AECL EACL

Analysis Report

Generic CANDU Probabilistic Safety Assessment - Methodology

91-03660-AR-001

Revision 0

2002 July

CONTROLLED

2251 Speakman Drive
Mississauga, Ontario
Canada L5K 1B2

Juillet 2002

CONTRÔLÉ

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

AECL EACL

Analysis Report

Generic CANDU Probabilistic Safety Assessment - Methodology

91-03660-AR-001

Revision 0

Prepared by
Rédigé par
P. Santamaura
Point Lepreau Refurbishment

Prepared by
Rédigé par
A. Nainer
Safety Engineering and Environmental Studies

Prepared by
Rédigé par
R.E.B. Henderson
Safety Engineering and Environmental Studies

Prepared by
Rédigé par
S. Aprodu
Safety Engineering and Environmental Studies

Reviewed by
Vérifié par
R. Jaitly, Safety Manager
Point Lepreau Refurbishment

Approved by
Approuvé par
M. Bonechi, Manager
Safety and Licensing, ACR

Approved by
Approuvé par
N. Popov, Manager
Safety Engineering and Environmental Studies

2002 July
CONTROLLED

2251 Speakman Drive
Mississauga, Ontario
Canada L5K 1B2

Juillet 2002
CONTRÔLÉ

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

AECL EACL

Release and Revision History / Liste des documents et des révisions

C939B Rev. 13

Document Details / Détails sur le document

Title / Titre	Total no. of pages / Nbre total de pages
Generic CANDU Probabilistic Safety Assessment - Methodology	384

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°	Date	No./N°	Date				
1	01/08/14	D1	01/08/14	Review and Comment	P. Sartamaura A. Nainer R.E.B. Henderson S. Aprodu	R. Jaitly	M. Bonechi N. Popov
2	02/02/22	D2	02/02/22	Issued for AECL review for export permit	P. Sartamaura A. Nainer R.E.B. Henderson S. Aprodu	R. Jaitly	M. Bonechi N. Popov
3		0	02/07/03	Issued as 'Approved for Use'	P. Sartamaura PS. A. Nainer A.N. R.E.B. Henderson RE S. Aprodu S.A	R. Jaitly RJ	M. Bonechi 04/03 N. Popov

DCS/RMS Input / Données SCD ou SGD

Rel. Proj. Proj. conn.	Project Projet	SI	Section	Serial Série	Sheet Feuille No. N°	Of De	Unit No.(s) Tranche n°
	91	03660	AR	001	1	1	

EXECUTIVE SUMMARY

This document presents the methods and tools that are used in the Generic CANDU® Probabilistic Safety Assessment (GPSA) program at Atomic Energy of Canada Ltd (AECL). The purpose of the program was to develop methodologies and obtain tools that cover full scope Level I and II Probabilistic Safety Assessment (PSA) including external events, to generate a reference analysis to be used as a framework for PSA of future AECL projects and lastly to gain insights into the design of the fully developed reactor products: CANDU 6 and CANDU 9.

In nuclear reactor PSAs, risk is usually defined by the frequency and magnitude of radioactive releases to the environment. A Level I PSA models accident sequences up to the point at which the reactor core either reaches a stable condition or becomes severely damaged, releasing large amounts of radionuclides into the containment. The probabilistic aspects of the analysis focus on the performance and reliability of nuclear plant systems and station staff in response to plant upsets. A Level II PSA examines severe reactor accidents through a combination of probabilistic and deterministic approaches, in order to determine the release of radionuclides from containment, including the physical processes that are involved in the loss of structural integrity of the reactor core.

This report describes methodologies for conducting the following analyses:

1. internal events PSA
2. common cause failure analysis
3. human reliability analysis
4. seismic events PSA
5. fire events PSA
6. flood events PSA
7. Level II PSA

The goals of the GPSA program for the establishment of these methodologies were:

1. to establish procedures, requirements and methods related to CANDU,
2. to develop or acquire analysis tools, including codes and databases,
3. to obtain or develop internationally recognized codes and tools to perform Level II severe core damage consequence analyses for CANDU 6 and CANDU 9 systems, and
4. to develop databases for reference CANDU 6 and CANDU 9 plants, in order to perform severe core damage progression analysis.

This report also describes the steps that are involved in performing a Level II PSA, for which the Modular Accident Analysis Program CANDU (M4C) code was chosen as the consequence

---

analysis code. This code was modified for CANDU 6 and CANDU 9 reactor designs, and this report describes the resulting M4C code.

This report is one of two documents that present an in-depth summary of the methods, assumptions, results and insights of the Generic CANDU Probabilistic Safety Assessment program at Atomic Energy of Canada Ltd. These reports may be used as reference documents for CANDU Probabilistic Safety Assessment practitioners, so that they may compare the assumptions, methods and results of their respective PSAs with those that are used at AECL. This comparison should be particularly applicable to CANDU utilities for which AECL was the Nuclear Steam Plant (NSP) design organization, since there is significant commonality of design between existing CANDU plants and the reference design on which the GPSA is based. The GPSA offers an instrument to assess the safety adequacy of AECL's new reactor designs as well as a basis for existing stations to conduct their PSAs.

ACKNOWLEDGEMENTS

Many staff at AECL participated in the development of methodologies for the Generic CANDU PSA Program. The assistance and contribution of the following staff is gratefully acknowledged:

S. Baset, A. Bujor, H.S. Chiang, T. Hiscock, S.C. How Pak Hing, L. Lee, X. Liu, M.S. Lwin, B. Ly, P. Santamaura, J.S. Smith, S. Petoukhov, T. Ramadan, and W. Vesik.

The direction and guidance of M. Bonechi, R. Jaitly, M. Elgohary, P.M. Mathew, A.H. Stretch, and T.S. Aziz for leading the Generic CANDU PSA Program effort at AECL is gratefully acknowledged.

Acknowledgements for earlier contributions to the setup of the Level 2 PSA program are given to L. Simpson, A. Muzumdar, S. Nijhawan, C.B. So and T. Andres.

Acknowledgements are also given to V.G. Snell, J.M. Hopwood, P.J. Allen, S.K.W. Yu and W. Kupferschmidt for their overall direction and support.

Finally, the assistance of EQE Company for their training courses on fire and seismic events, and of FAI and OPG in the development of the MAAP4 CANDU code is greatly appreciated.

Special thanks to the reviewers and to our technical editor Saulius Fidleris.

ACRONYMS

ABWR	Advanced Boiling Water Reactor
AC	Alternating Current
AECB	Atomic Energy Control Board
AECL	Atomic Energy of Canada Limited
AFW	Auxiliary Feed Water
ALWR	Advanced Light Water Reactor
AOM	Abnormal Operating Manual
ASDV	Atmospheric Steam Discharge Valve
ASEP	Accident Sequence Evaluation Program
ASME	American Society of Mechanical Engineers
ASQ	Accident Sequence Quantification
BE	Basic Event
BFR	Binomial Failure Rate
BHEP	Basic Human Error Probability
BNSP	Balance Nuclear Steam Plant
BOP	Balance of Plant
BSI	Basic Subject Index
BUE/F	Electrical Bus (E or F)
BWR	Boiling Water Reactor
CAFTA	Computer Aided Fault Tree Analysis
CANDU	CANadian Deuterium Uranium
CCDP	Conditional Core Damage Probability
CCF	Common Cause Failure
CCFP	Conditional Containment Failure Probability
CD	Complete Dependence
CDF	Conservative Deterministic Failure
CDFM	Conservative Deterministic Failure Margin
CE	Combustion Engineering
CET	Containment Event tree
CER	Control Equipment Room
CFF	Containment Failure Frequency
CFR	Code of Federal Regulations (US)
C&I	Control & Instrumentation
CIGAR	Channel Inspection and Gauging Apparatus for Reactors
CIS	Containment Isolation System
CN	Component Number
CNSC	Canadian Nuclear Safety Commission
COG	CANDU Owners Group
COMPBRN IIIe	Fire Computer Code
CRO	Control Room Operator
CSA	Canadian Standards Association
CSDV	Condenser Steam Dump Valves
CT	Calandria Tube

CV	Calandria Vessel
CVIS	Containment Ventilation Isolation System
DBE	Design Basis Earthquake
DC	Direct Current
DCC	Digital Control Computers
DCS	Distributed Control System
DG	Diesel Generator
DHC	Delayed Hydride Cracking
DR	Deficiency Report
D/S	Detection/Suppression
ETA	Event Tree Analysis
ECC	Emergency Core Cooling
ECCS	Emergence Core Cooling System
EF	Error Factor
EMFS	Early Manual Fire Suppression
EOP	Emergency Operating Procedure
EPRI	Electrical Power Research Institute
EPS	Emergency Power Supply
EQESRA	Earthquake Computer Code
EWD	Elementary Wire Drawings
EWS	Emergency Water Supply
F/M	Fuelling Machine
FD	Fire Detection
FDS	Fire Damage State
FDS	Flood Damage State
FM	Failure Mode
FMEA	Failure Mode and Effects Analysis
FO	Field Operator
FRS	Floor Response Spectrum
FS	Flow sheet
FSAR	Final Safety Analysis Report
FW	Feed Water
G1FW	Group One Feed Water
G1SW	Group One Service Water
G2	Gentilly 2 NGS
G2FW	Group Two Feed Water
G2SW	Group Two Service Water
GPSA	Generic CANDU Probabilistic Safety Assessment
GRS	Ground Response Spectrum
GSI	General Subject Index
GSS	Guaranteed Shutdown State
HCLPF	High Confidence of Low Probability of Failure
HEP	Human Error Probability
HPECC	High Pressure Emergency Core Cooling
HPGL	Hewlett Packard Graphics Language

HPI	ECCS High Pressure Injection
HRA	Human Reliability Assessment
HS	Hand Switch
HT	Heat Transport
HTS	Heat Transport System
HVAC	Heating Ventilation and Air Conditioning
HX	Heat Exchanger
I&C	Instrumentation and Control
I/A	Instrument Air
IAEA	International Atomic Energy Agency
IAS	Instrument Air System
IEEE	Institute of Electrical and Electronic Engineers
IE	Initiating Event
IBFI	Intermittent Buoyancy Induced Flow
ILD	Instrument Loop Diagram
INTEC	Electrical Connections Wiring Computer Code
IPE	Individual Plant Examination
IPEEE	Individual Plant Examination for External Events
LAC	Local Air Cooler
LCV	Level Control Valve
LED	Light Emitting Diode
LLNL	Lawrence Livermore National Laboratory
LMFS	Late Manual Fire System
LOCA	Loss of Coolant Accident
LOECC	Loss of Emergency Core Cooling
LPI	ECCS Low Pressure Injection
LRV	Liquid Relief Valve
LWR	Light Water Reactor
MAAP	Modular Accident Analysis Program
MAFS	Manual Actuation of Fire Spray System
MCCI	Molten Core Concrete Interaction
MCR	Main Control Room
MCRDE	MCR Design Earthquake
MFG	Multiple Failure Group
MFW	Main Feed Water
MGL	Multiple Greek Letter
MM	Maintenance Manual
MMI	Man Machine Interface
MOV	Motor Operated Valve
MPI	ECCS Medium Pressure Injection
MS	Microsoft
MSIV	Main Steam Isolation Valve
MSL	Main Steam Line
MSLB	Main Steam Line Break
MSSV	Main Steam Safety Valve

MTTR	Mean Time To Repair
MV	Motorized Valve
NB	New Brunswick
NDF	Not Developed Further
NEA	Nuclear Energy Agency
NGS	Nuclear Generating Station
NHEP	Nominal Human Error Proabability
NI	Nuclear Island
NPP	Nuclear Power Plant
NSP	Nuclear Steam Plant
NSQ	Non-Seismically Qualified
NSSS	Nuclear Steam Supply System
NU	Natural Uranium
OM	Operating Manual
OPG	Ontario Power Generation (formally OH - Ontario Hydro)
ORG	Operator Response Guidelines
P&IC	Pressure and Inventory Control
PAM	Post Accident Monitoring
PC	Personal Computer
PDS	Plant Damage State
PGA	Peak Ground Acceleration
PHWR	Pressurized Heavy Water Reactor
PL	Panel
PLG	Pickard, Lowe and Garrick
PLGS	Point Lepreau Nuclear Generating Station
PPO	Principal Power Operator
PRA	Probability Risk Assessment
PRESCON2	Containment Pressure Computer Code
PRV	Pressure Relief Valve
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor
PT	Pressure Tube
PV	Pneumatic Valve
PWR	Pressurized Water Reactor
RB	Reactor Building
RAB	Reactor Auxiliary Building
RC	Release Category
RCP	Reactor Coolant Pump (LWR)
RCW	Recirculating Cooling Water
RF	Recovery Factor
RFI/EMI	Radio Frequency Interference / Electro-Magnetic Interference
RIH	Reactor Inlet Header
RLE	Review Level Earthquake
RM	Release Mode
ROH	Reactor Outlet Header

