
EPRC	Ex-Plant Release Category
EPRI	Electric Power Research Institute
EQ	Environmental Qualification
ET	Event Tree
FADS	Filtered Air Discharge System
FBIO	Feeder Break
FDC	Fuel Damage Category
FSB	Feeder Stagnation Break
FW	Feed Water systems (includes MFW and AFW subsystems)
FWBA	Asymmetric feed water line break downstream of the SG check valve
FWBS	Symmetric feed water line break upstream of the feed water LCVs
GPSA	Generic Probabilistic Safety Assessment
HEP	Human Error Probability
HT(S)	Heat Transport (System) (equivalent to Reactor Coolant System (RCS) in LWRs)
HX	Heat Exchanger
IE	Initiating Event
IE-FB	Initiating Event Feeder Break
IE-FSB	Initiating Event Feeder Stagnation Break
IE-FWBA	Initiating Event Asymmetric feed water line break downstream of the SG check valve
IE-FWBS	Initiating Event Symmetric Feed Water Line Break Upstream of the Feed Water LCVs
IE-LCL4	Initiating Event Total Loss of Class IV Power Supply

IE-LOR	Initiating Event Loss of Regulation
IE-MSL3	Initiating Event Small Steam Discharge Causing Low Level in the Deaerator
IE-PCTR	Initiating Event Small LOCA - Pressure Tube & Calandria Tube Rupture
IE-PTR	Initiating Event Small LOCA - Pressure Tube Rupture
IE-SCB	Initiating Event Loss of Inventory in the Shield Cooling System
IE-SWD2	Initiating Event Total Loss of one Service Water Division (Division #2)
ISSAAC	Integrated Severe Accident Analysis Code for CANDU
KEMA	N.V. Tot Keuring van Elektrotechnische Materialen in Arnhem
KIRAP	KAERI Integrated Reliability Analysis Code Package
LCV	Level Control Valve
LOCA	Loss of Coolant Accident
LOECC	Loss of Emergency Core Cooling
LOR	Loss of Regulation
LRF	Large Release Frequency
LRV	Liquid Relief Valve
LTC	Long Term Cooling (system)
LTC-ECC	Long Term Cooling system - Emergency Core Cooling function
LTC-SDC	Long Term Cooling system - Shutdown Cooling function
LWR	Light Water Reactor
MAAP	Modular Accident Analysis Program
MCR	Main Control Room
MFW	Main Feed Water (subsystem)
MHS	Moderator (system) acting as active Heat Sink (does not include passive heat sink using water make-up from RWS)
MSL3	Small Steam Line Break – causing Low Deaerator Level
MSSV	Main Steam Safety Valve
NPD	Nuclear Power Demonstration
NPSH	Net Positive Suction Head
NRX	National Research Experimental (natural-uranium, heavy-water-moderated research reactor)
PARA	Pickering A Risk Assessment
PCTR	Pressure Tube / Calandria Tube Rupture
PDS	Plant Damage State
PSA	Probabilistic Safety Assessment

PTHT	Heat transport Pumps Trip on High upper bearing Temperature
PTR	Pressure Tube Rupture
PRA	Probabilistic Risk Assessment
PWR	Pressurized Water Demonstration
RB	Reactor Building
RCS	Reactor Coolant System (the Canadian terminology uses the Heat Transport System)
RCW	Recirculated Cooling Water
RIH	Reactor Inlet Header
RRS	Reactor Regulating System
RS	Reactor Shutdown
RSC	Royal Society of Canada
RSW	Raw Service Water
RWS	Reserve Water System
RWS-HTS	water makeup from Reserve Water System into the Heat Transport System
RWT	Reserve Water Tank (a component of RWS)
SCB	Shield Cooling Break
SCDF	Severe Core Damage Frequency
SDM	Safety Design Matrix
SDS1	Shutdown System #1
SDS2	Shutdown System #2
SG	Steam Generator
SGPR	Steam Generator Pressure Relief (system; includes ASDVs, CSDVs and MSSVs)
SSC	Systems, Structures and Components
SWD1&D2	Service Water (system) Division 1 & Division 2
TBD	To Be Determined
UPM	Unified Partial Method
USNRC	United States Nuclear Regulatory Commission

Note: The notations 1.0E-y and 1×10^{-y} are interchangeably used.

TABLE OF CONTENTS

SECTION	PAGE
1.	INTRODUCTION..... 1-1
2.	HISTORICAL REVIEW..... 2-1
2.1	Early Developments 2-1
2.2	The Siting Guide 2-2
2.3	Reliability Targets for Process Systems..... 2-3
2.4	System Reliability Assessments at Ontario Hydro 2-4
2.5	Safety Design Matrices 2-4
2.6	CANDU Reactor PRAs 2-5
2.6.1	Darlington Probabilistic Safety Evaluation (DPSE) 2-5
2.6.2	AECL/KEMA CANDU 6 PSA Study..... 2-7
2.6.3	Pickering A Risk Assessment (PARA) 2-8
2.6.4	AECL's Wolsong 2/3/4 PSA 2-10
2.6.5	Extension of Wolsong 2/3/4 PSA in South Korea 2-11
2.6.6	Bruce B Risk Assessment (BBRA) 2-11
2.6.7	CANDU 9 PSA 2-13
2.6.8	Generic PSA Program at AECL..... 2-14
2.7	Lessons from Risk-based Assessments 2-15
3.	ADVANCED CANDU REACTOR 3-1
3.1	ACR Design Features..... 3-1
4.	ACR PSA 4-1
4.1	PSA Objectives 4-1
4.2	Preliminary Event Tree (ET) Analysis..... 4-2
4.2.1	Selected Initiating Events..... 4-3
4.2.2	Event Tree End States 4-4
4.2.3	Operator Actions 4-4
4.2.4	System Reliability Targets 4-5
4.2.5	Sample ET Analysis (Feeder Break)..... 4-5
4.2.6	Results of Preliminary Event Tree Analysis 4-6
4.2.7	Role of Reserve Water System..... 4-7
4.2.8	Key PSA Assumptions..... 4-7
4.3	Fault Tree Analysis of Emergency Feedwater Supply..... 4-8
4.4	Early Contributions of PSA to ACR Plant Design..... 4-8
4.5	PSA Quality Assurance..... 4-9
5.	CONCLUSION..... 5-1
6.	REFERENCES..... 6-1

TABLE OF CONTENTS

SECTION **PAGE**

TABLES

Table A-1 Initiating Events for Preliminary Event Tree Analysis A-1
Table A-2 Plant Damage States..... A-2
Table A-3 System Reliability /Unavailability Targets (dependent on DG availability) A-4
Table A-4 System Reliability/Unavailability Targets A-5

APPENDICES

Appendix A Preliminary Event Tree Analysis A-1
Appendix B Event Tree for Feeder Break B-1

1. INTRODUCTION

Risk concepts have been utilized in the safety design of the CANDU reactor from its very inception as a potential source of electrical power. Risk-based methods have been used by the designer, the operator, and the Canadian regulator of CANDU reactors. Underlying the use of these methods has been the motivation to better understand the significance of safety issues, identify potential design deficiencies, and effect improvements in reactor safety.

In this report, we first review the history of the application of risk assessment techniques in the Canadian nuclear industry, particularly those called Probabilistic Risk Assessment (PRA) or Probabilistic Safety Assessment (PSA^{*}). The use of PSA in the design of the latest CANDU, the Advanced CANDU Reactor (ACR), is then described. The outputs of the preliminary PSA for the ACR design are reviewed and the manner in which they are being used to finalize the detailed design is discussed.

* The terms PRA and PSA are used interchangeably in this report.

2. HISTORICAL REVIEW

2.1 Early Developments

It was explicitly recognized early in the development of the Canadian nuclear power program that nuclear plants needed to be built to higher levels of safety than conventional plants given their potential to adversely impact public health in a unique way, viz., the inadvertent release of radioactivity. Attempts were made to express the required safety in quantitative terms. In 1957, a numerical frequency of 10^{-5} per year [1] was recommended as a limit on the likelihood of a nuclear accident that might result in significant public health impacts. The underlying basis of this recommendation was the assumption that such an accident should be a factor of five less likely than loss of life due to other forms of electricity production such as coal-fired plants. This figure was used to derive reliability requirements for control and safety systems, which were then utilized to guide the design of the 20 MWe Nuclear Power Demonstration (NPD) reactor placed in operation in 1962. While it was recognized that it would be difficult to demonstrate quantitatively that the risk-based target was met, the existence of such a target was, nevertheless, thought to be useful even if only addressed qualitatively.

Further application of the risk approach occurred in the licensing of the next power reactor design, viz. the 200 MWe Douglas Point reactor [2]. The licensing approach adopted was one of the prospective licensee identifying to the regulatory authority, Atomic Energy Control Board (AECB^{*}), various accident scenarios and estimating both the radioactivity release and the frequency of the scenario. Probability estimates were based, as much as possible, on component reliability data from fossil plants and the nuclear laboratories. It was conceded, however, that in many cases these were based on judgment due to lack of actuarial data.

Prior to the design of the NPD and Douglas point reactors important risk management insights were obtained from the accident at AECL's NRX reactor in Chalk River, Ontario. This accident taught the Canadian nuclear community some fundamental design and operational lessons, which are now firmly embedded in CANDU reactor design and operation. In summary, these were: the importance of keeping safety systems as separate as possible from normal process systems, and ensuring the safety systems had the required reliability.

* The AECB is now called the Canadian Nuclear Safety Commission (CNSC).

2.2 The Siting Guide

With the prospect of larger power reactors on the horizon in the sixties, the AECB developed rules for the licensing of power reactors, known as the Siting Guide and applied first to Ontario Hydro's (now Ontario Power Generation's) Pickering A reactor situated close to the city of Toronto, a major population center. Mindful of the difficulty of demonstrating that a proposed reactor design met an overall risk target, due to uncertainties in completeness of accident scenarios and failure data, the Siting Guide established lower-tiered risk targets, more amenable to verification, as well as codified the risk insights from earlier experience. Specifically, it categorized plant systems as being either “process systems”, i.e., those required for power production, “protective systems”, i.e., those required to mitigate failures of process systems, or part of containment [4]. Safety is then assured by limiting the

- Frequency of occurrence of process system failures,
- Unreliability of the protective and containment systems, defined as the fraction of time the system is unable to perform its function, and
- Consequences of process system failures, and combinations of process and protective/containment systems failures.

Further, the Siting Guide required the process and protective/containment systems to be sufficiently independent of each other. A frequency limit of 1 in 3 years for process failures, and an unreliability limit of $10^{-2.5}$ (3×10^{-3}) per year for each of protective and containment systems was established, leading to an overall accident frequency limit of less than 10^{-5} per year.

Later, the above classification was simplified such that a nuclear plant was divided into two groupings of systems, process and safety, for safety evaluation purposes [3], and the target reliabilities of safety systems were made more stringent (unavailability $< 10^{-3}$). The effectiveness of safety systems was required to be such that for any (single) serious process failure requiring safety system action, the exposure of any individual of the population would not exceed 500 milli-rem and of the population at risk 10^4 person-rem. Further, for any postulated combination of a process failure and failure of a safety system, the predicted dose to any individual was not to exceed 25 rem whole body, 250 rem thyroid, and to the population 10^6 person-rem. These came to be called the single failure / dual failure criteria of reactor licensing.

Even though the criteria did not require a quantitative assessment of public risk, their risk roots are unmistakable. These criteria have had a profound effect on Canadian reactor safety practices. By placing explicit unavailability limits on safety systems, they led to detailed reliability modeling and monitoring of such systems. Many safety improvements resulted from such studies in both system design and operation. Further, by requiring the consequences of dual failures to have pre-defined limits, they resulted in design provisions to cater to severe accidents. Striking examples of these provisions are the second shutdown system in post-Pickering A reactors, and measures to ensure the ability of the moderator to maintain fuel channel integrity following the combined loss of coolant and emergency core cooling failure.

2.3 Reliability Targets for Process Systems

The frequency limit on process system failures was large enough that it could easily be determined if it was met in practice. In reality, however, a process system failure rate of 1 in 3 years could not be tolerated due to the high economic cost of the associated reactor shutdown and repair. In fact, designers established their own targets for some of the serious process system failures requiring special safety system action, such as a loss of reactor power regulation (LOR) and loss of coolant (LOCA). For example, for both LORs and small LOCAs a frequency limit of 1 in 100 reactor-years was selected, on the basis that such events should be precluded from occurring during the operating life of a 4-unit generating station.