RRS	Required Response Spectrum
RS	Reactor Shutdown
RSW	Raw Service Water
RTD	Resistance Temperature Device
RV	Relief Valve
RWS	Reserve Water System
RWT	Reserve Water Tank
SAIC	Science Applications International Corporation
SAR	Safety Analysis Report
SBO	Station Blackout
SCA	Secondary Control Area
SCD	Severe Core Damage
SCDF	Severe Core Damage Frequency
SCL1	Loss of Group 1 Class I Power
SCL3	Loss of Class III Power
SDC	Shutdown Cooling
SDCS	Shutdown Cooling System
SDE	Site Design Earthquake
SDG	Safety Design Guide
SDM	Safety Design Matrix
SDS1/2	Shutdown System One / Two
SER	Significant Event Report
SERA	System and Equipment Reliability Analysis
SG	Steam Generators
SGPC	Steam Generator Pressure Control
SGPR	Steam Generator Pressure Relief
SHA	Seismic Hazard Analysis
SL	Small LOCA
SMA	Seismic Margin Assessment
SRP	Systematic Review of Plant
SRPD	Systematic Review of Plant Design
SRSS	Square Root of Sum Squares
SRV	Safety Relief Valve
SRWFW	Loss of Service Water and Feedwater
SS	Shift Supervisor
SSE	Safe Shutdown Earthquake
SSEL	Safe Shutdown Equipment List
SSM	Safety System Monitor
SV	Solenoid Valve
SW	Service Water
TB	Turbine Building
TCV	Temperature Control Valve
TC	Type Code
TC	Test Computer
T/G	Turbine/Generator

THERP	Technique for Human Error Rate Prediction
TRS	Test Response Spectrum
TS	Technical Specification
UPM	Unified Partial Method
UPS	Uninterruptible Power Supply
USNRC	United States Nuclear Regulatory Commission
VDU	Video Display Unit
VIS	Ventilation Isolation System
ZD	Zero Dependence
ZI	Position Indicator

TABLE OF CONTENTS

SECTION **PAGE**

TABLE OF CONTENTS

SECTION **PAGE**

TABLE OF CONTENTS

TABLE OF CONTENTS

SECTION **PAGE**

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLES

TABLE OF CONTENTS

SECTION **PAGE**

FIGURES

TABLE OF CONTENTS

SECTION **PAGE**

APPENDICES

1. INTRODUCTION

The Generic CANDU® Probabilistic Safety Assessment (GPSA) Program was undertaken by Atomic Energy of Canada Ltd (AECL) in 1998 to provide the bases for Level I and II Probabilistic Safety Assessment (PSA) studies of future AECL projects. There were four main objectives:

1. to develop a methodology that would cover the full scope of Level I and II PSA,
2. to acquire the tools and develop models for application of the methodology,
3. to generate a reference analysis that could be used as a framework by future AECL projects, and
4. to gain important insights into the design of the fully developed AECL's reactor products, CANDU 6 and CANDU 9.

In nuclear reactor PSAs, risk is usually defined by the frequency and magnitude of radioactive releases to the environment. A Level I PSA models accident sequences up to the point at which the reactor core either reaches a stable condition or becomes severely damaged, releasing large amounts of radionuclides into the containment. The frequency of this latter condition is of primary interest, because it provides a measure of the design robustness of the normal and emergency core cooling systems. The probabilistic aspects of the analysis focuses on the performance and reliability of nuclear plant systems and station staff in response to plant upsets.

A Level II PSA examines severe reactor accidents through a combination of probabilistic and deterministic approaches, in order to determine the release of radionuclides from containment, including the physical processes that are involved in the loss of structural integrity of the reactor core. The probabilistic part of the analysis focuses on the performance reliability of nuclear plant containment systems. This information is synthesized with Level I PSA, in order to derive the release frequencies of different release categories from the plant containment system. The deterministic part of the analysis focuses on the physical processes that occur as the plant status progresses through the various stages of a severe accident. This enables the estimation of the types and quantities of radionuclides that could be released in the unlikely event of containment failure.

For CANDU, the general approach at AECL has been to use the Level I PSA to derive the frequencies of sequences that lead to severe core damage - a state in which there is a widespread loss of core structural integrity subsequent to coolant voiding both within and outside the reactor fuel channels. The first step in establishing these frequencies is to determine all of the credible initiating events that require automatic or manual reactor shutdown and decay heat removal for a defined mission period. From this point, the PSA uses fault tree and event tree techniques to develop the plant response up to either the final steady state conditions, or the onset of severe core damage.

The events considered in the Level I PSA can include both internal and external events. Internal events are primarily events that are caused by random failures of process equipment, system piping within the plant. Internal events also include internal fire and internal flood events. External events are generally events that occur due to causes that are external to the plant (e.g., earthquake, tornado, external flood, etc.).

Another area within the scope of the Level I PSA is the analysis of events that occur while the plant is already shut down. During planned outages, various safety-related systems may be partly or fully unavailable due to maintenance. As a result, any event that leads to a loss of the primary heat sink while the reactor is shut down may have a non-negligible risk of developing into a severe accident. A shutdown state PSA systematically identifies the plant configurations that are possible, and quantifies the frequency of severe core damage for each configuration.

The development of the methodology was the first step in the implementation of the program. From the start it was decided that the methods should be based on internationally accepted practices and procedures. While the methods for the analysis of internal events were generally well established and had been applied already to various projects, other PSA areas required to be tackled for the first time at AECL. These areas included some Level I enhancements (optimised human reliability analysis, common cause failure analysis, seismic, fire and flood analysis), and the Level II component of the PSA, i.e., the analysis of severe core damage progression and containment response.

In parallel to the development of the methodology, tools were acquired to perform the new analyses. They included computer codes for the probabilistic analysis of fires and earthquakes and for the analysis of the integrated plant response to severe core damage accidents. In particular for the latter analysis, the Modular Accident Analysis Program (MAAP4) CANDU (M4C) code was acquired from Electrical Power Research Institute (EPRI) through a sublicense with Ontario Power Generation (OPG). Some of these tools are described in the relevant Sections for illustrative purposes only. Any equivalent computer code or tool is acceptable.

One of AECL's goals has been to develop expertise in the Level I and Level II PSA aspects described above. The framework under which this has been achieved is the Generic CANDU PSA Program, as described in the following section.

There are two reports which describe the GPSA program:

1. this report, which presents the CANDU methodology for analysing internal and external events, and
2. a report, which discusses the reference analysis of the CANDU 6 and CANDU 9 systems for specific events (Reference 1-1).

This report is one of two documents that present an in-depth summary of the methods, results and insights of the Generic CANDU Probabilistic Safety Assessment program at AECL. These reports are intended to be reference documents for CANDU PSA practitioners, so that they may compare the assumptions and methods of their respective PSAs with those that are used at AECL. This comparison should be particularly applicable to CANDU utilities for which AECL was the Nuclear Steam Plant (NSP) design organization, since there is significant commonality

of design between existing CANDU plants and the reference design on which the GPSA is based. The GPSA offers an instrument to assess the safety adequacy of AECL's new reactor designs as well as a basis for existing stations to conduct their PSAs.

1.1 Scope

The GPSA was undertaken at AECL, in order to perform Level I and Level II PSA for internal events, shutdown events, internal fires, internal flooding and specific external events - earthquakes. These events were selected based on international standards, their prevalence in a number of international PSA studies, and because they are of generic interest for CANDU PSA. The intent of the program has not been to perform detailed assessments for every initiating event, but rather to establish PSA methodologies that are consistent with the current international state-of-the-art, and to apply them to those areas that were deemed to be most critical in prior PSA analyses. Therefore, the GPSA methodologies are based on a number of source PSA documents, using relevant past AECL PSA work, and adding new analyses either for events that were not previously considered, or to replace previous analyses, which had become outdated.

The focus of the GPSA has been to examine areas requiring extension of the analysis scope or upgrading of the analysis methods used in previous AECL's PSA studies. With this focused approach, the GPSA has necessarily been developed on "base" versions of AECL's two main reactor products: the CANDU 6 and CANDU 9 designs. The CANDU 6 (700 MWe class) system is AECL's most known design for a single-unit containment pressurized heavy water reactor (PHWR). Currently, eleven CANDU 6 units are in operation or are under construction around the world. The CANDU 9 system is a new, larger PHWR design (900 MWe class), and contains a number of advanced features that enhance plant operability and safety.

1.2 Report Structure

This report is divided into 12 sections. Section 1 is the introduction. Section 2 provides a brief overview of the generic CANDU design. Section 3 provides a general overview of PSA methodology. Section 4 deals with internal events, Section 5 with dependent failure analysis, Section 6 with human reliability analysis, Section 7 with seismic events PSA, Section 8 with fire events PSA, Section 9 with flood events PSA, and Section 10 with Level II PSA. Section 11 contains report conclusions and finally Section 12 contains a glossary of terms. There are five Appendices which deal with internal event, seismic fragility analysis, a fire PSA example, a flood PSA example and a general description of CANDU features.

References, tables and figures are provided at the end of each section.

There is no separate methodology for the shutdown PSA as it basically follows the same procedure as the internal PSA. However, for the shutdown PSA special attention must be paid to manual operator actions, configuration of the systems, maintenance practices and available heat sinks.

The GPSA methodology is sufficiently general to apply to both the CANDU 6 and CANDU 9 designs, except in a few cases, where differences are explained explicitly. As well, the

methodology can apply to future designs. The methodology includes analysis techniques developed at AECL, as well as descriptions of internationally accepted approaches that AECL has adopted.

1.3 References

1-1. AECL, 2002, Generic CANDU Probabilistic Safety Assessment – Reference Analysis, AECL Report 91-03660-AR-002.

2. DESCRIPTION OF CANDU DESIGN

2.1 Introduction

The CANDU reactor is a nuclear power plant (NPP) of the pressure tube type, which utilizes heavy water as a coolant and as a moderator. In common with other thermal power plants, nuclear fuel produces heat, which is subsequently converted into electrical energy. With the CANDU design, the fission reaction in the natural uranium (NU) fuel produces heat that is removed by a flow of pressurized heavy water coolant. This heat is transferred to ordinary water in steam generators (SGs) to produce steam, which drives a turbine and an electrical generator. Most of the electricity produced is supplied through a distribution grid to end-consumers while a small fraction is used to drive equipment in the plant.

Some of the design features and characteristics of the CANDU reactor include:

- a reactor core that comprises several hundred small diameter fuel channels, rather than one large pressure vessel;
- heavy water (D_2O) is used as moderator and coolant;
- separate low pressure moderator and high pressure fuel cooling systems;
- on-power refuelling;
- reactivity devices that are located in the cool low pressure moderator and are not subjected to high temperatures or pressures;
- natural uranium fuel or other low fissile content fuel;
- reduced consequences due to accidental reactivity fluctuations—excess reactivity available from the fuel is small and the relatively long lifetime of prompt neutrons in the reactor precludes rapid changes in power levels; and
- two fully capable safety shutdown systems that are independent from each other and from the reactor regulating system.

All CANDU power plants follow the same fundamental principles, although there may be some significant design differences (i.e., vacuum building for multi-unit plants). The reference CANDU 6 design used for the purpose of the GPSA is a typical recent CANDU 6 design implemented according to current regulatory requirements, codes and standards.

A more detailed description of CANDU 6 reactor is presented in Appendix E.

A typical CANDU Nuclear Steam Supply system (NSSS) is presented in Figure 2-1.

2.2 Safety Systems

2.2.1 Overall Requirements

A fundamental requirement of the CANDU safety design is to provide complete physical separation and functional independence of the special safety systems from the process systems and from each other.

A brief description of the CANDU safety systems is presented below.

2.2.2 Safety Grouping

To provide defence against low probability incidents such as local fires or missiles (e.g. turbine blades), the station safety systems and safety support systems are separated into two groups that are functionally and physically independent of each other. Each group is designed to perform the following functions:

- shut down the reactor;
- remove decay heat from the reactor;
- supply the necessary information for post-accident monitoring.