It is instructive to review how these frequency targets were used in practice. Early operating experience at Pickering A indicated the self-imposed frequency of 1 in 100 reactor-years might not be met. As a result, a comprehensive examination of the reliability of the Pickering A reactor regulating system was undertaken in 1975 by a joint Ontario Hydro - AECL team of engineers, called the Pickering A Loss of Regulation (LOR) Study. The Pickering A LOR Study was one of the first applications in the Canadian nuclear industry of the developing field of reliability modeling of complex systems using the fault tree analysis technique. Fault trees were drawn for the various system failures that could contribute to a loss of regulation event, such as the inadvertent draining of the liquid zone compartments, failures of the in-core detectors, ion chambers and thermal power measurements to correctly sense reactor power, failures of the digital control computer leading to reactivity control devices being directed to introduce positive reactivity into the core, and so forth. The study also evaluated the human-machine interface and quantified the operator actions that could contribute to a loss of reactor control. It enabled expertise to be developed in Ontario Hydro in Probabilistic safety assessment technology, which was subsequently utilized in Ontario Hydro's PRA studies.

A number of recommendations came out of the Pickering A LOR Study, most of which were implemented.

Following the conduct of the Pickering A LOR study a similar assessment was undertaken for the Bruce A reactor regulating system and issued in 1979. Again, a number of recommendations were made to improve the system's reliability.

A key insight from the LOR studies related to the use of the dual digital control computer (DCC) configuration. To obtain the full benefits of redundancy, an extensive and thorough self-checking system was required on each computer, with rapid transfer of control to the standby computer via a watchdog timer if a malfunction was detected. Further, the self-checking mechanisms needed to be distinct from the checked device so that defensive actions could be reliably taken. Improvements were made to the self-checking features of the existing reactors, as well as the newer designs of Pickering B and Bruce B, and the 600 MWe units, such as allocation of redundant check inputs on different analog and digital input/output circuit boards.

Likewise, this aspect of the dual computer design was the focus of scrutiny during the course of the DCC replacement project at one of Ontario Hydro's stations, undertaken to replace the original, antiquated computers by hardware emulators based on modern technology [16]. A fault tree assessment during the design phase of the computer replacement project identified malfunctions of interval timers that would not only have led to the controlling computer sending out wrong signals, but also caused the computer's watch dog timer to fail to detect the fault.

Changes were made to the watchdog timer design to prevent such an eventuality. Very few LOR events have been experienced since the eighties. Those that have occurred have identified further possibilities for improving the self-checking features.

2.4 System Reliability Assessments at Ontario Hydro

In the mid-seventies, Ontario Hydro embarked upon an ambitious nuclear power program, which saw the commitment to build additional 4-unit CANDU stations at Pickering and Bruce and a new one at Darlington. A significant portion of the design work for these stations was carried out in-house by Ontario Hydro's Design and Construction Branch. Reliability assessments, typically using the fault tree technique, were an integral part of this design effort, carried out by the key design disciplines of Nuclear, Mechanical, Electrical, and Instrumentation & Control on their respective systems in both the conceptual and the detailed design phases. Safety / Reliability targets were apportioned to subsystem levels and used to guide designers to ensure their designs met requirements. Examples of these are: steam generator level control systems, standby electrical power, control power, primary coolant pressure and inventory control, and service water systems. The use of probabilistic safety assessment techniques was embedded into the system design process.

2.5 Safety Design Matrices

As noted, the single failure / dual failure approach to safety design and licensing served the Canadian nuclear industry well by providing substantial safety margins and in-depth defense. Of course, the attainment of these margins relies on there being no significant dependencies between process systems and safety systems. In the mid-seventies concerns were raised that for some classes of process failures there was not sufficient assurance that required mitigating systems were independent of process systems. For example, a loss of service water has the potential to lead to a loss of feedwater pumps, and hence loss of the normal reactor heat sink. It, however, can also contribute to failure of the backup shutdown cooling system. Further, the safety analyses carried out to demonstrate compliance with the single/dual failure rules did not extend into the long term to confirm that longer-term mitigating actions would be reliably taken. Some of these were manual actions by plant operators, such as valving-in a backup heat sink, or switching to the recirculation mode of emergency core cooling after a LOCA.

To deal with these concerns, an analysis approach was developed at AECL called the Safety Design Matrix (SDM) methodology. Initially, this comprised listing in a tabular form means of event mitigation for various initiating events, by themselves and in combinations with other failures, over three time frames, viz., the short (15 minutes), medium (hours), and long (days) time frames. This helped identify plausible event combinations for which there was no mitigation provided in the design. Later, event sequence diagrams were used to identify such combinations. These diagrams graphically represented the short, medium, and long term response, took into account potential post-event operator errors, and quantified the frequency of initiating events and failure probabilities of mitigating actions. Individual sequences were continued until the end state was shown to have a frequency of less than 10^{-7} per year. Where end-states with a frequency greater than 10^{-7} per year were identified for which the available analysis could not preclude the likelihood of fuel damage, either the end-state was analyzed to confirm there would be no significant fuel damage, or design changes were made [6].

The SDM analysis was first carried out for the loss of service water event at Bruce A. A number of design insights and modifications resulted from this analysis, such as identification of equipment needing backup cooling, and definition of operator actions required to be included in operating procedures. Subsequently, such analyses were carried out for four more initiating events for Bruce A, viz., loss of instrument air, loss of electrical power, loss of maintenance cooling, and loss of moderator and end shield cooling [42].

The value of SDM studies was recognized not only by AECL but also by the AECB. As a result, fifteen such assessments were carried out for the next population of CANDU reactors, viz., Pickering B, Bruce B, and the 600 MWe units (CANDU 6) at Gentilly 2, Pt. Lepreau, and Wolsong 1. The SDMs were effective in identifying design weaknesses during the design program and led to worthwhile design improvements, particularly with respect to safety support systems. Some of these design changes were [31]:

1. Gravity-fed backup cooling from reserve feedwater tank for feedwater pumps and instrument air compressors,
2. Provision of a second automatic auxiliary boiler feedwater pump (or auto depressurization of steam generators (SGs) and gravity feed from dousing tank to SGs) to cater to loss of off-site electrical power events,
3. Automated source of make-up to recirculated cooling water,
4. Local air tanks for various loads such as auxiliary feedwater control valves, HT liquid relief valves, pressurizer relief valves (seismically qualified),
5. Hardwired boiler level control feature to cater to loss of computers and instrument air,
6. Second source of bearing cooling water for raw service water pumps,
7. Automatic CCW pump trip on T/B basement high level,
8. Hardwired window annunciations on Reactor Inlet Header (RIH) high temperature to complement other indications of degraded heat sink,
9. Automatic isolation of hot D₂O flow out of the HT purification cooler and the degasser-condenser, and
10. Various setbacks such as on low level in end shield, moderator temperature, low moderator level.

The SDMs also influenced the provision of a secondary control center, emergency power system and emergency water system for mitigation of common mode events such as earthquakes and tornadoes [2]. These systems were separate from the primary means of mitigating other events, such as standby power generators and redundant cooling water pumps.

2.6 CANDU Reactor PRAs

2.6.1 Darlington Probabilistic Safety Evaluation (DPSE)

At about the same time as the SDM studies, the Probabilistic Risk Assessment methodology to assess nuclear power risk was developed, with the issuance of the US Reactor Safety Study in 1975. Compared to the SDMs, PRAs were more comprehensive, and provided a systematic means of identifying and quantifying dependencies between systems. Unlike the SDMs, PRAs also provided estimates of overall risk as a means of judging safety and prioritizing safety issues.

The first comprehensive PRA of a CANDU reactor was undertaken by Ontario Hydro for the Darlington Station and issued in 1987. The primary objective of the PRA, known as the Darlington Probabilistic Safety Evaluation (DPSE) Study, was to carry out a thorough review of the station design during the design phase, with a view to identifying any design vulnerabilities. It used state-of-the-art PRA methods of event tree and fault tree analyses, supported by reliability data and human interaction modeling to meet this objective. The Study identified key accident sequences leading to the release of radioactivity from the plant and estimated their frequencies of occurrence. The DPSE focused on accidents arising from plant malfunctions or loss of off-site power (so-called internal initiating events) to meet its design assessment objectives and excluded external events such as earthquakes and tornadoes for which separate bounding analyses were performed. As is typical in PRAs, it first identified the ways and means by which radioactivity could be released from the fuel. Such accident sequences were categorized into so-called Fuel Damage Categories (FDCs), based on the extent of associated fuel damage. Next, the response of the containment system to the occurrence of the fuel damage categories was assessed, thereby identifying containment subsystems whose failure would lead to a release out of containment. The various combinations of fuel damage categories and containment failure modes were categorized on the basis of the associated release into what were called ex-plant release categories (EPRCs). The summed frequency of FDCs comprising events in which the core was severely damaged was calculated, as was the summed frequency of EPRCs resulting in a potentially large release outside containment. For such severely damaged fuel events, consequence analysis was not carried out as their computed frequency of occurrence was judged to be sufficiently low. For all other events off-site consequences were estimated, in addition, of course, to their frequencies.

Frequencies of the FDCs and EPRCs were calculated by means of computer integration of the event and fault trees, thus accounting for any dependencies between systems and initiating events [9]. The Study assessed the severe core damage frequency to be $4E-6$ per reactor-year and large release frequency to be $8E-7$ per reactor-year [8].

The key DPSE core damage sequences were:

1. Pressure tube failure with failure of the associated calandria tube and annulus gas bellows rupture, leading to coincident loss of heat transport coolant and moderator via the annulus gas bellows and the calandria tube, followed by emergency coolant injection (ECI) failure,
2. Loss of off-site power followed by loss of all on-site standby generators due to common fuel supply faults, and emergency power generator supply failure due to operator error, and
3. Loss of service water followed by HT pump seal failure and loss of ECI.

These risk-dominant accident sequences are characterized by dependencies, sometimes subtle, between process and safety systems, and, generally, are not the ones analyzed in standard safety reports.

A number of design deficiencies were identified and corrected during the course of the DPSE Study. Some of these were as follows:

- The likelihood of a LOCA outside containment via the D_2O storage tank was reduced by
 - providing different temperature sensors to control bleed cooler outlet temperature and to close the bleed condenser level control valves (BCLCVs) on high temperature,

- changing the fail-state of BCLCVs on loss of power to their solenoid valves to fail-close rather than “as-is”,
- and providing automatic closure of bleed condenser isolation valve on high bleed condenser level. As a result, a core damage and containment bypass event with a frequency in the order of 1.0E-4 per year was eliminated.
- Automatic reactor setbacks on loss of end-shield cooling were installed resulting in reduction of the frequency of a 7E-5 per year core damage sequence by two orders of magnitude,
- Annunciation was provided of the failing low of a number of direct-acting transmitters, provided to sense high pressure or level (for example, due to loss of power to the transmitter), such as high reactor building pressure, high moderator level and high steam generator level, to improve their availability,
- The control circuits of the two ECI pump room air cooling units (ACUs) were modified to eliminate single failures affecting both ACUs and, potentially causing loss of high pressure emergency coolant injection, and
- A dependency between the redundant steam generator and shutdown cooling heat sinks was removed, whereby water supply to the shutdown cooling heat exchangers would be diverted, in the event of a main steam line break, due to failure to isolate non-essential loads as a result of the consequential failure of normal power and instrument air.

The information contained in the DPSE was also used to develop the station's emergency operating procedures [21] and operational reliability program [20]. As a pre-operational study, the DPSE played a significant design assist role [7].

In 1988, Ontario Hydro also established a set of safety goals to be used in conjunction with its PRAs to judge safety adequacy of its plants. Risk targets and limits were developed for individual early and delayed fatality, and large release frequency. Later, targets and limits were added for core damage and a severe release. The basis for these safety goals was the principle that the risk to a member of the public from the operation of nuclear plants should not be more than 1% of the accident risk to which he/she is normally exposed.