The following systems provide these safety functions:

- SDS1 in Group 1 and SDS2 in Group 2, which shut down the reactor;
- the process systems, including normal electric power and service water systems in Group 1 and the emergency power supply and emergency water supply systems in Group 2 to remove decay heat;
- the main control room or the secondary control area, which is used for post-accident monitoring.

2.2.3 Shutdown Systems

There are two “full capability” reactor shutdown systems, each capable of shutting down the reactor during any postulated accident condition.

The two shutdown systems are functionally and physically independent of each other and of the reactor regulating system, in the following manner:

- Functional independence is achieved by utilizing different shutdown principles i.e.: solid shutoff rods for SDS1 and direct liquid poison injection into the moderator for SDS2.
- Physical independence of the shutdown systems is achieved by positioning the shutoff units vertically through the top of the reactor and by positioning the poison injection tubes horizontally through the sides of the reactor.

2.2.4 Emergency Core Cooling System

The emergency core cooling system (ECCS) provides ordinary water to the heat transport system (HTS) to compensate for the heavy water coolant lost in a postulated loss-of-coolant accident (LOCA) and recirculates (and cools) the heavy water/light water mixture that collects in the reactor building floor to the reactor headers in order to maintain fuel cooling in the long term.

2.2.5 Backup Decay Heat Removal (Moderator Heat Sink)

In the very unlikely event that the ECCS fails during or following a LOCA, decay heat is transferred from the fuel to the moderator by radiation and conduction.

2.2.6 Containment

Containment comprises a number of systems that operate to provide a sealed envelope around the reactor systems if an accidental radioactivity release occurs from these systems. The following structures and systems form the containment system:

- a lined, post-tensioned concrete containment structure;
- an automatic dousing system (CANDU 6) or a vacuum building for multi-unit stations;
- air coolers;
- a filtered air discharge system for multi-unit stations;
- access airlocks;
- an automatically initiated containment isolation system; and
- hydrogen ignitors / recombination units.

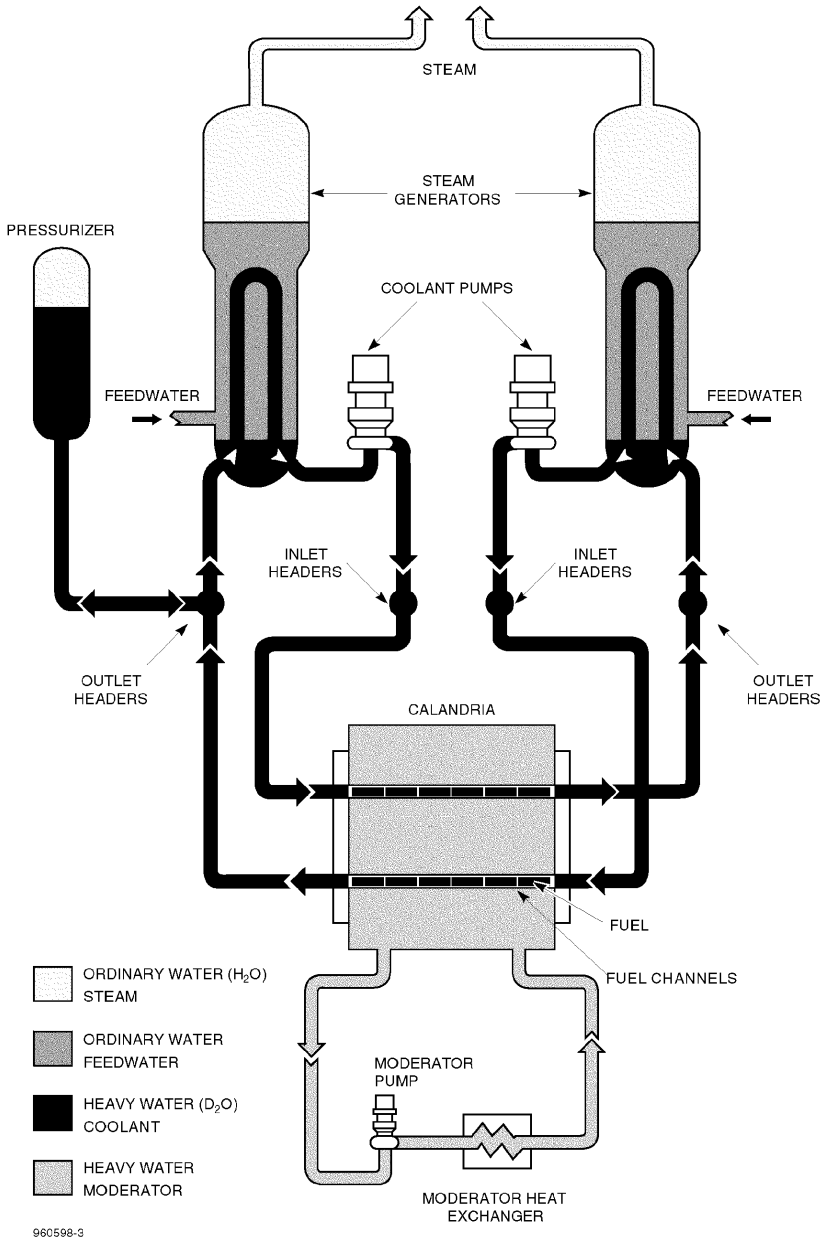


Figure 2-1 CANDU Nuclear Steam Supply System

3. PSA METHODOLOGY - GENERAL

3.1 Introduction

A PSA is an analytical technique used to integrate the many different aspects of design and operation in order to assess the safety of a particular facility and in order to develop an information base for analyzing plant-specific and generic issues. In particular, a PSA is used to determine core damage frequency and risk to the public.

If performed during the initial plant design, a PSA can be used to aide in the designer's understanding of the safety significance of plant design features and to optimize the design.

The adequacy of plant design and operation is assessed by identifying potential accident sequences that dominate the risk and by establishing the features of the plant that contribute most to the dominant accident sequences. These plant features may be potential hardware failures, common-mode failures, human errors during testing and maintenance, or procedural inadequacies leading to human errors.

PSAs vary widely in scope, depending on the available time and resources, as well as the purpose of the study. Depending on the objectives, PSAs may range in scope from an analysis of engineered systems to a full risk assessment. For this reason, PSAs have been divided into three levels as described in Reference 3-1, i.e.: Levels I, II and III.

A brief description of the analysis tasks covered in each of these levels is given below.

a) Level I - System Analysis

   A Level I PSA consists of the identification and quantification of accident sequences, component data and human reliability. It includes an analysis of plant design and operation, with emphasis placed on the accident sequences that lead to core damage, their basic causes and their frequencies. A Level I PSA does not investigate the frequency or mode of containment failure, or the consequences of radionuclide releases. Internal events, internal fire, internal floods and seismic events are included.

b) Level II - System and Containment Analysis

   A Level II PSA consists of an analysis of the physical processes of an accident (timing and magnitude of radioactive release) and the response of the containment, in addition to the analysis performed in a Level I PSA. A Level II PSA predicts containment failure modes, as well as the frequency and inventory of radionuclide releases to the environment at the containment boundary. While not providing a full risk assessment, some insight into risk is provided by the relative frequencies of various release categories.

c) Level III - Consequence Analysis

   A Level III PSA includes an environmental transport and consequence analysis. It analyzes the transport of radionuclides through the environment and assesses the public health risk and economic consequences of the accident, in addition to performing the tasks of a Level II PSA.

Figure 3-1, which is based on Figure 2-1 of Reference 3-1, gives an overview of the PSA process.

As explained in Section 1, Shutdown PSA is similar to internal PSA and is not further discussed.

Some of the CANDU PSA terms used are:

Severe accident—an accident, following which core heat removal by "normal" means is unavailable, due to initial or consequential failures of systems and structures. The normal design basis heat removal systems are the primary HTS, the shut down cooling system (SDCS) and the ECCS.

Example: A LOCA + LOECC is classed as a severe accident in a CANDU reactor, but does not lead to SCD if the moderator heat sink is available. These events have moderate fuel temperature excursions (i.e.: peak temperatures well below the melting point of core materials) and only a small, insignificant release of volatile fission products from the damaged core.

Severe core damage accident — Severe core damage requires a loss of HTS coolant, the failure of ECC injection and a loss of the moderator cooling system. These events lead to core heat-up, the disassembly of channels into debris and high releases of fission products.

Example: A LOCA + LOECC, combined with a failure of the moderator as a heat sink is a severe accident that leads to SCD.

Loss of core structural integrity—a loss of heat sinks that leads to core damage involving multiple fuel channel failures.

Fuel channel failure—the failure of the pressure tube (PT) and the calandria tube (CT).

Plant damage state—a group of releases into containment that include severe accident/core damage sequences that have similar characteristics, with respect to severe accident progression and containment performance.

Containment envelope—comprises the reactor building, sealed penetrations and closed and open penetrations. All open penetrations are part of the containment isolation system. An intact containment assumes that the reactor building perimeter wall is intact and that the main and auxiliary airlocks and the irradiated fuel transfer room are closed and intact

3.1.1 Scope

The scope of any PSA depends on the requirements of the project for which it is performed. In general, a Level I PSA for internal events that may be used as input to a Level II PSA involves tasks (a) through (l), below. Seismic events analysis is briefly described in Section 7. The fire and flood events are described in Sections 8 and 9, respectively. The Level II methodology for containment analysis and containment event trees is presented in Section 10.

The following tasks are involved in an internal events PSA (also applicable to internal fire, internal flood and seismic PSA):

a) Collecting Plant Information

b) Initiating Event Analysis
c) Event Tree Development
d) System Reliability Analysis
e) Dependent Failure Analysis
f) Human Reliability Analysis
g) Data Base Development
h) Accident Sequence Quantification
i) Plant Damage State Analysis
j) Uncertainty and Sensitivity Analysis
k) Quality Assurance
l) Reporting of Results

3.1.2 Acceptance Criteria

3.1.2.1 Frequency/Dose Criteria

For the recent CANDU 6 design, Table 1 of Reference 3-2 provides a minimum list of generic initiating events (accidents) that are required to meet the reference dose limits specified in Table 2 - Safety Analysis Class/Consequence Table, Reference 3-2. All of these events require safety analysis and are called design basis events. Reference 3-2 does not list any severe core damage (SCD) events in Table 1. Severe core damage events are beyond design basis accidents in that the core structural integrity is lost. Severe core damage events lead to core heat-up, the disassembling of channels into debris and a high release of fission products.

Frequencies vs dose criteria listed by class are described in Reference 3-3 for CANDU plants. The five classes are listed in decreasing order of the expected frequency with Class 1 events being the most likely and Class 5 being the least likely to occur. This information is also shown graphically in Figure 3-2 of Reference 3-3. These five classes of events are considered to be design basis events.

3.1.2.2 Severe Accident/Severe Core Damage Frequency

PSA methods are used to quantify accident sequences and to obtain a frequency of SCD due to internal and external initiating events. For the CANDU 6 and CANDU 9 designs, the following design targets are to be used for the maximum frequency of individual accident sequences:

- 10^{-5}/yr for any severe accident. A severe accident is defined as an accident following which core heat removal by the normal and emergency engineered heat removal systems is unavailable due to initial or consequential failures of these systems. Sequences with failure of the ECCS, but with the moderator heat sink available, are included in this category.

- 10^{-6}/yr for any severe core damage accident. These accidents are the subset of severe accidents in which there is a widespread loss of core structural integrity due to voiding both within and exterior to the fuel channels. Sequences with failure of all design basis heat removal systems, including the moderator heat sink, are comprised in this category.

These numbers represent targets only and are not minimum requirements. Design changes may be proposed if these targets are exceeded, but the minimum performance required of the design is based upon the summed severe core damage frequency, as discussed below.

Targets for the summed frequency of SCD accidents have also been established, based primarily on the United States Nuclear Regulatory Commission (USNRC) and the International Atomic Energy Agency (IAEA) safety objectives for operating nuclear power plants. The USNRC [3-4] has a safety objective of 10^{-4}/yr for the core damage frequency goal, which is derived from the NRC's safety goal and associated quantitative health objectives (0.1% of overall risk). The IAEA INSAG 3 [3-5] also has 10^{-4}/yr as the core damage frequency target for operating reactors.