2.6.2 AECL/KEMA CANDU 6 PSA Study

At about the same as the DPSE, a joint PSA Study was undertaken by AECL and the Dutch utility support organization N.V. Tot Keuring van Elektrotechnische Materialen in Arnhem (KEMA), using an operating CANDU 6 plant in Canada as the reference plant [5, 25]. The Study extended event sequences beyond the cut-off limit of 1.0E-7 per year employed in the previous SDM studies to the point of core disassembly. More significantly, it derived source terms for CANDU reactor accidents for possible comparison with those for light water reactors, utilizing a combination of CANDU-specific computer programs and the USNRC's Source Term Code Package. As such, it was one of the first level 2 PSA assessments for CANDU reactors.

Building on the fault tree and event tree information contained in the SDMs, the CANDU 6 PSA study calculated the core damage frequency to be 4.6E-6 per year. Fuel damage progression and releases outside containment were assessed for the following categories of events: early and late core disassembly, moderator as a heat sink with impaired containment, and the interfacing LOCA scenario. Licensing analyses were used for conditions other than core disassembly. For the latter, characteristics such as coolant mass and energy discharge rates, timing of fission

product releases to containment, energy released into containment, zircaloy-steam reactions, and hydrogen burning were estimated.

A best estimate evaluation of a representative event sequence leading to core disassembly was performed. The selected sequence comprised a loss of service water, resulting in loss of cooling to the main feedwater pumps with a consequential loss of normal power supply and other sources of feedwater to the steam generators. The loss of service water also led to loss of cooling to the moderator, calandria vault, and the ECC heat exchanger. The assessment determined that it takes many hours for the HT inventory to boil off after the loss of heat sink, followed by moderator boil-off, fuel channel failure, and accumulation of the core debris at the bottom of the calandria vessel. The debris bed is cooled by the calandria vault water until the water boils off at about 25 hours into the accident and calandria vessel failure occurs. Ultimately, core material penetrates the water-filled containment basement and is quenched, with the water in the basement providing a long-term heat sink [5, 38].

The early core disassembly event studied was the low-probability power runaway event, initiated by any event at full power that leads to a mismatch in power generated and power removed by the coolant (e.g., flow rundown, LOCA, or loss of reactivity control), and failure of the entire control and shutdown capability (including the regulating system and both fast, independent shutdown systems). The shutdown of the reactor is then caused by the displacement of the moderator due to steam discharge from fuel channel failure. The summed average early core disassembly frequency was calculated to be the low value of $3E-8$ events/year.

The CANDU 6 PSA concluded that the releases from containment for most core damage events are relatively modest due to the large amounts of water in the containment atmosphere, and the long time before building pressure rises high enough to cause through-wall cracks in containment. Catastrophic containment failure is not expected because of pressure relief caused by the cracks. Releases are limited to predominantly noble gases and organic iodines. All other radionuclides are almost entirely retained in the water in containment, either in the atmosphere, on walls or other surfaces, or in the reactor building (RB) basement.

The CANDU 6 PSA study helped steer the future direction of CANDU design to reduce both the frequency and consequences of severe accidents. It also identified specific design modifications such as the provision of a shutdown system trip on moderator high temperature, and DCC software changes to effect automatic cooldown of the heat transport system following a loss of end-shield cooling.

2.6.3 Pickering A Risk Assessment (PARA)

Following the completion of the DPSE, Ontario Hydro began a program of PRAs for its operational stations. The first such station selected was Pickering A, on the basis that it had not previously had the benefit of an integrated probabilistic safety assessment. The Pickering A risk assessment study (PARA), as it was called, had as its objectives the preparation of a risk model for the station to review the adequacy of the safety of the station design and provide a means to assist the safety-related decision-making process throughout the life of the station.

The PARA assessed the core damage frequency to be $1.3E-4$ per year, higher than calculated in the DPSE and other CANDU risk assessments, although similar to other reactor designs contemporary to Pickering A [12]. This higher core damage frequency arose due to a lack of

independence between the emergency coolant injection and the moderator system [10, 22]. In Pickering A the moderator pumps are used to recover the discharged coolant from the breach in the heat transport system following a loss of coolant and re-inject it into the core. Failure of these pumps, thus, leads to both the emergency coolant recovery and the moderator heat sink functions to fail simultaneously. The PARA's integrated system fault tree analyses identified a number of single failures that led to inability of the moderator pumps to provide sufficient recovery flow. Examples of these were failure of the dump port controller and loss of air supply to the calandria outlet valves leading to these valves failing open and gaslocking the moderator pumps. Other modes of failure of the moderator pumps were the inadvertent alignment of the moderator pumps to the empty reactor building sump immediately after a LOCA due to loss of air supply to an air-operated sump isolation valves, and loss of moderator room air cooling units due to failure of a control power bus. In some cases, the causes of failure of the emergency coolant recovery had also contributed to the occurrence of a LOCA through the heat transport liquid relief valves.

The bulk of the core damage sequences identified in the PARA resulted from pipe break initiating events. Transient initiators accounted for 17% of the core damage frequency, dominated by low pressure services water and condenser cooling water (CCW) line breaks. The importance of the CCW line break event was due to the consequent flooding of the powerhouse basement and, thus, loss of the instrument air compressors located there. About 14 % of core damage frequency was due to LOCAs caused by breaches in specific components such as steam generator tube ruptures and CANDU-specific initiators such as pressure tube and end-fitting failures, and stagnation feeder breaks.

The PARA's core damage frequency was not low enough to conclude that the frequency of a large release of radioactivity would be sufficiently low without further analysis. It, therefore, became necessary to study the progression of core damage events and the impact on containment.

The PARA developed core damage progression in terms of six possible core damage states (CDSs) depending on the accident sequence, using a spreadsheet-based analytical tool that also incorporated insights from the just-developed integral severe accident code MAAP-CANDU set up to study the Darlington station. CDS1 was the state in which fuel heats up due to loss of cooling, CDS2 represented the disassembly of hot fuel channels and the release of their contents into the calandria vessel, CDS3 failure of the calandria vessel due to the load of hot debris, CDS4 debris heat-up and spread into the calandria vault, core concrete interaction and subsequent erosion and failure of the dump tank, and so on. The timing of the core damage states was calculated for the various core damage events. Also, for each core damage state the fission product release into containment was assessed. Containment system failure events were postulated, such as failure of isolation, failure of hydrogen ignitors, reactor building ACUs, and filtered air discharge system (FADS). These were combined with the fuel damage categories, and the source term outside containment for the various combinations calculated. The resulting ex-plant sequences were categorized based on the magnitude and timing of the associated release into 7 ex-plant release categories. The EPRCs represented the full spectrum of releases outside containment ranging from a large early release driven by a steam surge or an uncontrolled global burn, to late release of noble gases through FADS with all containment systems operational.

Frequencies of EPRCs were calculated, using the same fault tree integration techniques as for the FDCs.

The ex-plant analysis determined the frequency of a large early release to be negligibly small. Multiple containment subsystem failures were required such as containment isolation, to provide an opening in containment, and RB ACUs or hydrogen ignitors, to provide a driving force to expel the fission products out of containment. Containment failure due to overpressure following a core damage event was precluded due to the very large volume of the post-accident containment envelope. The large containment volume results from the interconnection of the eight normally sub-atmospheric reactor buildings and the vacuum building, a structure normally maintained at about 1 psia pressure and able to be connected to an accident unit through self-actuating pressure relief valves. The Study calculated the frequency of a large off-site release, defined as one that would require long-term evacuation of a large number of residents living in the vicinity of the plant, and decontamination or abandonment of local buildings and land, to be $1.2 \text{ E-}7$ per year. The dominant ex-plant accident sequences were those in which some of the failures leading to a core damage event also contributed in some way to containment subsystem failure, such as losses of service water and electrical power.

The PARA was used in a number of ways to influence station design and operation. The most recent of these applications has been to identify ways of reducing the impact of the dependency between the emergency coolant recovery (ECR) and the moderator heat sink functions [39]. Changes were recently made to the moderator system during the Pickering A Return to Service project to reduce the likelihood of a severe core damage event by almost an order of magnitude. Prior to this, the PARA's loss of reactor shutdown logic and consequence analysis was used as the basis of a value/impact analysis of the provisions for a second full-fledged shutdown system comprising liquid poison injection. The analysis found the occupational radiological dose incurred to install a second shutdown system would obviate the public health benefits of a fully-independent second shutdown system. This was an important consideration in the ultimate decision to install a second independent instrumentation and trip system in lieu of a liquid poison injection second shutdown system.

The results of the PARA were also influential in shaping the recommendations of a special committee of the Royal Society of Canada (RSC) to advise the Government of Ontario on a proposal to include additional population areas for emergency preparedness and pre-distribution of potassium iodide pills. The RSC committee recommended against the expansion of the planning basis. Further, the PARA provided unavailability models of special safety system for use in the station's operational reliability program.

2.6.4 AECL's Wolsong 2/3/4 PSA

PRA methods also continued to be utilized at AECL in establishing the detailed design and assessing the safety of AECL's off-shore reactor sales. In 1995, an internal events (Level 1) PSA of the Wolsong units 2/3/4 reactors in South Korea was completed by AECL and the Korea Atomic Energy Research Institute [13]. The PSA methodology comprised the development of medium-sized event trees with post-accident operator actions modeled in the event trees. In addition, detailed system fault trees were developed for 25 systems. The event trees and the fault trees were merged using the Computer-Aided Fault Tree Analysis, CAFTA, computer code. Accident sequences were categorized into eleven categories of plant damage states (PDSs).

Three of these represented events beyond the design basis, and were taken to result in severe core damage. The summed severe core damage frequency was calculated to be $6.1E-6$ per year, based on a mission time of 24 hours for mitigating systems.

The Wolsong 2/3/4 PSA identified that accident sequences initiated by the loss of normal AC power (Class IV power), dual computer control failure, end shield cooling failure, and service water failure contributed the most to the severe core damage frequency. Pipe break initiating events did not turn out to be significant, suggesting that the risk from these design basis events had been adequately controlled. Transients events were dominant contributors to core damage, as they led to losses of reactor heat sink in conjunction with failures of the emergency feedwater system, shutdown cooling and emergency water supply to the steam generators. Moreover, post-accident operator actions were found to feature prominently in the dominant core damage event sequences. The study also assessed the core damage frequency for mission times of 1 month and 3 months to be $7.7E-6$ per year and $1.4E-5$ per year respectively, still fairly low values.

A number of design changes resulted from the Wolsong 2//3/4 PSA, such as automatic start of the emergency coolant recovery pumps, provision of redundant valves in the ECC system, improved design of heat transport pump high bearing temperature trip, and changed failure position of certain valves in screen wash system to fail closed on loss of instrument air. The study also resulted in code classification upgrade to the boiler blowdown piping inside containment [23].

2.6.5 Extension of Wolsong 2/3/4 PSA in South Korea

The Wolsong 2/3/4 Level 1 PSA was extended by Korean staff at the request of the Korean Regulatory authority to include Level 2 and external event analyses [14]. As well, human reliability and parametric common cause methodologies that had been utilized in the latest PWR PSAs were adopted. External events analyzed were seismic, fire and flooding, and a new severe accident code called ISSAAC (Integrated Severe Accident Analysis Code for CANDU) was developed and used for assessing core damage progression. The Korean fault tree evaluation code, KAERI Integrated Reliability Analysis Code Package (KIRAP), was used for sequence quantification [25]. The assessment was completed in 1997 and submitted in support of the operating license.

The revised Wolsong 2/3/4 PSA estimated the core damage frequency to be $1E-5$ per year. The inclusion of the CCFs led to about a 40% increase in the CDF, based on CCF parameters used in PWR PSAs.

Some design improvements resulting from the revised Wolsong 2/3/4 assessment [31] were:

1. Heavier steel bracing of emergency water supply building,
2. Additional lateral restraints for battery racks, and
3. Anchorage of Motor Control Centers and transformers.

2.6.6 Bruce B Risk Assessment (BBRA)

Following the completion of the Pickering A Risk Assessment, Ontario Hydro undertook the PRA of the Bruce B station. The Bruce B Risk Assessment (BBRA) was issued in 1999 and had

similar objectives as the PARA, viz. assessment of the station's safety design and the development of a plant risk model for use in operational safety-related decision-making. The BBRA also considered only internal events, with explicit modeling of the impact of flooding due to internal initiating events such as condenser cooling water and service water pipe breaks, and severe high and low temperature conditions. Unlike the PARA, the BBRA also contained an assessment of core damage events when the reactor is operating in the shutdown state. Further, the BBRA made some use of the MAAP-CANDU code for severe accident analysis in addition to the analytical methodology developed during the PARA.