Safety objectives should be set consistent with attaining very low probabilities of severe core damage accidents and of large releases of radioactive materials to the environment. Safety targets for summed severe core damage frequency for internal, internal flood, fire and shutdown state events for CANDU 6 designs is $3x10^{-5}$/yr. Safety targets for summed severe core damage frequency for internal, internal flood, fire and shutdown state events for new CANDU designs such as CANDU 9 is $3x10^{-6}$/yr. For common cause events, such as earthquakes that are affected by large uncertainties, success path assessments based on design margins may be used.

3.1.3 Initial Information Collection

PSAs are broad, integrated studies that require large amounts of information. Naturally, the information that is required depends on the scope of the analysis. For most studies, this will entail gathering information on all aspects of the design of the plant being modelled, the environmental and seismic conditions of the site, reliability data for the plant's components and previous operating experience data from the plant of interest or other CANDU plants. While this is by no means an exhaustive listing of what is needed to complete this task, the following types of documentation provide much of the necessary background information:

a) CANDU system design manuals,

b) CANDU safety design guides and safety analysis basis documents,

c) CANDU safety analysis reports,

d) CANDU system flow sheets (FS) and elementary wiring diagrams (EWD),

e) CANDU equipment technical specifications and

f) Significant events reports.

3.2 Internal Events PSA

Internal events are always considered in a PSA. Internal events that lead to abnormal situations in the plant may arise from random failures of equipment or from components of systems in the plant. Loss of Class IV electrical power is also considered as an internal event. Generally, internal events are divided into two categories: (1) events causing LOCAs or small heat transport leaks and (2) transient events, such as the loss of feedwater system, the loss of in-support systems (e.g., service water or instrument air) and the loss of moderator or end shield cooling systems. These events all have a potential to release radionuclides. The PSA models mitigating systems that prevent these releases, including special safety systems, such as emergency core cooling and containment.

Internal fires and internal flooding may be of significance in quantifying generic CANDU 6 or CANDU 9 plant risk and therefore, methodologies for their evaluation will be developed for application on specific projects. An overview of the method by which these events are analysed is provided in the following sections. The detailed methodology is described in Sections, 8 and 9 for fire and flood events, respectively.

3.3 External Events Analysis

External events, which can be analysed as part of a PSA, include common cause events such as external fires, earthquakes, external floods, winds/tornadoes, transportation accidents and other site-specific external hazards. The term “external events” refers to events that are external to the systems performing safety functions for the plant. Therefore, they include events that are external to the plant (e.g., external fires or floods and earthquakes).

Each of these events may be considered in a PSA, depending on the objectives and scope of the study. Typically, many of these events are screened out from further analysis based on their low probability of occurrence or they are examined qualitatively, rather than quantitatively. However, well-developed quantitative techniques do exist for seismic events. Seismic events are expected to be of significance in quantifying generic CANDU 6 or CANDU 9 plant risk and therefore, methodologies for their evaluation will be developed for application on specific projects. An overview of the method by which these events are analysed is provided in the following sections. The detailed methodology is described in Sections 7 for seismic events.

For external events, the plant damage states, uncertainty analysis, sensitivity analysis, input to Level II PSA, quality assurance and reporting of results are similar to the internal events PSA, as described in Section 4.

3.3.1 Seismic PSA

Earthquakes of sufficient magnitude will disrupt the power operation of a plant and may require operator actions and the operation of safety related systems to ensure that the plant is brought to a stable state. Since earthquakes are “common cause” events, which may cause both active and passive redundant component failures, the potential exists for significant plant damage at non-negligible frequencies. This is dependent on the level of seismic design in the plant and the

seismic hazard of the specific site. Seismic PSA is a useful tool to assess the design in terms of the seismic-induced severe core damage frequency and it can reveal optimal design (e.g., in equipment anchorage), which can be optimized for plant safety. The methodology for conducting a seismic PSA is described in Section 7. The following general steps illustrate the process:

- A seismic hazard curve, which expresses the frequency of occurrence of various earthquake levels for the site, is developed. The level of the earthquake is assessed in terms of a seismic parameter, such as the peak ground acceleration.
- The important safety functions that follow a seismic event are identified. From this information, a seismic equipment list is developed to encompass all of the equipment for which seismic-induced failures might affect these safety functions. Some systems, particularly in the balance of plant (BOP), might be assumed to be failed, in order to reduce the systems analysis effort.
- A seismic walk-down is performed at the plant, during which the components on the seismic equipment list are examined as installed. In particular, the component anchorage, spatial interactions with surrounding structures and equipment and the potential for seismic-induced fires and flooding are areas of concern. Based on the results of the walk-down, many components on the equipment list can be screened out from detailed analysis if they are not expected to be risk-significant.
- Fragility curves are calculated for those structures and equipment that are not qualitatively or quantitatively screened out. These curves express the components' probabilities of failure vs a seismic parameter such as the peak ground acceleration.
- A seismic event tree is developed in which the top event success and failure probabilities are based on simplified seismic fault trees. The probabilities for each equipment failure event in the fault trees will be based on a fragility curve. Human errors will be quantified using a special human reliability analysis methodology that is specific to seismic events.
- The seismic event tree is integrated with the seismic hazard curve to obtain the frequencies of various seismic damage states. For each sequence that does not directly lead to core damage, the conditional core damage probability (CCDP) is then calculated using an appropriate internal events event tree, with appropriate dependencies being taken into account. This process ensures that random, non-seismic failures are included in the analysis. The seismic damage state frequency multiplied by the CCDP gives the seismic severe core damage frequency (SCDF) for a given sequence. A total seismic SCDF may be then calculated.

3.4 Internal Fire PSA

Like a seismic event, fires that are internal to a nuclear power plant can potentially cause multiple failures in safety-related systems, therefore, fire can be a risk-significant event. The fire PSA is used to quantify the risk in terms of SCDF taking into account the location-based frequency of fire occurrence, the impact on safety-related equipment, the possible fire progression pathways and the capabilities of fire suppression systems. The detailed

methodology for fire PSA is described in Section 8. The following constitutes an overview of the activities that are involved for fire PSA:

- Fire event data are collected to establish location-based and component-based fire initiation frequencies. Sources of data include generic US experience, screened for CANDU applicability, as well as CANDU significant event reports (SERs).
- The plant is conceptually divided into "fire zones" and "fire areas", usually based upon the location of barriers to fire propagation. A database is constructed that lists the physical parameters of each zone, including its location in the plant, its fire rating and any fire progression pathways to other zones.
- The safety-related components and other components that are credited in the internal events PSA, and that would be affected by fire in each zone, are documented. This information can be gained by consulting layout drawings and by performing a walk-down of the plant under analysis. The mitigating systems and features of each zone, such as automatic fire suppression systems, are identified. The amount of combustible material in each fire zone is also established.
- Hazard scenarios for the various fire zones are constructed. Essentially, this step gathers the information collected on the various fire zones and identifies the fire sources and describes the fire's potential effects. Scenarios may be qualitatively screened from further analysis, based on a variety of reasons. If, for example, fire in an area does not cause a demand for plant shutdown or the area does not contain any safety-related equipment, a scenario might be screened out. Other scenarios might be screened out on the basis of small volumes of combustible materials in an area. The intention of the screening is to focus analysis efforts on the critical areas of the plant.
- For those scenarios that are not screened out, fire initiating event frequencies are established based on the amount and type of fire sources in the area. The generic/CANDU-specific component-based data are used for this task, in which the total fire frequency for each component type is apportioned to the various fire zones.
- Quantitative screening of the fire scenarios is performed by assuming that all of the safety-related equipment in the area is damaged, including any cables that lead to equipment in other areas. By modifying the relevant fault tree/event tree models, the fire-induced SCDF for each scenario can be calculated, such that both fire-induced and random failures are taken into consideration.
- By performing further analysis to eliminate conservatisms, the results for some scenarios may be further refined. The fire growth and propagation is modelled, using a code such as COMPBRN, in order to obtain a more realistic estimate of the effects of a fire on the safety-related components in the zone. The internal events plant models are re-evaluated using this updated information to obtain core damage frequencies. The probabilities of non-suppression and any human recovery actions that might be taken are factored into the analysis.
- Based on the frequencies obtained from the detailed and screening analyses, a total fire-induced SCDF may be calculated.

3.5 Internal Flooding PSA

Another "common cause" initiator, is a flood within the plant. Flooding can cause system/component failures by submerging equipment, by spray impact on equipment, or by cutting off the water supply to safety-related systems. Much of the methodology for quantifying the SCDF, due to internal floods, is similar to that for internal fires. The methodology for flood PSA is described in Section 9. The following general steps are involved:

- Flood event data are collected to establish building-component-based flood frequencies. The term "building-component-based" means that the frequencies are for a given type of component in a given building (e.g., turbine building, reactor building). Sources of data include generic US experience, screened for CANDU applicability, as well as actual CANDU Significant Event Reports (SERs).
- Possible flood areas in the plant are identified. Information on each location is collected in a database and includes the flood sources, drainage paths to other locations, flood detection/mitigation equipment and the safety-related equipment that is affected by flooding in the area. Much of the information is obtained from plant layout drawings and a plant walk-down. It is also important to estimate the dimensions of the flood area and the fraction of the total volume that is occupied by equipment. This data can be used later in detailed analyses.
- Hazard scenarios for the various flood locations are constructed. Essentially, this step gathers the information collected on the various areas and formally describes the potential effects of flooding and the various sources. The scenarios should consider the worst case impact on the equipment in the location. Scenarios may be qualitatively screened from further analysis, based on a variety of reasons. If, for example, flooding in an area does not cause an initiating event or the area does not contain any safety-related equipment, then a scenario might be screened out. The intention of the screening is to focus the analysis efforts on the critical areas of the plant by examining worst case scenarios only.
- For those scenarios that are not screened out, flood initiation frequencies are established, based on the amount and type of flood sources in the area. The generic/CANDU-specific data are used for this task, in which the building-component-based flood frequencies are apportioned to the flood areas in each building, after which the frequencies are summed over all the types of flood source components in the area.
- Quantitative screening of the flood scenarios is performed by assuming that all of the safety-related equipment that can be submerged or impacted by water spray in the area is failed. By modifying the relevant fault tree/event tree models, a CCDP for each scenario (or group of scenarios that have similar impacts), can be calculated, such that both flood-induced and random failures are taken into consideration. If the initiation frequency, multiplied by the CCDP gives a negligible SCDF compared with the internal initiating event caused by the flood, then the flood scenario may be screened from further analysis.
- By performing further analysis to eliminate conservatisms, the results for some scenarios may be further refined. Each scenario can be divided into subscenarios based on the individual sources present in the flood location, if their impact is expected to be greatly

different. Then, the flood scenario frequency is reduced by empirical factors (<1) that lower the frequency used in the screening analysis. Credit can be taken for the following factors:

1. location factor – the likelihood of the leakage location being close enough such that "target" safety-related equipment will be impacted.
2. direction factor – the likelihood of spray being directed at "target" equipment.
3. propagation factor - if applicable, this is the likelihood of a propagation path (e.g., door) being open.
4. severity factor – the probability that the leakage rate is great enough to cause the submergence assumed in the screening analysis.
5. operator factor – the likelihood of a successful operator recovery action to isolate or otherwise mitigate the leakage before the target equipment is affected. This factor will be based on the time available to the operator which can be calculated from the leak rate, room dimensions and equipment occupancy.

- The detailed scenario/subscenario frequencies are then combined with the appropriate CCDP to obtain better estimates of the flood-induced SCDF for each flood area. These may be summed with the SCDFs retained from the screening analysis to obtain a total SCDF.

3.6 References

3-1. USNRC, 1983, PRA Procedures Guide - NUREG/CR-2300: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, USNRC Report, NUREG/CR-2300, Volumes 1 and 2.

3-2. CNSC, 1980, Requirements for the Safety Analysis of CANDU Nuclear Power Plants, CNSC Consultative Document, C-6, Revision 0.

3-3. V.G. Snell, 1987, Probabilistic Safety Assessment Goals in Canada. Presented to the IAEA Technical Committee on Prospects for the Development of Probabilistic Safety Criteria, January 27-31, 1987, Vienna, Austria. Also AECL Report, AECL-8761.

3-4. USNRC, 1989, Implementation of Safety Goal Policy. USNRC Report, SECY 89-120.

3-5. IAEA, 1988, Basic Safety Principles for Nuclear Power Plants. IAEA Safety Series Document, 75-INSAG 3.