The BBRA calculated Bruce B's severe core damage frequency to be $6.4E-5$ per reactor-year [17]. About 10% of this value was attributed to initiating events occurring during the long term shutdown mode of the reactor. This value was within Ontario Hydro's core damage frequency limit of $1.0E-4$ per year, but above the goal of $1.0E-5$ per year. The BBRA also defined the severe off-site release category as comprising events in which greater than 10% of Cs-137 was released from the containment, and calculated its frequency to be $1.2E-7$ per year, marginally higher than the goal of $1.0E-7$ per year, but well-below the limit of $1.0E-6$ per year. The large off-site release (greater than 1% of Cs-137) frequency was calculated to be $3.7E-7$ per year, below the Ontario Hydro goal of $1.0E-6$ per year.

The BBRA's dominant accident sequences leading to core damage arose from a range of intermediate steam/feedwater line breaks in the power house for which the automatic actuation of the powerhouse venting system was precluded. These so-called blinding breaks are associated with a steam discharge rate that is not high enough to actuate the powerhouse venting system or lead to a reactor shutdown on low heat transport pressure. Operator action is required to remote-manually open the powerhouse vents. Failure of the operator to act leads to a high enough powerhouse temperature that not only do the unqualified normally-operating systems fail, but so do the standby systems such as the emergency power and water systems, and steam-protected rooms whose qualification envelope is based on successful power house venting.

The slightly higher off-site release frequency for Bruce B than for Pickering A results from Bruce B's smaller multi-unit containment volume and the existence of more steam post-accident, due to vaporization of the shield tank inventory, acting as a driving force to expel fission products from a postulated pre-existing containment opening.

Modifications to the powerhouse venting system had already been committed to by the time the BBRA was issued. The BBRA concluded that with these modifications installed, the Environmental Qualification (EQ) program implemented, and the improvement initiatives in Ontario Hydro to improve component reliability and human performance completed, the core damage and severe release frequencies would approach target values.

The BBRA models have been used as the basis for operational reliability monitoring of the four special safety and 17 safety-related systems. A major application of the models has been in the management of shutdown risk. Bruce B has implemented the BBRA outage risk models on EPRI's Risk & Reliability Workstation tool EOOS (Equipment out of service) for outage configuration assessment, and routinely uses it to ensure high risk plant configurations are identified and controlled [24].

2.6.7 CANDU 9 PSA

AECL used its PSA methodology during the design process of its next product line, the CANDU 9 design. This reflected the conviction since the days of the SDMs and the DPSE that the greatest use of a PSA was to ensure safety design adequacy while the plant was still in the design phase. For the CANDU 9 design, AECL first ensured that enhancements based on earlier PSAs and those then underway, such as for the Phase 3 Qinshan CANDU units, were implemented. A PSA of the reference design was then undertaken to identify any further design improvements.

The CANDU 9 reference design incorporated a number of improved design features [40] as follows:

1. Two independent means were provided of supplying high pressure auxiliary feedwater to the steam generators, one of which was seismically qualified and the other included a diesel-driven pump,
2. The number of ECC valves was reduced, changeover from the injection to the recovery mode was made automatic, sustained low heat transport pressure was used as a conditioning signal to initiate injection, and the number of recovery pumps and heat exchangers in the ECC system was increased to 4. The reduction in ECC valves was achieved by replacing conventional check valves by a combination that incorporated one-way rupture disks and a floating ball inside the high pressure injection tanks,
3. Service water pumps and the electrical distribution system were relocated to make them immune to steam and feedwater line breaks,
4. Redundant service water supplies were provided to the shutdown coolers, one of which was seismically-qualified,
5. An automatic trip of HT pumps on high bearing temperature was provided,
6. Rubber expansion joints in the recirculated cooling water system were eliminated and their number in the raw service water system reduced,
7. Automatic reactor power reduction in the event of low flow or high temperature in the end shield cooling system was provided,
8. Four on-site diesel generators, automatically initiated on loss of off-site power, were provided,
9. A reserve water tank was included to provide gravity makeup to the calandria vessel, the steam generators, and the end-shield cooling system. Also, a capability to recover the moderator inventory from the reactor building floor was added,
10. Means were provided to rapidly bolt-up and fill-up the heat transport system in the event of a loss of shutdown cooling during maintenance outages requiring the HT system to be drained. This enabled the steam generators to be used for decay heat removal for such infrequent reactor states as well.
11. The potential for shutdown cooling pump gaslocking was reduced by maximizing the elevation difference between SDC take-off line and HT level in the drained state,

12. Local air coolers in the reactor building were supplied power from the emergency power system.

A target summed core damage frequency of $1.0E-5$ per year was established for the CANDU 9, similar to that for Advanced Light Water Reactors (ALWRs). As well, a $1.0E-6$ per year limit was placed on the frequency of each event sequence leading to core damage. The preliminary PSA of the un-sited CANDU 9 design determined these frequency limits were met. It enabled reliability targets to be set for process systems and safety related systems.

The CANDU 9 PSA also helped identify critical operator actions so these could be used as input into control center design and emergency operating procedures. The preliminary PSA also provided input to the test and maintenance program.

2.6.8 Generic PSA Program at AECL

In 1998, AECL undertook a program of Generic PSA for its line of power reactors, comprising primarily the CANDU 6 and CANDU 9 products, in response to requests of prospective customers. The purpose of the program was to establish a standard state-of-the-art PSA as an integral part of the product offering based on commonly-accepted scope and methodologies of PSAs [41]. This involved enhancements to Level 1 PSA scope to include common cause failure (CCF) analysis and improved human reliability modeling, Level 2 severe core damage analysis using MAAP4-CANDU, and inclusion of seismic, fire and flooding risk analyses. AECL adopted the Unified Partial Method (UPM) to perform common cause modeling [33], the ASEP Human Reliability Procedure [34], and developed methodologies to explicitly link core damage sequences with containment mitigating systems to provide input to the Level 2 analysis.

The UPM method permits a qualitative evaluation of the vulnerabilities of redundant components to CCF, while providing a reasonable quantitative estimate of the effects of these failures on the eventual in-service reliability of the systems. It considers the impact of such factors affecting CCFs as redundancy & diversity, separation, equipment complexity, awareness of CCF issues amongst designers, quality of training, safety culture, and quality of the human-machine interface.

As part of the Generic PSA, the seismic hazard input to be used in the assessments was defined based on the seismic hazard data for current and future CANDU plants around the world. Design information on the Nuclear Steam Plant and Balance of Plant for CANDU 6 was used to calculate the seismic fragilities of structures and equipment based on analysis, test, combination of analysis and test, experience and judgment. A Fire PSA methodology was also developed comprising calculation of fire initiating event frequencies for CANDU plant, identification of plant characteristics relevant to fire events, fire scenario analysis, and quantification of fire risk in terms of severe core damage frequency. The plant characteristics relevant to fire were assembled in a database that included fire zone data (fire ratings, rooms, size etc.), a list of safety related and PSA credited equipment, and details of fire hazards (ignition sources, combustible loading, etc.). A fire and seismic walkdown training exercise with an experienced consultant was conducted at a Canadian CANDU plant.

The Generic PSA studies enabled a number of design improvements to be identified for inclusion in new designs. For example, the flooding PSA proposed adding the following [31]:

1. Automatic CCW pump trip on Turbine Building basement high level,

2. Automatic trip of Raw Service Water (RSW) pumps on Recirculated Cooling Water (RCW) heat exchanger (HX) pit high level,
3. Flood/Steam barriers in RCW HX room and feedwater pump room, and
4. Fewer unlimited flooding sources due to air-cooled standby diesel generators and RCW cooling of spent fuel pool cooling heat exchanger.

2.7 Lessons from Risk-based Assessments

From the foregoing description of the various risk-based assessments of CANDU plants, such as system reliability studies, SDMs and PRAs, it is possible to identify the following as some of the important design lessons for future reactors:

1. Minimizing the likelihood of loss of reactor power regulation events (Ontario Hydro's LOR-related experience),
2. Ensuring low likelihood of loss of heat transport integrity following process failures, such as through HT relief valves, pump seals, or interfacing systems (SDMs, DPSE, PARA),
3. Improving reactor heat sink reliability (SDMs, AECL's Wolsong 2 PSA),
4. Controlling the impact of high energy secondary side line breaks (BBRA),
5. Improving the ability of calandria tubes to withstand pressure tube ruptures (DPSE),
6. Providing severe accident mitigation, (PARA, Korean Wolsong 2/3/4 Level 2 PSA, CANDU 9 PSA),
7. Reducing the potential for intra-system component redundancy to be compromised (PARA, CANDU 9 PSA),
8. Assessing the impact of severe accidents on containment integrity (CANDU 6 PSA, PARA, Wolsong 2/3/4 Level 2 PSA),
9. Assessing the impact of external events on reactor safety (Korean Wolsong 2/3/4 PSA, GPSA),
10. Improving the human-machine interface to reduce post-event human error probability (Wolsong 2/3/4 PSA, GPSA).

As we shall see next, a number of these lessons have been incorporated in the proposed design of the next generation CANDU, viz. the Advanced CANDU Reactor.

3. ADVANCED CANDU REACTOR

3.1 ACR Design Features

The ACR design incorporates a number of enhanced safety features based on experience gained with previous CANDU designs, including the insights from the various CANDU risk-based studies. Some of these features are presented below, along with a description of how they reduce plant risk. Further, the ACR's safety is being examined extensively through safety analysis including a PSA.

- a) The ACR employs solid reactivity control devices for spatial power control instead of the injection of water into zone compartments, with their attendant potential to initiate an upward power excursion on failure of the liquid zone pumps, e.g. due to loss of power to the pumps. This takes into account prior experience with reactivity control systems indicating the need for simplifications to reduce the frequency of loss of regulation event.
- b) The void reactivity coefficient is small and negative, due to the use of slightly enriched fuel and light water coolant. This provides a good balance of inherent nuclear protection between loss-of-coolant accidents (LOCA) and accidents leading to fast cooldown of the heat transport system. It provides greater design margins than before in the capability of the shutdown systems. The frequency and consequences of LOCAs and coincident shutdown system failure are greatly reduced, thereby constituting a significant safety improvement, as well as reducing operational constraints.
- c) One-way passive rupture discs are used in the Emergency Coolant Injection system to provide make up to the HT system following a LOCA. As well, the ECI accumulator tank is located inside the reactor building. Further, the ultimate rupture strength of the long term cooling (LTC) system is capable to withstand the operating pressure of the heat transport system. Together these features both increase the reliability of emergency injection, as well as reduce the probability of an interfacing systems LOCA (called "Blowback" in CANDU PRAs).
- d) The calandria tubes are of high strength. This enables them to withstand the loading due to a pressure tube failure for considerable time so operator action can be taken to reduce heat transport pressure and temperature, thereby preventing creep rupture of the calandria tube of the affected fuel channel.
- e) A particular feature of the design is the provision of large quantities of water located in a tank in the reactor building dome called the Reserve Water Tank (RWT), which is part of the Reserve Water System (RWS). The RWS is used to supply water from the reserve water tank for a number of purposes such as:
 - Ensuring adequate net positive suction head (NPSH) for the long term cooling pumps in the event of a LOCA,
 - Filling the steam generators under gravity to allow core heat removal for extended periods of time via thermosyphoning,
 - Providing a gravity-fed source of water for moderator inventory makeup enabling the fuel to be cooled while still retained in the fuel channels in the event of a LOCA coincident with loss of emergency coolant injection, and

- Making up end shields and calandria vault inventory and enabling heat rejection from the calandria to arrest core melt progression following disassembly of the core in the event of a sustained loss of all engineered heat sinks.

The RWS system, thus, plays a role both in the avoidance of fuel damage, as well as mitigation of events that may have resulted in core damage. Once actuated, the system carries out its functions passively, without any reliance on motive power. Its risk reduction worth is likely to be substantial.

- f) Improved containment design features such as passive autocatalytic recombiners for post-accident hydrogen control, and vault and dome local air coolers for steam pressure control.
- g) Provision of distributed control systems to control the plant routinely, freeing the operator from mundane tasks, thus reducing the likelihood of operator error. The safety system responses are automated to the extent that no operator action is needed for a minimum of eight hours following most design basis accidents.

It should be noted that while the ACR design includes a number of improvements relative to previous reactors as discussed above, it also departs from some previously-standard features of the CANDU design. These are as follows:

- a) The same set of pumps and heat exchangers is used for the shutdown cooling function, or residual heat removal, as well as for ECC recovery. This equipment is located outside containment, whereas in previous designs the shutdown cooling system was located inside containment. However, this feature of the ACR is consistent with international pressurized water reactor practice, and, as such, should be found acceptable, particularly in view of the ultimate rupture pressure of the system being capable to withstand the operating pressure of the heat transport system.
- b) In past CANDU designs, two separate sets of electrical power and water systems, termed standby and emergency, were provided for decay heat removal, of which the "emergency" systems were designed to withstand the impact of common mode events such as earthquakes and manually initiated. In the ACR, the standby systems themselves are qualified for common mode events and, as such a separate set of "emergency" systems is not necessary. This actually provides more reliable mitigation of common mode events because of reduced reliance of the surviving system on operator action. The apparent reduction in redundancy for other initiating events is minimized by configuring key mitigating systems in the form of multiple redundant "divisions", analogous to the "train" concept of LWRs.

The impact of these departures will be assessed by the intended detailed PSA of the ACR design.

4. ACR PSA

4.1 PSA Objectives

An integral part of the design, safety assessment, and licensing activities for the ACR is the development of a PRA using state-of-the-art methods that meet regulatory expectations.

The overall objectives of the ACR PSA are to [35]:

- Identify dominant accident sequences leading to core damage and large release, and estimate their frequencies for comparison with acceptance criteria,
- Rank Structures, Systems and Components (SSCs) in terms of significance to core damage frequency (CDF) and large release frequency (LRF). The resulting risk insights into the ACR design are to be fed back into the design, and the operation and maintenance of the plant.

The PSA will be integrated into the ACR design process and its results used as one of the major inputs for the design. Designers will review any design vulnerabilities and significant accident sequences identified by the PSA and will consider modification of the design if practicable.

The PSA will consist of both a Level 1 and a Level 2 assessment.

The Level 1 portion will include the assessment of risk from internal events, internal floods, internal fire, and operation in the shutdown state. As well, a seismic margin assessment will be conducted.

Containment performance analysis, and analysis of physical processes associated with key severe core damage accidents will be performed as part of the Level 2 study.

The ACR PSA methodology is guided by the following two USNRC documents: NUREG/CR-2300, *PRA Procedures Guide*, Volume 1, Section 2.2 [36], and NUREG/CR-4550, Volume 1, Revision 1 [37].

The PSA has already identified a comprehensive list of initiating events by conducting a systematic review of the plant design [19].

The shutdown state PSA will address additional concerns to those that are addressed in the full power PSA. It will include simultaneous system unavailability during different phases of an outage, important operator actions to restore functions, and maintenance restrictions on various mitigating and safety systems while the plant is in a specified shutdown state. A shutdown state PSA can provide insight to outage planning, outage management practices (e.g., maintenance restrictions), and design modifications to lower the risk of severe core damage.

The ACR PSA will establish the spectrum of accident sequences that could lead to specified design basis accidents, limited core damage accidents, or severe core damage accidents, determine their basic causes and calculate their frequencies.

Acceptance criteria (safety goals) specified in the ACR's Licensing basis [15] will be used to judge safety design adequacy. Specifically, these goals call for the summed severe core damage frequency to be less than 1E-5 per year and large release frequency to be less than 1E-6 per year (except for seismic). As well, the guideline in CNSC document C-006 Rev. 1 [27] that the use of the moderator system as a reactor heat sink should be less than 1E-4 per year will be utilized. A

further goal is that no individual severe core damage accident sequence should be more likely than $1E-7$ per year. A mission time of 24 hours is specified for purposes of comparison of computed values with these criteria.

The PSA will help:

- a) Identify feasible design changes required to minimize the need for operator actions to mitigate the accident consequences,
- b) Identify key operator actions and provide supporting information for subsequent use in the preparation of emergency operating procedures (EOPs).
- c) Provide input to the environmental qualification program and control center design.
- d) Influence the test and maintenance programs such that they can be optimized in terms of cost and safety.
- e) Establish system reliability targets via high level fault tree analysis of the front-line and support systems.

External events like high winds and tornadoes will not be studied as they are not expected to be safety significant contributors because the plant is designed for these hazards. Site-specific external events will be evaluated as per the recommended progressive screening approach specified in NUREG-1407 [26].

The PSA will provide information on accident sequences and their frequencies to classify design basis events for purposes of licensing analysis. It will confirm that the safety system unavailability targets of CNSC's Regulatory Documents R7 [28], R8 [29] and R9 [30] are met.

As a main purpose of the PSA is to assist the design process, it is being conducted iteratively as the design progresses.

A number of "design-assist" assessments have already been conducted in support of the ACR design. Specifically, a preliminary event tree analysis of selected initiating events [18], a fault tree analysis of the emergency feedwater supply to the SGs, and assessments to help decide specific design configurations have been completed. Brief descriptions of these assessments are provided in the following sections as an indication of the extent of such analyses in the finalized PSA.

4.2 Preliminary Event Tree (ET) Analysis

A number of modifications to the reactor core and plant design have been made in the ACR in comparison with previous CANDU designs as noted earlier. A preliminary event tree analysis was, therefore, conducted to assess the ability of the proposed design to meet the criteria listed in Section 4.1. Eleven internal initiating events were considered, based on a review of the ACR safety design, and engineering insights from previous CANDU PSA work.

The main purpose of the preliminary ET analysis is to provide early inputs to the design teams regarding the reliability/unavailability requirements of the ACR systems that are used for accident mitigation as well as feedback on some of the system performance requirements. These inputs/feedbacks are a part of iterative process in which the reactor design is finalized and optimized while ensuring nuclear safety requirements are not compromised.

The preliminary ET analysis is a screening analysis, with credit for passive mitigation features, such as supply of water from the Reserve Water System to the HT system, taken in only those sequences which would otherwise have a higher than target frequency. Further, uncertainties associated with actions of active mitigating systems are treated conservatively. For example, it is assumed that the Emergency Core Cooling (ECC) function fails following all small breaks if steam generator cool down is not available to reduce the HTS pressure. In reality, only a small spectrum of such breaks will require automatic cooldown. Deterministic analyses are in progress to facilitate realistic modeling in the final PSA.

Results indicate that the ACR design can meet the prescribed severe core damage frequency (SCDF) criteria.

Salient aspects of the preliminary Event Tree Analysis are described below, extracted from Reference [18].

4.2.1 Selected Initiating Events

Initiating events examined in the event tree analysis are listed in Table A-1 in Appendix A, along with their estimated frequencies of occurrence. All these events are postulated to occur during the full-power operation of the ACR.

Initiating events 1 to 4 are small breaks, which have different characteristics in terms of accident mitigation. Pressure tube rupture, IE-PTR (No. 1), results in a leak through the channel bellows, just in excess of the HTS make-up capacity, that relies mostly on SG cool down for mitigation. Pressure tube/ calandria tube rupture, IE-PCTR (No. 2), is a larger in-core break that might affect the ability of the moderator to act as an alternate, long-term heat sink. Feeder break, IE-FBIO (No. 3), is a prototypic small break, which occurs in a feeder of the HTS. Feeder stagnation break, IE-FSB (No. 4), is a unique small break that could potentially lead to loss of both heat transport and calandria inventory, similar in effect to a pressure tube / calandria tube rupture.

For the preliminary analysis, conservatively, the frequency of the feeder stagnation break was assumed to be 10% of the feeder break frequency. This high frequency value was deliberately selected to evaluate the robustness of the ACR mitigating system design. During the detailed PSA, a best estimate of the feeder stagnation break frequency will be calculated. The frequency of a stagnation break that leads to fuel melting and channel failure is expected to be at least an order of magnitude lower than the $2E-4$ /yr value assumed in this report, justifying the exclusion of this event as a design basis event, similar to the pressure tube/calandria tube rupture event (IE-PCTR).

Initiating Event 5 (IE-SWD2), total loss of Division 2 service water, partially disrupts the gland seal cooling of two HT pumps and at the same time leads to loss of half of the mitigating system heat sinks (as Division 1 service water is available).

Initiating Event 6 (IE-LCL4) is a loss of normal power supplies to one unit in a two-unit ACR station, which constrains some options available for providing active heat sinks after the accident.

Initiating Event 7 (IE-SCB) is a shield water loss, which does not immediately impact on fuel cooling, but could potentially cause excessive thermal stresses in reactor structures if not mitigated by a timely reactor cool down.

Initiating events 8 to 10 are secondary-side breaks that disrupt the normal HTS heat sink. Small steam line discharge, IE-MSL3 (No. 8), is a high-frequency accident initiator that includes a number of operator actions for normal mitigation. Symmetric feedwater line break upstream of the feedwater level control valves in the turbine building, IE-FWBS (No. 9), could cause a consequential loss of normal power supply to complicate the accident mitigation. Asymmetric feedwater line break downstream of a steam generator check valve in the reactor building, IE-FWBA (No. 10), is a unique break that cannot be isolated from the affected SG. The inability to isolate constrains the options that are available for accident mitigation.

Loss of regulation, Initiating Event 11 (IE-LOR), is a power excursion that would cause a power-cooling mismatch at high power and high HTS pressure if not automatically mitigated in timely manner by the two independent reactor shutdown systems.

4.2.2 Event Tree End States

The development of event trees includes the assignment of each accident sequence to a Plant Damage State (PDS) that reflects the progression of the accident and the extent of associated fuel damage. The PDSs used in the ET analysis are defined in Table A-2 in Appendix A, and are based on experience from a number of previous PSAs.

PDS 0 to 2 are Severe Core Damage states used for SCDF quantification. The PDSs 3, 4, 6 are Limited Core Damage states, which are not used to enumerate the SCDF.

Event tree analysis is carried out for each initiating event in Table A-1. The event tree depicts various possible sequences, which could occur after the initiating event, by modeling combinations of mitigating system success or failure.

Each sequence in a tree concludes when one of the following conditions exists:

- The reactor has been shut down and decay heat is being adequately removed. No significant plant damage has resulted. Such sequences are labeled “S” (success).
- Failures have resulted in some degree of plant damage. Depending on the initiating event, whether shutdown has occurred or not, and how (if at all) decay heat is being removed, a label is assigned from the listing of PDSs in Table A-2.
- The estimated frequency of the sequence is so low that further study is not meaningful. These sequences are labeled “NDF” (not developed further). A sequence is terminated and labeled “NDF” when its estimated frequency is lower than 1.0E-9 events per year.

The preliminary event trees for ACR are of medium to large size. Separate branch points are assigned not only to heat sinks, but also to the operator actions and services which are required to support the heat sinks (e.g., electrical power and service water).

4.2.3 Operator Actions

Modeling of operator actions in the preliminary ET analysis is largely based on a simplified Human Error Probability (HEP) quantification. It should be recognized that the detailed ACR PSA would incorporate errors of diagnosis as well as execution based on the ASEP procedure (Reference [34]).

Two event trees, viz. IE-PCTR describing the rupture of pressure and calandria tubes and IE-FWBA describing the asymmetric feed water line break downstream of SG check valve, employ more detailed human error analysis methodology rules of ASEP defined in Reference [35] because operator interventions have a considerable impact on the SCDF in these accidents.

4.2.4 System Reliability Targets

The event tree analysis uses system reliability/unavailability values based on simple fault tree analyses of the early ACR design and on experience with PSAs of existing CANDU reactors to estimate individual accident sequence frequencies. These values serve as system reliability targets to be used to guide the detailed design and to be verified by detailed fault tree analysis of the ACR design configuration. These system design targets are provided in Tables A-3 and A-4 (Appendix A).