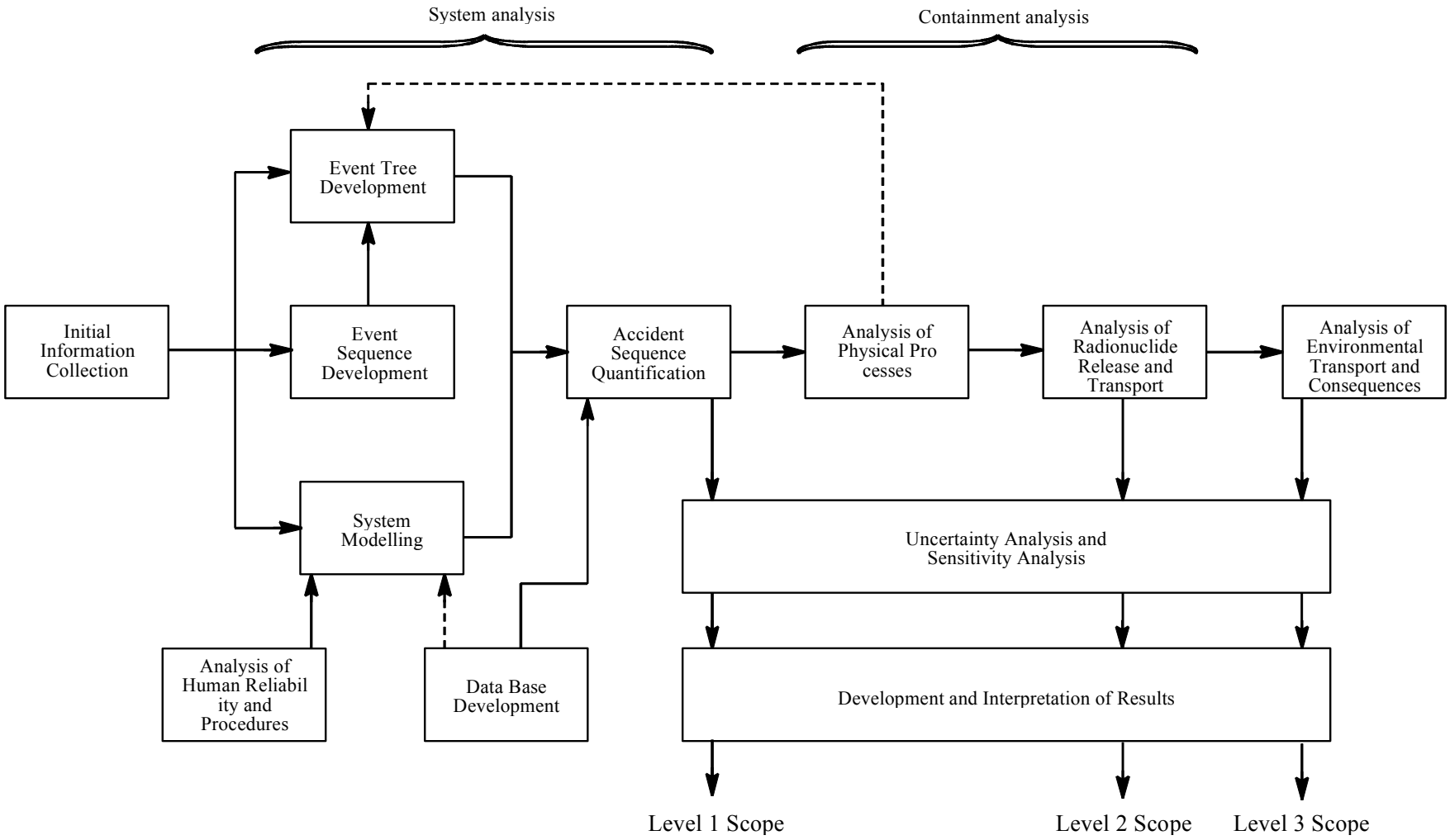
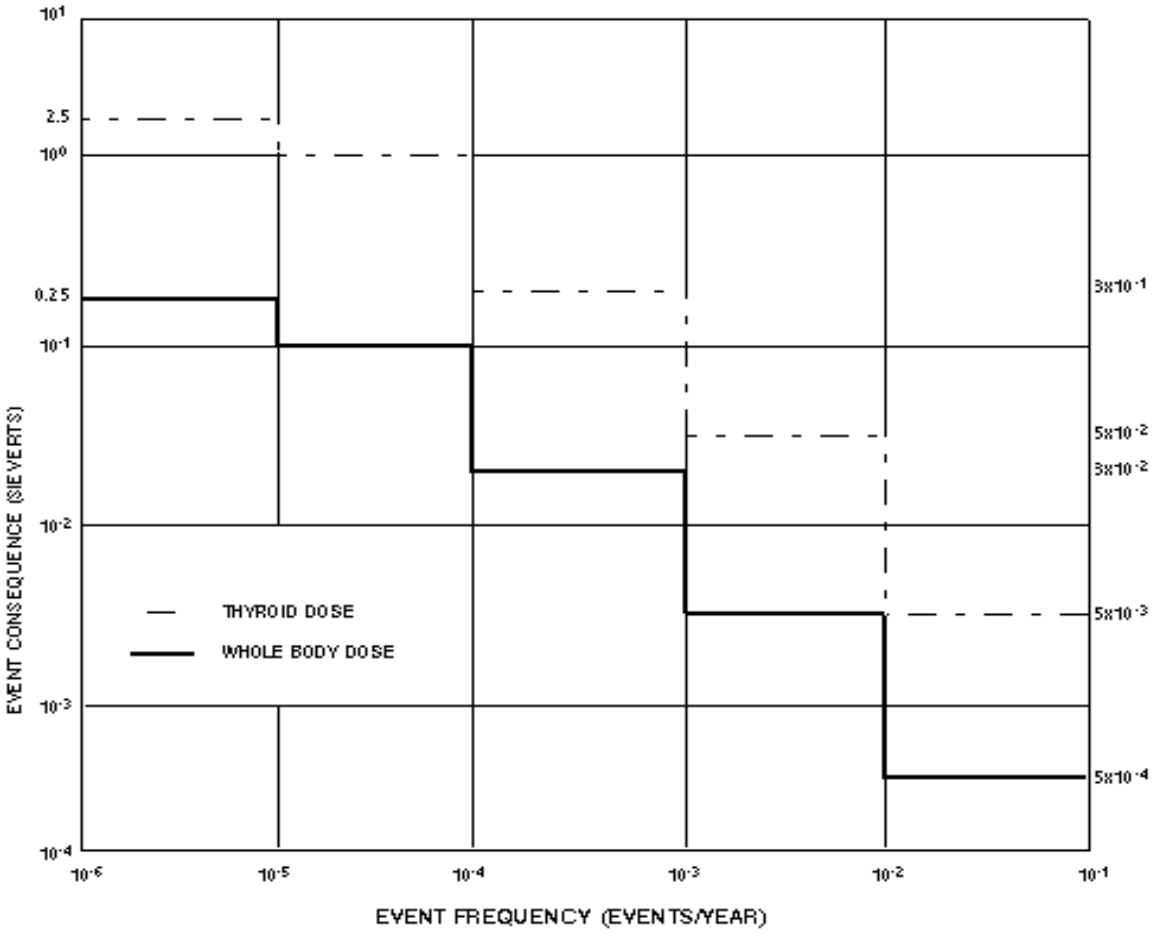


Figure 3-1 Overview of Probabilistic Safety Assessment Process



1. EVENT FREQUENCY = FREQUENCY OF EVENT SEQUENCE END-POINT OR FREQUENCY OF INITIATING EVENT, FOR SINGLE EVENTS.
2. EVENT CONSEQUENCE = DOSE TO INDIVIDUAL MEMBERS OF THE PUBLIC.

Figure 3-2 PSA Acceptance Criteria for Design Basis Events – CANDU 6

4. INTERNAL EVENTS PSA

4.1 Introduction

A Probabilistic Safety Assessment is an analytical technique that is used to integrate the many different aspects of design and operation, in order to assess the safety of a particular facility (in this case, a nuclear power plant), and in order to develop an information base for analyzing plant-specific and generic issues. In particular, a PSA is used to determine core damage frequency and risk to the public.

An internal events PSA investigates potential accidents that are due to random failures from components and equipment within the plant.

The methodology generally follows that described in Reference 4-1.

Internal events PSAs require the collection of a large amount of information, since they are broad integrated studies. This requirement necessitates the gathering of information on all aspects of the design of the plant being modelled, the reliability of data for plant components, operating experience data, etc.

Appendix A expands further on Internal Events PSA supporting information.

4.2 Initiating Event Analysis

4.2.1 Overview

In a PSA, those events that disrupt the normal conditions in the plant and, in general, lead to the need for reactor subcriticality and decay heat removal are referred to as accident sequence initiating events. There are two general categories of initiating events: internal events and external events.

Typically, internal initiating events are abnormal conditions that are generated within the plant, as the result of a failure of some safety-related process function, either due to equipment failure or human error. External events such as earthquakes which originate outside the plant, have the potential for causing multiple, widespread internal events.

Once sufficient familiarity with the CANDU design has been gained, the next step is to identify a list of the potential accident sequence initiating events. The objective is to establish a comprehensive list of initiating events for probabilistic and consequence analysis.

After the initiating events are identified (and before event tree development can begin), the safety functions that are necessary to prevent core damage (e.g., removal of heat) are defined. Based on these initiating events and functions, the safety and/or safety related systems that are required to operate to perform the functions are identified, along with any required support systems, such as service water or electric power. For each of these systems, success criteria that are necessary for the performance of the safety function are then defined. For a particular

system, typical success criteria may include the number of pumps that are required to operate (along with the timing of when they are required to operate), so that the safety function can be performed.

4.2.2 Assumptions and Limitations

One current limitation of the PSA approach is the difficulty of ensuring that all appropriate initiating events have been identified. As a first step, CNSC Consultative Document C-6 (References 4-2 and 4-3) specifies a generic list of initiating events that require safety analysis (Revision 1 of the C-6, Reference 4-3, document is presently undergoing review and comment). In addition, to ensure the completeness of the plant-specific list of events, the C-6 document requires that a systematic review of the plant design be performed. The purpose of this review, which is carried out during the preliminary phase of a PSA, is to identify initiating events or combinations of events that are unique to the particular CANDU design.

For internal events PSA, identification of the initiating events is limited to those events that are associated with plant equipment or the loss of Class IV (offsite) power. The events that are identified are for reactor full power (100%) operation and events during shutdown or planned maintenance outages.

4.2.3 Identification of Initiating Events

An overview of the general plant internal initiating event identification process is shown in Figure 4-1. Applicable initiating events are selected from Reference 4-2 (C-6, Rev. 0) and from similar systematic design review studies of previous CANDU plants. The main process, shown on the right hand side of Figure 4-1, is the systematic review of the CANDU 6 or CANDU 9 plant design that is to be modelled in the PSA.

4.2.3.1 Selection of Events from CNSC Consultative Document C-6

A generic list of initiating events to be analyzed for a typical single- or multi-unit CANDU plant design is given in Reference 4-2 (C-6, Rev. 0).

4.2.3.2 Systematic Review of CANDU Plant Design

Following the event selection, a rigorous and systematic review of the project-specific CANDU plant design is carried out to identify events that require analysis in the overall safety assessment program. Briefly, the approach consists of looking systematically for mechanisms that can cause the release of radioactive materials from their normal locations, and thus can potentially expose the public to radiation levels beyond acceptable limits.

For the current CANDU 6 plant design, the initiating events to be considered have been well established by previous PSA studies and the extensive operating experience of CANDU plants worldwide. The list of CANDU 6 initiating events is obtained by a logic diagram analysis procedure (refer to the left branch under “Systematic Review of Plant Design” in Figure 4-1).

This diagram is essentially a high-level tree model, which focuses on the release of radionuclides to containment and the potential causes of this event. Individual logic diagrams are constructed for each of the main (front-line) systems that contain radionuclides, and their support systems.

For new designs, such as the CANDU 9 or advanced versions of the CANDU 6, an additional technique for identifying initiating events is used to ensure that possible initiators are not missed. This second method uses a failure mode and effects analysis (FMEA) procedure (refer to the right branch under "Systematic Review of Plant Design" in Figure 4-1). This procedure examines the consequences of the failure of individual and multiple components of the main systems that contain radionuclides, and also examines the various failure modes of their support systems. The FMEA approach is particularly useful for examining, in a systematic manner, the failure modes of the support systems that have plant-wide implications. The logic diagram method is a top-down approach, whereas the FMEA method is a bottom-up approach. The two methods thus complement each other, and provide assurance of a comprehensive list of identified events.