Typical system headings in the event trees are:

1. Reactor Shutdown via the Reactor Regulating System (RRS), Shutdown System 1 (SDS1), and Shutdown System 2 (SDS2),
2. Automatic isolation of HTS inventory loss (e.g. bleed condenser bottle-up after failed open liquid relief valve (LRV)),
3. Availability of Support Systems, such as Class IV and III electrical power, and service water for pumps and heat exchangers,
4. Avoidance of consequential LOCAs by timely HT pump trip,
5. Steam generator pressure relief via Atmospheric Steam Discharge Valves (ASDVs), Condenser Steam Discharge Valves (CSDVs), and Main Steam Safety Valves (MSSVs).
6. Replacement of lost HTS inventory via H₂O feed and bleed system, ECC, and RWT make-up to the HTS, and
7. Decay Heat Removal via the steam generators, long term cooling system (via the shutdown cooling function), and the moderator.

4.2.5 Sample ET Analysis (Feeder Break)

The treatment of the feeder break initiating event in the event tree analysis is presented below as an illustration of the scope and extent of the preliminary ET analysis. The plant response to the event is described first, followed by the key ET end states. The event trees themselves are included in Appendix B.

Inlet or outlet feeder pipe failures would typically not cause any appreciable mismatch in the amount of heat produced and removed in the affected fuel channel. An outlet feeder break can only lead to an increase in the flow through the affected channel. An inlet feeder break would likely cause the forward flow to be reduced by a small amount (very small break). In the extreme, it could cause the channel flow to reduce to a very low value (so-called feeder stagnation break) or cause the channel flow to reverse (larger breaks). The FBIO event represents off-stagnation breaks, which include all outlet feeder breaks and the vast majority of inlet feeder break sizes and locations. In the absence of a significant mismatch in heat generated

and removed, these breaks are not appreciably different from small LOCAs in reactor headers or other HTS piping. All pressure tubes and calandria tubes are intact after the initiating event.

The reactor trips on low heat transport system pressure, low heat transport system flow or high reactor building pressure.

The ECC conditioning signal is generated on sustained low heat transport system pressure. It activates the crash cool-down of steam generators, opens the isolation valves of ECI accumulator tanks and readies the LTC-ECC subsystem for longer term injection.

The injection from ECI accumulator tanks refills the HTS. The running HT pumps (if not tripped) provide forced flow through steam generators to maintain the heat sink. Some fraction of HTS heat (which depends on the break size) is carried into the containment by the discharging HT coolant. The HT pumps are tripped or turned off before the ECI accumulator inventory depletes and long-term injection by the LTC-ECC system commences. The steam generators continue to serve as heat sinks in conjunction with LTC heat exchangers. The fractions of heat transferred to these two heat sinks depend on the break size.

The passive make-up of steam generators from the RWS cannot be used in this accident, as this supply is isolated on high reactor building pressure to preclude the possibility of an open path between the reactor building atmosphere and the steam generator secondary side.

The plant conditions at the end of mission time (at 24 hours) are stable. The fuel damage is limited to incipient fuel defects, which had opened during the HTS depressurization. Long term actions (beyond the scope of this assessment) would be to isolate the affected channel (e.g., freeze plugs), de-fuel it and repair the broken feeder.

The event trees of Appendix B show that severe core damage results following a feeder break with no flow stagnation if any of the following occurs:

- A failure to shut down the reactor.
- A failure to depressurize the HTS such that a coolant make-up is not possible; this is conservative since in reality a few fuel channels will fail, resulting in HTS depressurization and injection of ECI.
- A failure to provide service water to active mitigating systems.
- Failures of ECC systems to provide make-up to the depressurized HTS in conjunction with a failure of moderator system to provide an alternate heat sink. Only the 'active' heat sink mode of moderator system is credited (i.e., the pumps and the heat exchangers) for conservatism. The 'passive' mode of 'moderator as a heat sink', which involves boiling off water in the calandria vessel and water make-up from the RWS is also expected to be effective, and would yield a lower severe core damage frequency. It is very conservative to not credit the makeup to the calandria from the RWS.

4.2.6 Results of Preliminary Event Tree Analysis

The quantification of the preliminary event trees showed that for almost all accident sequences resulting in core damage the frequency is small enough that the summed frequency would be well within the SCDF targets of Section 4.1. Those accident sequences that were significant to the overall severe core damage frequency were found to be conservatively modeled. Typical conservatisms were the lack of credit for the RWT supply to the moderator, the requirement of

both steam generators for heat removal instead of one for loss of forced primary flow events, the need for steam generator heat sink for small LOCAs, and the simple human reliability model.

4.2.7 Role of Reserve Water System

The limited credits for the Reserve Water System indicate it has a major impact on the severe core damage frequency. A sensitivity assessment was performed by removing all RWS-related credits from the events trees. The summed SCDF value for the 11 selected initiating events was found to increase by an order of magnitude demonstrating the value of the RWS system. When coupled with further credits for RWS that are possible, the advantage of this system will likely be even more striking.

4.2.8 Key PSA Assumptions

The event tree analysis utilized many assumptions related to design and plant response. As part of the ACR detailed design development process, these assumptions are required to be supported by analysis and/or equipment suppliers' test records as appropriate. A list of key PSA support assumptions is provided below:

- A connection from reserve feed water tank (turbine building) to the auxiliary feed water pump suction header is important. This connection will enable the auxiliary feed water pumps to maintain supply to the steam generators in the event of a loss of the auxiliary condensate pump.
- A reliable, automatic closure of the auxiliary feedwater level control valves when discrepancy between the two steam generator levels is sensed is important to crediting the auxiliary feed water in certain accidents.
- The assigned $1.5E-2$ probability of calandria tube failure following a pressure tube rupture requires demonstration that the calandria tube will survive all relevant loading conditions, and that the calandria tube has a high creep rupture resistance. The latter is the ability of the calandria tube to withstand the elevated pressure and temperature environments after a pressure tube failure for long enough time that operator action can be relied upon to reduce the HTS pressure and temperature. To afford high reliability credit for this operator action, the calandria tube needs to survive for about 2 hours or longer.
- The operator plays a crucial role following shield cooling accidents. For highly reliable actions, long times need to be available for manual actions. The current assumption based on CANDU-9 analysis is that 8 hours is available before the HTS pressure boundary, or any other boundary that holds water, could be threatened following a loss of shield water inventory. Analyses need to ascertain that long times are available for the ACR as well.
- Although the HT pumps are not formally environmentally qualified, it is assumed (as a best estimate) that at least one pump can run for up to 60 minutes after a secondary side line break in the reactor building (asymmetric feedline break event). This assumption is reasonably supported by the fact that the HTS pumps are not exposed to cavitation conditions as the HTS remains full and that the discharge from the broken line will not directly impact the pumps. As far as practicable, the layout of the piping needs to minimize a harsh environment around the HT pumps. As only one SG is available (due to the initiating event), and thermosyphoning is assumed to require both SGs, HT pumps are required to maintain

circulation. Therefore, the HTS pumps are credited in the short term in conjunction with AFW which acts as the heat sink until LTC in shutdown cooling mode is valved in. During detailed PSA, this conservative assumption will be assessed and the event trees will be revised appropriately.

The preliminary ET analysis provides a high degree of confidence that the design target for the summed SCDF for all internal and external events can be met.

4.3 Fault Tree Analysis of Emergency Feedwater Supply

A preliminary fault tree analysis has been completed for the Emergency Feedwater (EFW), including parametric common cause modeling using the Unified Partial Method (UPM) [33]. The unavailability of the Emergency Feedwater is defined as the failure of the system to inject water from the reserve water tank (RWS) into the Steam Generators.

Two cases were analyzed: one in which both steam generators are required to act as a heat sink in the event of loss of Class IV power and thermosyphoning is credited as the method of removing decay heat, and the other in which either steam generator is sufficient. The results show that the EFW unavailability result is almost an order of magnitude better in the case where either steam generator is sufficient, attesting to the need to analytically confirm the assumption related to steam generator capability.

The assessment also showed common cause failures of the motorized valves in the system to be dominant contributors to the unavailability of the EFW.

The results of the fault tree analysis are being reviewed by the system designers to effect improvements to the design of the emergency feedwater supply as practical. Further, analysis is being initiated to establish whether feedwater flow to any steam generator is sufficient for decay heat removal via thermosyphoning. This demonstrates the value of the preliminary fault tree analysis to the design of the ACR.

4.4 Early Contributions of PSA to ACR Plant Design

The resolution of a number of design issues during the preliminary design phase of the ACR was facilitated by the use of PSA techniques. The designers and the PSA staff worked closely to ensure the PSA's reliability requirements would be met while at the same time optimizing the design. The following is a list of some of these design items:

1. All systems were analyzed qualitatively to ensure they meet the single failure criterion.
2. The optimal number of Class III diesel generators was determined by assessing the impact of various proposed configurations on the accident sequences involving loss of Class III power.
3. Similar to item 2 above, the required number of main and auxiliary feedwater pumps, and the configuration of the back-up source of water for the auxiliary feedwater supply, was established using a similar methodology as in item 2.

4. The recirculated cooling water (RCW) system and the raw service water (RSW) system were reviewed by examining selected accident sequences involving these systems and by simplified fault tree modeling. A configuration was selected that provided the highest reliability taking into account the major failure modes to which these systems and their components were subjected, such as expansion joints failures, screen-wash system failure and pump failures.
5. PSA staff also provided input to the system designers to remove potential sources of unreliability in their systems. For example, in an early configuration of the ECI system it was identified to the designers that the one-way rupture disks could inadvertently burst while reactor power maneuvers were underway. Provision for additional operating procedures was identified to remove this possibility.

4.5 PSA Quality Assurance

The ACR PSA will be governed by the Quality Assurance procedures applicable to the ACR project as described in Reference [11]. Procedures of particular applicability are those dealing with personnel qualifications and training, design verification, design review, change control and record keeping.

As noted before, the conduct of the PSA for the ACR is an integral part of the design process. As such AECL has made mandatory the review of PSA event trees and fault trees by the relevant design staff and the formal dispositioning of comments and issues raised. The PSA forms the basis of a continuing dialogue between designers and safety analysts and is iterative in nature.

The ACR PSA will also be subjected to a formal independent peer review to confirm it possesses attributes generally considered essential for a quality PRA, e.g., those outlined in Reference [32].

5. CONCLUSION

This report has traced the use of PRA in assessing CANDU reactor safety. It is shown that risk concepts have been widely utilized in the Canadian nuclear industry. As such, it is only natural that the latest CANDU reactor design, the ACR, should also be subject to evaluation by PRA techniques. The report has reviewed the status of the ACR PSA and highlighted the role the PSA is playing in informing the ACR design with risk insights.

It is concluded that the ACR design incorporates a number of design enhancements identified in previous PSAs. PSA techniques are being widely used during the design phase of the ACR to ensure the design is capable of meeting PSA objectives such as the frequency limits on occurrences of core damage and large release.

6. REFERENCES

- [1] E. Sidall, W.B. Lewis, "Reactor Safety Standards and their Attainment", Atomic Energy of Canada Ltd., Report AECL-498, September 1957.
- [2] G. Brooks, "Early Steps in the Evolution of CANDU Probabilistic Safety Assessment", IAEA workshop on Heavy Water Reactor (HWR) PSA, Toronto, Canada, May 1999.
- [3] D.C. Hurst, F.C. Boyd, "Reactor Licensing and Safety Requirements", Proceedings of the 12th Annual conference of the Canadian Nuclear Association (CNA), Ottawa, 1972.
- [4] G.C. Laurence, "Required Safety in Nuclear Reactors", Atomic Energy of Canada Ltd., Report AECL-1923, 1961.
- [5] P.J. Allen, J.Q. Howieson, H.S. Shapiro, J.T. Rogers, P. Mostert, R.W. van Otteloo, "Summary of CANDU 6 Probabilistic Safety Assessment Study Results", Nuclear Safety, Vol. 31, No. 2, April-June 1990.
- [6] P. Gumley, "Use of Fault Tree/Event Sequence in a Safety Review of CANDU Plants", International Conference on Current Nuclear Power Plant Safety Issues, Stockholm, Sweden, 1980.
- [7] F.K. King, V.M. Raina, "The Benefits of Pre-Operational Risk Assessment Based on Experience with the Darlington Probabilistic Safety Evaluation, PSA 85, San Francisco, USA, 1985.
- [8] V.M. Raina, P.A. Webster, E.M. Chan, "Darlington Probabilistic Safety Evaluation, Review of Results, and future Applications", PSA 89, Pittsburgh, USA, 1989.
- [9] V.M. Raina et al, "System Modeling Techniques and Insights from the Darlington Probabilistic Safety Evaluation Study", PSA 87, Zurich, Switzerland, 1987.
- [10] V.M. Raina, "Impact of CANDU design features on PSA Results", IAEA PHWR conference, Toronto, Canada, 1993
- [11] AECL, "ACR Quality Assurance Manual", Report No. 108-01913-QAM-001, Rev. 3, June 2003.
- [12] K. Dinnie, V. Raina, "Evaluation of Severe Accident Risk in the Pickering A Risk Assessment," Canadian Nuclear Society (CNS) Conference, Toronto, Canada, 1997.
- [13] H.S. Shapiro, P.A. Santamura, T.H. Nguyen, R.E.B. Henderson, B.A. duQuesnay, J.G. Tielmans, "Severe Core Damage Frequency and Insights from CANDU 6 Level 1 Probabilistic Safety Assessment, Pacific Basin Nuclear Conference (PBNC), Banff, Canada, 1998.
- [14] Korea Electric Power Corporation / Korea Electric Power Research Institute, "Level 2 PSA for a Wolsong Units 2, 3,4", Presentation at IAEA workshop on Heavy Water Reactor (HWR) PSA, Toronto, Canada, May 1999.
- [15] AECL, "Licensing Basis for ACR", Licensing Basis Document 108-00580-LBD-001, Rev. 0, July 2002.
- [16] V.M. Raina, "Experience with PRA Applications in Ontario Hydro Nuclear", Pacific Basin Nuclear Conference (PBNC), Banff, Canada, 1998.

- [17] R. Parmar, W. Webb, V.M. Raina, "Bruce B Risk Assessment: Results and Applications, Proceedings of the 21st Annual Canadian Nuclear Society Conference, CNS, Toronto, 11-14 Jun 2000.
- [18] AECL, "Preliminary Design Assist PSA Level 1 – Selected Full Power Event Trees", AECL Report 10810-03660-AR-001 Revision 1, January 2004.
- [19] AECL, "Systematic Review of Plant Design for Identification of Initiating Events", AECL Report 108-03660-ASD-001, Revision 1, January 2004.
- [20] F.K. King, S. Harvey, C. Packer, "An integrated Program of Risk Assessment and Operational Reliability Monitoring at Ontario Hydro", Reliability Engineering System Safety (UK), 27, 1990.
- [21] F.K. King, C.W. Gordon, V.M. Raina, "The Role of the Safety Analyst in the Development of Abnormal Incident Procedures", IAEA Seminar on Diagnosis of and Response to Abnormal Occurrences at Nuclear Power Plants, Dresden, June 1984.
- [22] V.M. Raina, "Identification of Inter-System Dependencies in the Pickering A Risk Assessment", American Nuclear Society (ANS) Annual Meeting, San Diego, USA, 1993.
- [23] V.G. Snell, R. Jaitly, "Probabilistic Safety Analysis", CANDU Safety Lecture # 20, Shanghai, China, 1999.
- [24] R. Mohindra, "Risk Management Program - Bruce Power Perspective", NSS Risk Management Seminar, Toronto, Canada, 2003.
- [25] IAEA, "Heavy Water Reactors: Status and Projected Development", Technical Report Series No. 407, Vienna, Austria, 2002.
- [26] USNRC, "Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities", NUREG-1407, 1991.
- [27] CNSC, "Safety Analysis of CANDU Nuclear Power Plants" - Draft Regulatory Guide C-006, Rev. 1, September, 1999.
- [28] AECB, "Requirements for Containment Systems for CANDU Nuclear Power Plants", AECB Regulatory Document R-7, February 1991.
- [29] AECB, "Requirements for Shutdown Systems for CANDU Nuclear Power Plants", AECB Regulatory Document R-8, February 1991.
- [30] AECB, "Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants", AECB Regulatory Document R-9, February 1991.
- [31] H.S. Shapiro, "Level 1 PSA", Presentation to USNRC, Washington D.C., May 8, 2003.
- [32] USNRC, "SRP Chapter 19.1, Determining Technical Adequacy of PRA Results for Risk Informed Activities." Draft, 2002.
- [33] V.P. Brand, "The Unified Partial Method: Pragmatism and Expert Assistance in Dependent Failures Analysis", European Safety and Reliability Conference, ESREL 95, Bournemouth, UK, June 1995.
- [34] USNRC, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure", NUREG/CR-4772, February 1987.

- [35] AECL, "Probabilistic Safety Assessment Methodology for ACR", AECL Report 108-03660-AB-001, Rev. 1, July 2003.
- [36] USNRC, "PRA Procedures Guide - NUREG/CR-2300: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", Volumes 1 and 2, January 1983.
- [37] USNRC, "Analysis of Core Damage Frequency: Internal Events Methodology", NUREG/CR-4550, Volume 1, Rev. 1, January 1990.
- [38] J.Q. Howieson, H.S. Shapiro, P.J. Allen, J.T. Rogers, P. Mostert, R.W. Van Othello, "A Probabilistic Risk Assessment Study of a CANDU 600", IAEA International symposium on severe accidents in nuclear power plants, Sorrento, Italy, 21-25 March 1968, IDEC-SM-296/5.
- [39] C. Dross, P. Santamaura, "Pickering A Return to Service - Reduction in Severe Core Damage Frequency", IAEA/AECL Probabilistic Safety Assessment for Pressurized Heavy Water Reactors Workshop, Toronto, Canada, October, 2001.
- [40] R.K. Jaitly, P. Santamaura, H.S. Shapiro, C. Drost, J.R. Fisher, B. duQuesnay, "The Role of CANDU 9 Preliminary PSA in Making Design Decisions", ANS Conference, Pasco, Washington, April 1998.
- [41] M. Bonechi, T. Aziz, R. Jaitly, P.M. Mathew, A. Sretch, "Generic CANDU PSA Program at AECL", Presented at IAEA workshop on Heavy Water Reactor (HWR) PSA, Toronto, Canada, May 1999.
- [42] Rennick, D., Snell, V.G., Gumley, P., and Narayanan, P., "Enhancements in Safety Resulting from Probabilistic Safety Assessments – A Designer's Perspective", Presented at the American Nuclear Society, Topical Meeting on Nuclear Power Plant Operations, Chicago, Illinois, September 1987.

Appendix A**Preliminary Event Tree Analysis**

**Table A-1
Initiating Events for Preliminary Event Tree Analysis**

No	IE ID	INITIATING EVENT DEFINITION	Frequency (yr⁻¹)
1	IE-PTR	Small LOCA - pressure tube rupture (with calandria tube remaining intact)	4.0E-03
2	IE-PCTR	Small LOCA - pressure tube & calandria tube rupture	6.0E-05
3	IE-FBIO	Feeder break	2.0E-03
4	IE-FSB	Feeder stagnation break (with consequential channel rupture)	2.0E-04
5	IE-SWD2	Total loss of one service water division (division 2)	5.0E-02
6	IE-LCL4	Total loss of Class IV power supply to one ACR unit	3.0E-01
7	IE-SCB	Loss of inventory in shield cooling system	4.0E-04
8	IE-MSL3	Small steam discharge causing low deaerator level	1.0E-01
9	IE-FWBS	Symmetric feed water line break upstream of feed water level control valves	2.2E-03
10	IE-FWBA	Asymmetric feed water line break downstream of SG check valve	5.8E-05
11	IE-LOR	Loss of reactivity control leading to uncontrolled power increase	4.24E-02

Notes

- The frequency of the feeder stagnation break event, IE-FSB, is conservatively assumed to be 10% of the feeder break frequency. During the detailed PSA, a best estimate of the feeder stagnation break frequency will be calculated. The frequency of a stagnation break that leads to fuel melting and channel failure is expected to be at least an order of magnitude lower than the 2E-4/yr value above, justifying the exclusion of this event as a design basis event, similar to the pressure tube/calandria tube event.

**Table A-2
Plant Damage States**

PDS 0	Early loss of core integrity at high power and pressure as a result of a failure to shutdown when required.	This PDS is assigned to end states resulting from failure of all shutdown functions when the shutdown is required to mitigate a power-cooling mismatch. The reactor core disassembles at high internal pressure	Severe Core Damage
PDS 1	Late loss of core integrity at decay power starting from high HTS pressure caused by a loss of all primary and backup heat sinks.	Loss of primary heat sinks at HTS high pressure (e.g., loss of FW + SW + RWS make-up to SGs). A small number of channels fail to relieve HTS pressure, but ECC and moderator heat sinks are unavailable. The reactor core disassembles at low internal pressure. The core debris can be retained in the calandria if the shield water heat sink is available.	Severe Core Damage Note: Loss of crash cooldown after a small LOCA is conservatively allocated to PDS1. In reality, the event will lead to fuel channel failure, HT depressurization and emergency coolant injection.
PDS 2	Late loss of core integrity at decay power starting from low HTS pressure caused by a loss of all primary and backup heat sinks.	LOCA + LOECC + loss of moderator heat sink. The reactor core disassembles at low internal pressure. The core debris can be retained in the calandria if the shield water heat sink is available.	Severe Core Damage
PDS 3	Early, widespread fuel and channel damage at decay power starting from low HTS pressure caused by a loss of primary heat sinks + a failure of ECCS.	LOCA + LOECC cause rapid core voiding (e.g., large LOCA + failure of ECIS and LTCS). The moderator heat sink is available to maintain the fuel within the fuel channels, which are deformed but intact.	Limited Core Damage
PDS 4	Late, widespread fuel and channel damage at decay power starting from low HTS pressure caused by a loss of primary heat sinks + a failure of ECCS.	LOCA + LOECC cause slow core voiding (e.g., a small LOCA + failure of ECIS & LTCS or any size LOCA + failure of LTCS). Moderator heat sink is available to maintain the fuel within the fuel channels, which are deformed but intact.	Limited Core Damage
PDS 5	Early, limited fuel damage at decay power starting from low HTS pressure caused by a loss of primary heat sinks.	LOCA with ECCS performing as intended. No temperature-induced fuel failures, but some incipient cladding defects open. All pressure tubes remain intact.	

PDS 6	Late, limited fuel and channel damage at decay power starting from high HTS pressure caused by a loss of primary heat sinks.	A small LOCA (or leak) + a loss of SG cool-down or a loss of all feed water supplies. The HTS voids gradually at a high pressure. A small number of pressure tubes + bellows (or a few fuel channels) fail to depressurize the HTS. The ECIS activates while the fuel temperatures are moderate. The LTCS provides the long-term heat sink. The fuel damage is mainly mechanical.	Limited Core Damage
PDS 7	Early but limited fuel damage caused by a single channel LOCA + containment pressurization.	Inlet feeder or end fitting breaks with ECCS performing as intended. Up to whole-channel FP inventory could be released into the containment.	
PDS 8	Early but limited fuel and channel damage caused by a single channel LOCA + no containment pressurization.	In-core LOCAs (pressure tube rupture + calandria tube rupture) with ECCS and moderator system performing as intended (i.e., no significant steam discharge into containment, FP release into moderator).	
PDS 9	Tritium release	Moderator spills or boiling, but no fuel damage.	

**Table A-3
System Reliability /Unavailability Targets (dependent on DG availability)**

Electric Power Supply Status / Systems' Unavailability	Electric Power Supply (Composite Unav.)	AFW	SWD1&D2	D1SW	MHS	LTC-SDC	DECC	LTC-ECC
Class IV Available	-	3.0E-03	1.0E-05	5.0E-03	5.0E-03	1.0E-02	7.0E-04	5.0E-03
All DGs Available (Class IV lost)	-	6.0E-03	1.0E-05	5.0E-03	8.0E-03	1.0E-02	7.0E-04	5.0E-03
Class IV & 1 DG Unavailable	7.00E-02	1.0E-02	1.0E-03	1.0E-02	1.0E-02	5.0E-02	2.0E-03	8.0E-03
Class IV & 2 DGs Unavailable	7.75E-03	5.0E-02	5.0E-03	5.0E-02	5.0E-02	1.0E-01	1.0E-02	1.5E-02
Class IV & 3 DGs Unavailable	6.60E-04	1.0E-01	1.0E-02	x	1.0E-01	5.0E-01	2.0E-02	5.0E-02
Class IV & 4 DGs Unavailable	5.75E-05	x	x	x	x	x	5.0E-02	x
Class IV Unavailable and 1 SW Division lost			x	x	1.0E-02	x		

Auxiliary Condensate Extraction Pump is going to be supplied from an MCC connected to the Class III "F" (EVEN) bus.