Both methods require, as a first step, the identification of the sources of radioactive material that can result in releases to the public. Following this, the systems and equipment that are required to prevent or mitigate the release of radioactive materials are identified. Finally, the potential ways in which these systems and equipment can fail are identified.

4.2.3.3 Sources of Radioactive Material

A large volume of radioactive material (mainly the reactor fuel) is present in the reactor core, and a release of these radioactive materials from the core into the plant systems, and ultimately to the environment, will result in a risk to the public.

The major sources of radioactive material, and thus the locations/systems from which radionuclides can be released, are as follows:

a) the fuel bundles,

b) the HTS,

c) the moderator system,

d) the fuelling machine,

e) the spent fuel handling systems,

f) the spent fuel bay,

g) the heavy water (D_2O) management systems, and

h) the solid and liquid radioactive waste management systems.

4.2.3.4 Logic Diagram Analysis

The starting point for the identification of initiating events by this approach is the specification of the undesired state or top event of the "system", and determination of all credible ways in

which the undesired event can occur. In this case, the undesired state or top event is the release of radionuclides from the major systems. A high-level logic diagram is then constructed to identify the possible ways in which radioactive material can be displaced from its normal location. The process that is followed to develop the logic diagrams consists of the following steps:

a) identification of the sources of radioactive materials that can result in releases to containment,

b) identification of the systems or equipment that are required to keep radioactive materials from being released to containment, and

c) identification of the ways in which these systems or equipment can fail, causing releases to containment.

The level of detail of the logic diagrams is normally limited to the failure of the system function or the failure of the main equipment that leads to the event under consideration. Some events, however, involve the loss of specific components, rather than a system. For these events, e.g., a liquid relief valve or pressurizer relief valve failing "open", the component failure could result in a reactor trip and/or radionuclide release, as well as necessitating decay heat removal. These events are included in the logic diagrams.

The failure of more basic components and control instrumentation is taken into account in the initiating event fault tree analysis, which is used to predict the frequency of these events. This information will be documented in the system reliability analysis.

Logic diagrams are constructed for the heat transport, moderator, fuelling machine, spent fuel handling and spent fuel bay systems. Initiating events that lead to the release of radionuclides from the D_2O management and radioactive waste management systems are not analysed. This is because their consequences with respect to releases to the public are not considered to be significant. The total radioactivity associated with these systems is small. For example, the radioactivity associated with the solid waste management system ranges from about 1×10^{10} to 1×10^{13} Bq., whereas the release from a typical LOCA ranges from about 1×10^{15} to 1×10^{18} Bq.

4.2.3.4.1 Grouping of Logic Diagram Initiating Events

The events that result from the development of the logic diagrams are subsequently grouped, according to similarity of plant response, into a single, bounding, higher-level event. The justification for the event grouping (e.g., same mitigating actions, bounding consequence) is described in detail. For example, the loss of moderator circulation and the loss of moderator cooling events can be grouped into a single event, i.e.: the "loss of moderator heat sink" event, for the purpose of analysis. It is recognized that the dynamics of plant response for the two basic events will be different, in that, compared to loss of cooling, the loss of circulation results in a faster rate of rise in moderator temperature. However, the event tree analysis will assume the faster of the transients, thus bounding the slower transient. Therefore, the results will be somewhat conservative for a loss of cooling event. In system reliability documents, the estimate

for frequency of loss of moderator heat sink will account for the contribution from the loss of moderator circulation, as well as the loss of moderator cooling.

The objective of the grouping process is to yield a smaller, more manageable number of initiating events for the purpose of analysis.

4.2.3.4.2 Output of Logic Diagram Analysis

The following outputs of the systematic plant review by the logic diagram method are generated:

a) logic diagrams for the events that are related to the failure of the heat transport, moderator, fuelling machine, spent fuel handling and spent fuel bay systems;

b) a logic diagram for the events that are related to the failure of the support systems;

c) a table that defines the rationale for grouping the logic diagram basic events with similar plant responses into a single, bounding, higher-level event; and

d) a table that states, for each of the logic diagram basic events, the location of the basic event in a grouped event.

4.2.3.5 Failure Mode and Effects Analysis (FMEA)

With this method, each significant component in the systems listed in Section 4.2.3.3 is identified. Then, for each component, the analyst determines (1) its function, (2) the possible failure modes, (3) the failure mechanisms, (4) the effects on the system, and (5) the method of failure detection. In addition, combined failures of multiple components that can defeat the system function are also identified.

As a minimum, the following system function impairments are considered:

a) increase in heat generation,

b) partial or total loss of the heat sink,

c) partial or total loss of circulation, and

d) partial or total loss of inventory (this includes random pipe breaks and loss of pressure boundary due to any other reason).

Note that the FMEA does not need to address the failure of the control instrumentation, since this is taken into account in the initiating event fault tree analysis. This analysis will be documented in system reliability documents.

All systems that interface with the systems listed in Section 4.2.3.3 are then identified. The interfacing systems are defined as those that are functionally connected to the systems in Section 4.2.3.3. For example, the main interfacing systems for the moderator include the moderator cover gas, moderator purification, liquid poison addition, reactivity control, reserve water tank, and liquid injection shutdown system.

Failures in the interfacing systems are then examined to determine if they can cause the release of radionuclides. As a minimum, loss of system function, loss of flow, loss of pressure boundary integrity, and loss of heat sink are addressed, if applicable.

Systems that are physically adjacent to the systems listed in Section 4.2.3.3 are also identified. The adjacent systems are defined as those that share the same pressure boundary as the identified systems, but that have no functional link with them. For example, for the moderator system, the physically adjacent systems are the shield cooling and annulus gas systems.

Failures in the adjacent systems are then examined to determine if they can cause radionuclide releases. As a minimum, loss of system function, loss of flow, loss of pressure boundary integrity, and loss of heat sink are addressed, if applicable.

The above steps provide an insight into the various failure modes and mechanisms of the systems that can displace radionuclides from their normal locations.

4.2.3.5.1 Grouping of FMEA Failure Modes

The individual failure modes identified above are subsequently reviewed for similarities, in order to group failure modes that have a similar plant response (e.g., same mitigating actions, bounding consequence) into a single event. The main objective of this exercise is to group a large number of failure modes into a smaller, more manageable number of initiating events for the purpose of analysis. For example, as explained in Section 4.2.3.4.1, the failure modes relating to the loss of moderator circulation and the loss of moderator cooling can be grouped into a single event called "loss of moderator heat sink", for the purpose of analysis.

4.2.3.5.2 Output of FMEA Analysis

The following outputs of the systematic plant review using the FMEA approach are generated:

a) FMEA tables that are related to the failure of the heat transport, moderator, fuelling machine, spent fuel handling and spent fuel bay systems. Note that an analysis of the D_2O management and radioactive waste management systems is not required, since the consequences of their failure, with respect to releases to the public, are not considered to be significant.

b) a table that defines the rationale for grouping the failure modes with a similar plant response into a single, bounding, higher-level event.

c) a table that states, for each of the failure modes, the location of the basic failure mode in a grouped event.

4.2.4 Identification of Plant Safety Functions

After the initiating events are identified (and before event tree development can begin), the safety functions that are necessary to prevent core damage, e.g., removal of decay heat, are defined. Identification of the plant safety functions that are required to mitigate the initiating

events and to prevent core damage and radionuclide release forms the preliminary basis for the event tree analysis.

4.2.5 Identification of Plant Systems

Based on these initiating events and functions, the safety systems that are required to operate (in order to perform the functions) are identified, along with any required support systems, such as service water or electric power. For each of these systems, success criteria that are necessary for the performance of the safety function are then defined. For a particular system, typical success criteria may include the number of pumps that are required to operate (along with the timing of when they are required to operate), so that the safety function can be performed. Information for this task is obtained from design documentation such as system design descriptions.

4.2.6 Initiating Event Frequency Quantification

Various methods, including fault tree analysis and CANDU operating experience, are used to estimate the frequencies of initiating events. The objective here is to provide a best-estimate frequency, along with a measure of uncertainty, for every identified initiating event. Frequencies derived from fault tree modelling should be based on the system design of the plant of interest and the current system reliability analysis. Initiating event frequencies from operating experience can be based on CANDU significant event reports. The three methods listed below are used to derive best-estimate frequencies, depending on the number of occurrences found.

4.2.6.1 Commonly Occurring Events

Initiating events with ten or more occurrences over the operating history or time frame analyzed are classified as commonly-occurring events. The justification for the use of the arithmetic mean (n/T) to calculate the frequencies of the initiating events in this classification is as follows. The numerical difference between the chi-square approximated mean and the arithmetic mean becomes smaller as the number of occurrences increases. The difference between the chi-square mean and the arithmetic mean in this classification is judged to be insignificant, given that the initiating event frequencies are calculated to a precision of two significant digits.

4.2.6.2 Rare Event Occurrences

Initiating events with one to ten occurrences over the operating history or time frame analyzed are classified as rare events. The upper limit in this classification of ten occurrences was arbitrarily chosen. The rationale presented in Section 4.2.6.4 supports the use of the chi-square approximation to derive the frequencies for rare events.

4.2.6.3 Zero Event Occurrences

The third classification of initiating events involves events for which no occurrences have been observed. Since there is no CANDU experience from which to calculate a frequency, this

class of initiating events requires the use of fault tree analysis or special quantification techniques, such as the chi-square approximation (see Section 4.2.6.4).

4.2.6.4 Chi-Square Approximation

Component failures within a mature system occur randomly, but at a rate that is approximately constant with time. This behaviour, which applies to failures that occur frequently, can also be assumed to apply to less frequent random failures. Under these circumstances i.e.: for rare events, the distribution of the observed mean time between failures (the inverse of the failure rate) about the true mean follows a chi-square distribution, with 2n+1 degrees of freedom (where n = the number of observed failures).

By assuming the chi-square distribution, it is possible to estimate the mean failure rate and the associated confidence limits for rare events. This method also provides a method for estimating these parameters for zero failures. A sample calculation can be found in Appendix A of this document.

4.2.6.5 Treatment of Uncertainty

To ensure consistency with the other tasks that are involved in quantifying the event sequence frequencies requires the determination of a best-estimate for each initiating event frequency, together with an expression of uncertainty. The degree of uncertainty is indicated by the "uncertainty factor" or "error factor", which determines the upper bound (95% confidence limit) of an assumed lognormal distribution. The uncertainty factor is defined as the ratio of the 95% confidence value to the best-estimate value.

For rare events (less than ten occurrences) determined from CANDU operating experience, the uncertainty or error factor is determined using the chi-square distribution. For most initiating event frequencies determined by fault tree analysis, and for events that have more than ten occurrences, an error factor (EF) of 3 is assumed. See Section 4.10 for further details on the treatment of uncertainty.

4.3 Event Tree Development

4.3.1 General

A PSA includes the evaluation of accident sequences. The methodology used to develop event trees for plant internal events and to perform accident sequence event tree analysis is described in this section. The methodology for internal fire, internal floods and seismic events is different, and is discussed in Sections 7, 8 and 9, respectively, although some steps and terms are similar.

Generally, accident sequence event trees are developed for each initiating event group. In the Level I PSA domain, the event tree structure describes the combination of system successes and failures that can result in the design basis accidents or core damage. The event tree reflects system interrelationships and accident phenomenology that determine whether or not the

sequences lead to core damage. In association with the mitigating systems' fault trees, the event tree is used to perform accident sequence quantification, in order to derive the frequency of the final state (end-state) of a particular accident sequence. The mitigating systems for which the availability is explicitly questioned in the event trees, up to the point of core damage, are referred to as front-line systems. Any system that provides a service (e.g., electrical power, cooling water, instrument air) to a front-line system is called a support system.

Two sets of event trees will be developed in the PSA. The first set of event trees will be strictly used to define and quantify the Level I sequences that lead to severe core damage. As such, the sequences in the Level I event trees will terminate on a success state, a damage state in which the reactor core has disassembled (severe core damage), or a lesser damage state, i.e.: damage either to fuel bundles or to a limited number of channels within the core. The essential purpose of the Level I event trees is to easily determine the summed SCDF, as well as the frequencies of lesser damage states, if desired.