Note: “-” sign means it is not applicable to place a value in that spot;
 “x” sign means the system is unavailable or no credit is given to its function.

Table A-4
System Reliability/Unavailability Targets

System	Acronym	Support Supply Status	Unavailability
Auto De-pressurization Water	ADW	Not dependent of Class IV power supply status	1.0 E-04
Main Feed Water (excludes auxiliary feed water pumps sub-system)	MFW	Class IV power available	3.5 E-03
Feed Water (includes MFW and AFW)	FW	Class IV power available	5.0 E-04
Feed Water (includes MFW and AFW)	FW	One SW Division available; Class IV power available	1.0 E-03
Emergency Feed Water Supply	EFW	Class IV power available	1.0 E-04
Emergency Feed Water Supply	EFW	Class IV power unavailable; Class III DGs all available	1.0 E-04
Emergency Feed Water Supply	EFW	One SG unavailable	7.0 E-04
Consequential Loss of Class IV Power Supply	LCL4	Not applicable	5.0 E-02
Crash Cool (overall Crash Cool unav. – including CC1 + CC2)	CC	Not dependent of Class IV power supply status	1.0 E-05
Condensate System	CND	Class IV power available	5.0 E-04
Auxiliary Condensate Extraction System	ACND	Class IV power unavailable	5.0E-02
Auxiliary feed water or SGs (break) Isolation Failure	AFW-IS	Class IV power available	1.0 E-02
Boiler Pressure Control Cooldown	BPCC	Class IV power available	5.0 E-03
Steam Generator Pressure Relief	SGPR	Class IV available	1.0 E-06
Steam Generator Pressure Relief	SGPR	Class IV unavailable	1.0 E-05
Main Steam Safety Valves failure to open on demand	MSSV	Not dependent of Class IV power status	1.0 E-05

System	Acronym	Support Supply Status	Unavailability
Reserve Water Make-up into the Heat Transport System	RWS-HTS	Not dependent on Class IV power supply status	1.0 E-02
HT pumps seals integrity maintained.	CLPS	Applicable only when pumps are running (Class IV should be available)	8.0 E-05
HT Pumps Trip on High Upper Bearing Temperature	PTHT	Only on sequences in which Class IV power supply is preserved.	5.0 E-03
Liquid Relief Valves and degasser condenser relief valves Fail to Reclose after an HTS Overpressure Transient	CLPRV	Not dependent of Class IV power supply status	4.0 E-06
Reactor Shutdown by SDS1 & SDS2	RS	Not dependent on power supply	1.0 E-06

Appendix B

Event Tree for Feeder Break

Initiating Event	Reactor Shutdown	Support Systems			HTS Makeup		Heat Sink		SEQ.FREQ.	PLANT DAMAGE STATE	SEQUENCE DESIGNATOR	SEQUENCE NUMBER
		No Consequential loss of CL4 Supply	Crash Cooldown	SWD1&D2 (RSW/RCW) System (CL4 available)	HTS Makeup	Long Term Cooling System (ECC function)	FW Supply to SGs	Moderator Acts as Heat Sink				
IE-FBIO	RS	CL4	CC	SWD1&D2	DECC	LTC-ECC	FW	MHS				
<p>The diagram is a fault tree for a Feeder Break event. It starts with the top event 'IE-FBIO' at a frequency of 2.00E-03. This event branches into several paths based on the state of various support systems: <ul style="list-style-type: none"> RS (Reactor Shutdown): Frequency 1.00E-06, leading to sequence IE-FBIO/RS (FBIO10). CL4 (No Consequential loss of CL4 Supply): Frequency 5.00E-02, leading to sequence IE-FBIO/CL4 (FBIO-A). CC (Crash Cooldown): Frequency 1.00E-05, leading to sequence IE-FBIO/CC (FBIO9). SWD1&D2 (SWD1&D2 System): Frequency 1.00E-05, leading to sequence IE-FBIO/SWD1&D2 (FBIO8). DECC (HTS Makeup): Frequency 7.00E-04, leading to sequence IE-FBIO/DECC (FBIO6) and IE-FBIO/DECC/MHS (FBIO7). LTC-ECC (Long Term Cooling System): Frequency 5.00E-03, leading to sequence IE-FBIO/LTC-ECC (FBIO4) and IE-FBIO/LTC-ECC/MHS (FBIO5). FW (FW Supply to SGs): Frequency 5.00E-04, leading to sequence IE-FBIO/FW (FBIO2) and IE-FBIO/FW/MHS (FBIO3). MHS (Moderator Acts as Heat Sink): Frequency 5.00E-03, leading to sequence IE-FBIO/FW/MHS (FBIO3). </p>									1.89E-03	PDS7	IE-FBIO	FBIO1
									9.40E-07	PDS4	IE-FBIO/FW	FBIO2
									4.72E-09	PDS2	IE-FBIO/FW/MHS	FBIO3
									9.45E-06	PDS4	IE-FBIO/LTC-ECC	FBIO4
									4.75E-08	PDS2	IE-FBIO/LTC-ECC/MHS	FBIO5
									1.32E-06	PDS4	IE-FBIO/DECC	FBIO6
									6.65E-09	PDS2	IE-FBIO/DECC/MHS	FBIO7
									1.90E-08	PDS2	IE-FBIO/SWD1&D2	FBIO8
									1.90E-08	PDS1	IE-FBIO/CC	FBIO9
									1.00E-04	CONT'D	IE-FBIO/CL4	FBIO-A
2.00E-09	PDS0	IE-FBIO/RS	FBIO10									

Fig.1 (Feeder Break)

FBIO-A	Class 3 Power				SEQ.FREQ.	PLANT DAMAGE STATE	SEQUENCE DESCRIPTION	SEQUENCE NUMBER
IE-FBIO/CL4 (RS via SDS1/2)	4 DGs available for 24hrs.	3 DGs available for 24hrs.	2 DGs available for 24hrs.	1 DG available for 24hrs.				
IE-FBIO	DG-AV=4	DG-AV=3	DG-AV=2	DG-AV=1				
		9.30E-05	CONTD	IE-FBIO/CL4/UNAV-DGS=0	FBIO-A1			
		6.23E-06	CONTD	IE-FBIO/CL4/UNAV-DGS=1	FBIO-A2			
	7.00E-02 AV-DGS<4	7.04E-07	CONTD	IE-FBIO/CL4/UNAV-DGS=2	FBIO-A3			
	.11 AV-DGS<3	6.05E-08	CONTD	IE-FBIO/CL4/UNAV-DGS=3	FBIO-A4			
	8.60E-02 AV-DGS<2	5.76E-09	PDS1	IE-FBIO/CL4/UNAV-DGS=4	FBIO-1			

Fig.2 (Feeder Break)

FBIO-A1	Heat Sink	Support Systems	PHT Makeup	HTS Makeup	Heat Sink		SEQ.FREQ.	PLANT DAMAGE STATE	SEQUENCE DESIGNATOR	SEQUENCE NUMBER
FBIO/LCL4, all 4-DGs available	Crash Cooldown	SWD1&D2 SW System (CL4 unavail.)	ECC Supply	LT-ECC(Long -Term ECC Supply)	AFW Supply to S/Gs(CL4 unavail.)	Mod. Acts as Heat Sink				
IE-FBIO	CC	SWD1&D2	DECC	LTC-ECC	AFW	MHS				
							9.19E-05	PDS7	FBIO-A1	FBIO-A11
							5.50E-07	PDS4	FBIO-A1/AFW	FBIO-A12
							4.44E-09	PDS2	FBIO-A1/AFW/MHS	FBIO-A13
							4.61E-07	PDS4	FBIO-A1/LTC-ECC	FBIO-A14
							3.72E-09	PDS2	FBIO-A1/LTC-ECC/MHS	FBIO-A15
							6.46E-08	PDS4	FBIO-A1/D-ECC	FBIO-A16
							5.21E-10	PDS2	FBIO-A1/D-ECC/MHS	FBIO-A17
							9.30E-10	NDF	FBIO-A1/SWD1&D2	
							9.30E-10	NDF	FBIO-A1/CC	

Fig.3 (Feeder Break)

FBIO-A2	Heat Sink	Support Systems	HTS Make-up		Heat Sinks		SEQ.FREQ.	PLANT DAMAGE STATE	SEQUENCE DESIGNATOR	SEQUENCE NUMBER
			Dormant ECC	LTC-ECC (Long-Term ECC Supply)	AFW Supply to S/Gs	Mod. Acts as Heat Sink				
FBIO/CL4 & 1-DG unavailable	Crash Cooldown	SWD1&D2 SW System								
IE-FBIO	CC	SWD1&D2	DECC	LTC-ECC	AFW	MHS				
							6.10E-06	PDS7	FBIO-A2	FBIO-A21
							6.10E-08	PDS4	FBIO-A2/AFW	FBIO-A22
							6.16E-10	PDS2	FBIO-A2/AFW/MHS	FBIO-A23
							4.92E-08	PDS4	FBIO-A2/LTC-ECC	FBIO-A24
							4.97E-10	PDS2	FBIO-A2/LTC-ECC/MHS	FBIO-A25
							1.23E-08	PDS4	FBIO-A2/DECC	FBIO-A26
							1.24E-10	PDS2	FBIO-A2/DECC/MHS	FBIO-A27
							6.23E-09	PDS1	FBIO-A2/SWD1&D2	FBIO-A28
							6.23E-11	NDF	FBIO-A2/CC	

Fig.4 (Feeder Break)

FBIO-A3	Heat Sink	Support Systems	HTS Make-up		Heat Sinks		SEQ.PROB.	PLANT DAMAGE STATE	SEQUENCE DESIGNATOR	SEQUENCE NUMBER
FBIO/LCL4, 2-DGs unavailable	Crash Cooldown	SWD1&D2 SW System	Dormant ECC Supply	Long-Term ECC Supply	AFW Supply to S/Gs	Mod. Acts As Heat Sink				
IE-FBIO	CC	SWD1&D2	DECC	LTC-ECC	AFW	MHS				
							6.49E-07	PDS7	FBIO-A3	FBIO-A31
							3.24E-08	PDS4	FBIO-A3/AFW	FBIO-A32
							1.71E-09	PDS2	FBIO-A3/AFW/MHS	FBIO-A33
							9.88E-09	PDS4	FBIO-A3/LTC-ECC	FBIO-A34
							5.20E-10	PDS2	FBIO-A3/LTC-ECC/MHS	FBIO-A35
							6.65E-09	PDS4	FBIO-A3/DECC	FBIO-A36
							3.50E-10	PDS2	FBIO-A3/DECC/MHS	FBIO-A37
							3.52E-09	PDS2	FBIO-A3/SWD1&D2	FBIO-A38
7.04E-12	NDF	FBIO-A3/CC								

Fig.5 (Feeder Break)

FBIO-A4	Heat Sink	Support Systems	PHT Makeup	HTS Makeup	Heat Sink		SEQ.PROB.	PLANT DAMAGE STATE	SEQUENCE DESIGNATOR	SEQUENCE NUMBER
FBIO/LCL4, 3-DGs unavaialable	Crash Cooldown	SWD1&D2 SW (RSW/RCW) System	ECC System	Long-Term ECC Supply	AFW Supply to S/Gs	Moderator Acts as Heat Sink				
IE-FBIO	CC	SWD1&D2	DECC	LTC-ECC	AFW	MHS				
							5.02E-08	PDS7	FBIO-A4	FBIO-A41
							5.02E-09	PDS4	FBIO-A4/AFW	FBIO-A42
							5.58E-10	PDS2	FBIO-A4/AFW/MHS	FBIO-A43
							2.64E-09	PDS4	FBIO-A4/LTC-ECC	FBIO-A44
							2.93E-10	PDS2	FBIO-A4/LTC-ECC/MHS	FBIO-A45
							1.08E-09	PDS4	FBIO-A4/DECC	FBIO-A46
							1.20E-10	PDS2	FBIO-A4/DECC/MHS	FBIO-A47
							6.05E-10	NDF	FBIO-A4/SWD1&D2	
6.05E-13	NDF	FBIO-A4/CC								

Fig.6 (Feeder Break)