In order to effectively interconnect Level I and Level II PSA activities, there is a need to consider failures of containment mitigating systems, in addition to considering the state of the core. This is accomplished by creating a second set of event trees, which also consider the availability of containment systems—their availability can affect the accident progression analysis. These trees are called extended Level I event trees. They are identical to the Level I event trees, up to and including the failure of the last system that can prevent severe core damage. The event tree is then extended, by questioning the availability of containment mitigating systems at the end of these sequences. The selection of the relevant containment systems should be based on consultations between the Level I and Level II PSA analysts. Strictly speaking, it is only necessary to include in the event tree those containment systems, for which the availability may be affected by either the initiating event itself, or any of the failures implicit in the accident sequence. In this way, any dependencies between the containment and other front-line or support systems will be taken into account. Other containment systems that exhibit no such dependencies can be easily incorporated into a subsequent event tree, e.g., a Level II containment event tree (CET), as described in Section 10.

4.3.2 Event Tree Construction

Accident sequence event trees are usually bimodal logic diagrams at the system level of detail, and describe the possible sequences of events that follow each initiator. The objective is to define all possible combinations of successful and unsuccessful system responses to an initiating event. Each event tree starts with the initiating event, progresses through a logical set of decision branch points (failure states or mitigating system successes), and concludes when either stable conditions (with or without releases) are achieved, or when there are no more available mitigating systems.

A desktop-computer-based proprietary event tree program called ETA-II developed by Data System and Solutions (DS&S) (Reference 4-5) is used to produce the event trees by AECL. ETA-II is one of several codes available for event tree development. A simplified form of an event tree is shown in Figure 4-2.

4.3.2.1 Event Tree Modelling Assumptions - Sources of Information

To prepare the event trees, the physics, fuel and thermalhydraulic response to each initiating event must be known. Most of the deterministic analysis that is associated with the above responses will be documented in project-specific safety analysis reports (SARs), and can be considered, in general, to be PSA support analyses. However, additional analyses that do not yet exist may be required, in order to support assumptions made in the preparation of the event trees for a given PSA. In this document, any additional analyses that are required to support PSA assumptions are termed PSA support analyses—they are required for conditions that are beyond the scope of the safety analyses. PSA support analysis may be required in the following situations:

a) the event has never been analyzed before,

b) design changes in the plant of interest have an impact on the plant response, or

c) other new information (e.g., more recent research and development results) regarding plant response becomes available.

For each event that requires analysis, the event sequence, success or failure criteria, and the system assumptions should be described.

Another important element of the analyst's assessment while developing the event trees is a review of the scenario(s) with designers of the pertinent systems that may be called upon to mitigate the accident, beyond those systems analyzed as part of the SAR.

4.3.2.2 Order of Events

The order of mitigating system behaviour and operator actions in the event trees depends on the particular initiating event. However, Level I event trees will have branch points, which roughly correspond to the following sequence:

a) The initiating event,

b) Reactor shutdown,

c) If liquid relief valves (LRVs) opened, did they re-close?,

d) Operator action,

e) Preferred heat sink,

f) Alternate heat sink(s).

In addition to these events, the extended Level I event trees will subsequently check the availability of containment mitigating systems for SCD sequences. The interface between the extended Level I event trees and Level II CETs shall be determined as work progresses and is documented in the PSA report.

4.3.2.3 Operator Actions

Operator actions are included as far as possible, and are usually placed just before the system that is to be manually initiated. Operator branch points are modelled on a per system basis, which means that more than one operator branch point could appear in the same sequence. Repeat operator branch points (e.g., the operator is called upon to mitigate his or her own previous failure) can be credited if there is time available for the subsequent actions, and if there are independent signals, which indicate that previous actions taken were ineffective. These signals might originate from the clear annunciation of abnormal conditions, or from instrumentation that the operator is procedurally required to monitor to verify successful operation of the initiated system. Details of the pre- and post-accident operator model are provided in Section 6.

4.3.2.4 Mitigating Systems

The top events for the mitigating systems, which appear in an event tree symbolically, represent a fault tree that defines the mitigating system reliability. Mitigating (front-line) system fault tree models include running failures, as well as starting failures. In each case, the mission time is selected on the basis of accident repair times or redundant mitigating system repair times. Accident repair time refers to the time required to gain access to the failed process system, and to return it to a functioning configuration, as well as servicing any other required equipment that was subsequently affected.

If a particular mitigating system is required to function, and no other redundant system exists (or is called upon) to perform the same function, then the mission time for this system is equal to the mission period (see below).

If two redundant mitigating systems exist, then the mission time for either need not be taken as the full mission period. In such cases, the mission time for one system may be taken as the accident repair (including access) time of the other. These time periods are referred to as redundant mitigating system repair times.

In general, the mission period for systems that are necessary to maintain core cooling after an initiating event is chosen as 24 hours. The rationale for this choice is given based on a reasonable time to either recover the system or establish an alternative heat sink while maintaining adequate core cooling. Since decay heat levels are significantly lower after 24 hours have passed, the demands on the mitigating systems are less restrictive, and a variety of recovery/repair actions can be undertaken. Therefore, it is expected that the contribution to the SCDF of events that occur beyond 24 hours is relatively small, compared with the event sequences within the first 24 hours. However, in order to justify this mission time, there is a requirement to explicitly consider the actions that will be taken beyond 24 hours. If only a single, un-repairable system exists to maintain core cooling over the long term, then a longer mission time (e.g., 1 month) will be adopted as the base case for analysis, as alternate heat sinks can be established within 1 month. The potential for optimized risk reduction with a shorter mission time than 24 hours can be determined by means of a sensitivity study.

Systems that are required to function in order to maintain containment integrity shall also have mission times of 24 hours. However, for sequences in which core damage is predicted to occur, equipment repairs may not be possible due to adverse environmental conditions, and the containment integrity may be challenged if cooling is not available after 24 hours. Therefore, a mission time of 72 hours or 1 month may be appropriate for containment systems, depending on whether or not there are alternate means of cooling available.

Front-line or support systems that are credited to mitigate any initiating event that results in harsh environmental conditions must be environmentally qualified to operate in those conditions.

4.3.3 Event Tree Evaluation

Event tree evaluation, more commonly known as accident sequence quantification (ASQ), is used to estimate the frequency for individual accident sequences. The objective is to merge the fault trees for all the branch points that lead to the particular event tree sequence under study. In so doing, the frequency estimate for this sequence factors in any modelled failures that are common between systems. The ASQ process thus provides an accurate assessment of the end-state frequency, by accounting for the various cross linkages. See Section 4.8 for further details.

4.3.4 Event Sequence Termination

As described in Section 4.3.1, the development of a typical accident sequence ends with the determination of the state of damage to the plant. Specifically, the outcome or end-state (final state) of an event tree sequence is either a plant success state, where fuel cooling is maintained with no radionuclide release into containment, or a plant damage state (PDS), with a radionuclide release into containment. The methodology for determining the PDSs is described in Section 4.9. The PDSs define the status of the core, as well as those front-line and containment systems that have an impact on the subsequent accident progression, once radionuclide release into containment occurs. The plant success states are described in Appendix A, and correspond to a set of stable conditions, for which fuel cooling is maintained.

The end-states for the Level I event trees are defined as follows:

a) Success states, where the plant is shown to be in a safe shutdown condition, with no releases for the entire duration of the accident repair time. The plant damage state label for these sequences is “S”.

b) Plant damage states, where all pertinent front-line mitigating systems have been called upon in an effort to prevent releases to containment. If the sequence leads to severe core damage, (i.e.: all means of fuel cooling have been lost, including the moderator system), then the sequence is labelled “SCD”. The PDSs will be explicitly categorized for these sequences in the extended Level I event trees, based on the criteria in Section 4.9. Other, lesser damage states (not SCD) should be labelled according to the criteria in Section 4.9.2 (e.g., PDS 3, PDS 4, etc.).

c) Sequences that are not developed further. These are sequences for which the frequency of occurrence, as determined by accident sequence quantification, is less than 10^{-9} occurrences

per year, and additional mitigating systems may still be credited to prevent core damage. Rather than fully developing the event tree to show these additional systems, a label of "NDF" (not developed further) is shown.

A probability truncation limit of 10^{-10} per year is used in accident sequence quantification. Since the expected summed SCDF is on the order of 10^{-6} per year, the truncation limit is set four orders of magnitude below this value. It is therefore expected that cutsets of lower frequency will not significantly alter the summed SCDF results, and that any slight change will be well within the uncertainty bounds of the analysis. For a given sequence, if no cutsets are generated after accident sequence quantification is performed at a probability truncation of 10^{-10}, then the event tree logic is not developed further, since this is considered to be the cut-off value for risk significance.

In order to keep the extended Level I event trees to a manageable size, the branches that consider the availability of containment systems will only be developed for sequences that result in SCD at risk-significant frequencies, i.e. greater than 10^{-10} occurrences per year. The end-states of the extended Level I event trees are defined as follows:

a) Success states, where the plant is shown to be in a safe shutdown condition, with no releases for the entire duration of the accident repair time. The plant damage state label for these sequences is "S".

b) Plant damage states, where SCD has been prevented, but releases to containment do occur. Containment availability for sequences that are grouped into these PDSs will be addressed later as part of the containment analysis described in Section 10.

c) Severe core damage PDSs, in which all relevant mitigating systems that might have prevented core damage have been called upon and have subsequently failed. These PDSs also include possible impairments of the various containment systems, as described in Section 4.9. The labels for these states are numerical, e.g., PDS 0, PDS 1, etc.

d) Sequences that are not developed further. Two types of sequences are considered here. One type corresponds to those sequences, for which the frequency of occurrence, as determined by accident sequence quantification, is less than 10^{-9} occurrences per year, and additional mitigating systems may still be credited to prevent core damage. The other type corresponds to SCD sequences, for which no cutsets were generated in the Level I ASQ process. Both types are given the label "NDF".

4.3.5 Accident Sequence Nomenclature

A labelling scheme or nomenclature is developed for the accident sequences. Generally, the dominant sequences are tabulated, and the nomenclature is described as follows:

a) Sequence name, consisting of
   1) initiating event/event tree name, e.g., MSIV, and
   2) sequence number—each sequence is given a specific number, e.g., MSIV-S1, etc.

b) Plant damage state.

c) Sequence descriptor, which includes the initiating event (IE), and the success or failure of the various mitigating systems involved. For example, sequence MSIV-S10C is described by the sequence descriptor IE-MSIV * /RS * /SGPR * FW * OSDC2B * EWS3.*ECC-D

The forward slash (/) in the sequence descriptor indicates the success of the mitigating system or operator action. The lack of the forward slash indicates the failure of the system or operator action. The asterisk (*) indicates that all the events in the sequence are "anded."

In the above example, the label of the initiating event is IE-MSIV, which indicates the spurious closure of the main steam isolating valve (MSIV). The other sequence descriptors are described below:

- Descriptor /RS indicates successful reactor shutdown (RS).
- Descriptor /SGPR indicates successful steam generator pressure relief (SGPR), i.e.: the main steam safety valves (MSSVs) are open.
- Descriptor FW without the forward slash indicates the failure of the feedwater (FW) supply to the steam generators.
- Descriptor OSDC2B indicates the failure of the operator to establish shutdown cooling in the abnormal mode within 60 minutes.
- Descriptor EWS3 indicates the failure of the emergency water supply (EWS) from the dousing tank, and includes auto-depressurization.
- Descriptor ECC-D indicates failure of emergency core cooling system demand.

4.3.6 Reporting of Event Tree Analysis Results

Three items that result from an accident sequence event tree analysis are generally reported. These items, which are based on CANDU practice and are also listed in Reference 4-6, are listed below:

a) Assumptions

Any assumptions made in developing the event trees are discussed, including the manner in which they could affect the final result.

b) Event tree

Event trees for each initiating event are presented in graphic form to show all sequences that could be potentially dominant.

c) Accident sequences

Each sequence or group of similar sequences is described. Sequences that are not completely developed should be explained. In CANDU practice, sequence descriptions include the following information:

1) a brief description of the initiating event,

2) a description of the plant response (event sequence), and

3) a brief description of each event tree heading (top event).

4.4 System Reliability Analysis

4.4.1 General

In order to estimate the sequence frequencies, the success and failure probabilities are determined for each branch point on the event trees. This requires the identification and quantification of the important contributors to failure for each of the systems identified by the event tree development.

Fault tree modelling and evaluation is the main tool that is used to derive the failure probabilities of the mitigating systems. Fault tree analysis is also used to derive the frequencies of some initiating events. Initially, fault trees are constructed for all front-line systems.

For mitigating systems, if a front-line or containment system interconnects with support systems, such as electrical power or service water, then models are developed for the required support systems and are later integrated with the front-line systems. However, for initiating event fault trees, support systems are not modelled or integrated with the front-line systems, since the support systems can cause a reactor trip, and are themselves initiating events.

System reliability analysis includes human reliability analysis (described briefly in Section 6), and is dependent on the reliability data in the various databases. Human errors associated with test and maintenance activities are modelled directly in the fault trees.

Dependent failures that arise from system interdependencies and component common cause failures are also modelled (see Section 5).

The requirements for reliability analyses of safety related systems are described in the Consultative Document C-98 (Reference 4-4). The system reliability analysis follows C-98.

4.4.2 Fault Tree Analysis

Fault tree analysis is a deductive method of failure analysis, which focuses on one particular undesired event (e.g., a system failure), and which provides a method for determining the causes of this event. The undesired event constitutes the top event in the fault tree diagram constructed for the system, and corresponds to some particular system failure mode. The fault tree top event is an event that appears in the event tree.

A fault tree is a logical representation of the ways in which a specified undesirable event may occur. The Boolean solution of the fault trees defines the combination of events that can lead to system failure. The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that can result in the occurrence of a predefined undesired event or system failure.

The methodology to be used in the fault tree analysis follows that described in CNSC Consultative Document C-70 (Reference 4-7) and NUREG-0492, Fault Tree Handbook

(Reference 4-8). Logic is developed using the principle of immediate cause. The top event failures are clearly defined, as are the system boundaries.

4.4.3 Computer Codes Used in System Analysis

For the GPSA program, the desktop-computer-based package of fault tree analysis codes called "CAFTA" (Reference 4-9) is used throughout to construct, evaluate and quantify the fault trees. CAFTA also maintains the primary event database. A companion code to CAFTA, called "SAIPLOT" (Reference 4-10), is used to draw the fault trees, and another program CSRAM is used to calculate initiating event frequencies. Codes with equivalent capabilities may be substituted. From this point on, CAFTA is described for information purposes only.

4.4.4 System Information

Before attempting to construct the system fault tree, the analyst identifies and collects the information that is necessary to develop the system models. Information is collected for each system regarding its (1) operation, (2) interfaces and dependencies, (3) design, and (4) testing and maintenance. This information is usually found in the following documents:

a) design manuals (including design requirements and design descriptions),

b) operating manuals (OMs),

c) maintenance manuals (MMs),

d) emergency operating procedures (EOPs),

e) technical specifications (TS),

f) system flow sheets (FS),

g) instrument loop diagrams (ILDs),

h) elementary wiring diagrams.

4.4.5 Fault Tree Event Nomenclature

An essential part of fault tree modelling and analysis is a fault tree event naming or labelling scheme. The labelling scheme or methodology covers all types of fault tree events, i.e.: top, intermediate and primary, although the labelling of the basic events is the main focus.

All intermediate and primary events in a fault tree require unique event nomenclature (names or labels) to enable the evaluation of the fault tree. A fundamental objective in evaluating a fault tree is to ensure that if the same failure event occurs in more than one place in the fault tree, then its impact on the top event is taken into account. To accomplish this objective, the same failure events must be assigned the same labels to enable the computer codes used in the fault tree analysis to recognize the commonality of the events.

An effective labelling scheme is also helpful in interpreting the results of the computer analysis, since only the labels (and not the full descriptions) for the failure events are retained in the evaluation process.

The fault tree labelling scheme must be compatible with the fault tree analysis code. It must also be consistent with the depth of resolution of the component reliability data.

In the development of complex fault trees, there is a risk that labels will be inconsistently applied. Such inconsistent application can seriously jeopardize the validity of the results. Two possible types of errors are

a) assigning different labels to two identical failures, and

b) assigning the same label to two different failures.

In order to address these concerns, an inherently consistent, understandable and easy to use labelling scheme is required. The main objectives of the labelling scheme are

a) the systematic identification of fault tree events, particularly basic events,

b) the consistent application of labels by different analysts,

c) the evaluation of cross links (dependencies) within systems and between systems, and

d) the successful merging of a large number of system fault trees.

The overall structure of the primary event labelling scheme consists of 16 characters grouped in five segments or fields, as shown in the Figure 4-3. The event labels must incorporate the equipment identification used in the specific CANDU design flow sheets.

The segments of the labelling scheme are described below:

BSI/GSI Field: A four-character field, which identifies the system to which the component belongs, and which is based on the basic subject index (BSI) for CANDU 6. CANDU 9 uses a general subject index (GSI).

CN Field: A six-character field, which identifies the specific number of the component that has failed. This is the component or equipment number specified on the flow sheets and bills of material for the system under analysis.

CT Field: A three-character field, which identifies the particular component type, and which is based on the component device code specified by the labelling scheme (see Appendix A).

CC Field: A single-character field, which is used to identify the component class—this distinguishes between sizes, rating or capacities of the component, and identifies whether or not the component is nuclear.

FM Field: A two-character field, which identifies the specific failure mode for the component scheme (see Appendix A).

4.4.6 Generic Fault Tree Models

To reduce the effort that is required to model the control and instrumentation (C&I) logic for each controlled device (many are similar in nature), generic C&I fault tree models may be used for the following devices:

a) motorized valves, e.g., electrically operated valves,

b) pneumatic shut-off valves,

c) pneumatic process control valves, e.g., pressure and temperature control valves, and

d) pump motors.

Where appropriate, each analyst can show the C&I logic as an undeveloped event in the front-line system fault tree, and can use the unavailability derived from the appropriate generic model.

For specific devices with very complex C&I logic, the fault tree logic is modelled individually.

4.4.7 Calculation of Event Probabilities

To calculate failure probabilities for basic events, the computer code CAFTA extracts the needed information from the basic event (BE) and component reliability/type code (TC) databases, and performs the necessary calculation.

4.4.7.1 Assigned Probability

The calculation type identifiers that can be used in the **C** field are designated by 0, 1, 2, 3, 4 or 5. When a probability is assigned, rather than calculated by the CAFTA program, the value **C** = 0 is entered by the analyst in the FACTOR field of the BE database.

4.4.7.2 Active Failures

For an active failure, where the product of the failure rate (λ) and the characteristic time (τ) is less than 0.01, the calculation type **C**=1 is specified. It can be used to calculate both unavailability and mission unreliability. In the case of unavailability, the characteristic time is the restoration time. For mission unreliability, the characteristic time is the mission time.

4.4.7.3 Restoration Time

The restoration time is estimated, by adding the administration time and the time required to return the component to service, to the MTTR. The minimum restoration time is MTTR + one 8-hour shift, except where the Technical Specification (TS) or the operating policies and procedures (OPPs) specifies a shorter period. For these cases, the period specified by the latest documents should be used.

4.4.7.4 Dormant Failures

For dormant failures, the value **C** = 2 is used. In this case, the characteristic time is the average time between tests (T/2), i.e.: the detection time.

This calculation type (C = 2) does not take into account the other elements of the restoration time, i.e.: the administration time + MTTR + the time to return the repaired component to service. For test intervals > 2 months, the restoration time is usually negligible compared with the test interval, and may be ignored by the analyst.

For test intervals < 2 months, the component failure is modelled as a single primary event, to reduce the complexity of the fault tree. However, the calculation must include the test interval ***plus*** the restoration time, i.e.: to calculate the failure probability the following formula is used: $P_f = \lambda\tau = \lambda(T/2 + T_r)$, where T = the test interval, and T_r = the restoration time. As noted above, T_r = MTTR + 8 hours, unless otherwise specified. The characteristic time $\tau = T/2 + MTTR + 8$ hours, and is combined manually by the analyst. When entering the value for τ in the CAFTA BE database, use **C** = 2 for this calculation. For **C** = 2, CAFTA divides the characteristic time by 2; therefore, the analyst must enter $\tau = 2(T/2 + T_r) = T + 2T_r$.

4.4.7.5 Mitigating Systems

For mitigating systems, dormant failures and mission (active) failures must be modelled. In this case, two basic events are modelled as inputs to an **OR** gate, one for the dormant failures prior to the event, and the other for active failures during the mission (mission failures). The failure events are calculated as follows:

a) Dormant failures prior to the initiating event are modelled/calculated using **C** = 2.

b) For mission failures, $P_f = \lambda\tau$, where τ = the mission time. In general, the mission time assigned to most systems is 24 hours.

If the test interval for the dormant failure is > 2 months, then a mission time of 24 hours is negligible and may be ignored to simplify the fault tree model. Use **C** = 1 for the calculation of mission failures, where applicable.

In most cases, calculation types 0, 1 or 2 (dormant failure calculation methods) are satisfactory. When dealing with large numbers, e.g., $\lambda\tau > 0.05$, the more precise formulas represented by calculation types 3, 4 or 5 may be used –(see Table 4-4a in CAFTA User's Manual (Reference 4-9).

4.4.8 Modelling of Specific Events

4.4.8.1 Modelling of Forced Outage in a Mitigating System

A forced outage of a component refers to the failure of a running (active) component *prior* to an initiating event. This type of failure is immediately detectable, as opposed to a dormant failure.

This failure usually results in an outage of the component (the component must be repaired); hence, the term "forced outage". In Light Water Reactor (LWR) practice, this is usually referred to as "unscheduled maintenance."

For this event, the probability is calculated using the restoration time as the characteristic time (τ). If the component is in an inaccessible area (e.g., an area where radiation fields are too high), then the restoration time is the time until the next plant outage, since this represents the time for which the component is unavailable. This duration is typically assumed to be six (6) months.

The examples given below illustrate the treatment of forced outages, which apply only to active (running) component failures, *prior* to an initiating event.

Example #1: Moderator pump failures are modelled as a forced outage, since the moderator system is an active system. On the other hand, the emergency core cooling (ECC) system is a dormant system, and only becomes active during its mission *after* an initiating event. In this case, ECC pump failures are *not* modelled as forced outage events; however, they are modelled for both dormant and mission failures.

When modelling mitigating systems, it is necessary to check if any failures within the system can cause an initiating event. Any failures that are themselves initiating events are not modelled in mitigating system fault trees.

Example #2: There are two pumps, P1 and P2, in a system—P1 is running, and P2 is on standby. If both pumps fail before a postulated initiating event, then the dual pump failure itself results in an initiating event. Therefore, in mitigating systems with two pumps, only one pump is modelled as a forced outage, since only one pump is running *prior* to the event. In a three or four component system, the treatment is more complicated, although similar logic applies.

An active (running) component, such as P1 above, and its associated equipment may fail prior to the initiating event (forced outage), or it may fail during its mission period following an initiating event. If the forced outage is modelled under the running component (P1) logic, then the cutsets will require editing later to remove nonsense (i.e.: mutually exclusive) cutsets. To avoid this problem but, at the same time, retain the cutsets associated with the forced outage of P1 (and the overall failure probability), the forced outage for P1 is modelled under the standby component (P2) logic. P1 is modelled only during the mission. The standby component (P2) is modelled for the mission, dormant failure and forced outage events (and for maintenance outage, if appropriate).

4.4.8.2 Initiating Event Fault Trees

The modelling of initiating event fault trees is significantly different from the modelling of mitigating system fault trees. Active failures, which occur prior to the initiating event, are similar to forced outages. There is no mission time for initiating event fault trees. Standby components are modelled for both dormant and running failures. The characteristic time for a running failure is the restoration time.

4.4.8.3 Routine Maintenance During Plant Operation

Routine maintenance, also known as maintenance outage or preventative maintenance, is defined as the unavailability of a component when regular scheduled maintenance is performed on the equipment. This routine maintenance does not include the major overhaul of equipment.

Routine maintenance during full power operation is modelled in the fault trees, when the component is taken out of service and is unavailable for operation. The probability assigned to routine maintenance is the frequency of maintenance (occurrences/year) multiplied by the total maintenance outage time. Equipment such as a pump and motor are considered as a single unit for maintenance calculations.

4.4.8.4 Modelling of Local Instrument Air Stations

The instrument air system (IAS) contains many air stations in the reactor building (RB), turbine building (TB) and the reactor auxiliary building (RAB). To reduce the number of top events in the IAS fault tree, the local air distribution system, which comprises a shutoff valve, air station manifold and pressure reducing valve(s), is modelled by the analysts in the fault tree logic of each pneumatic valve as one undeveloped event.

There are four basic types of undeveloped events for this situation, depending on the location of the instrument air (inside the reactor, service or turbine building), and depending on whether the valve that is receiving air is a pneumatic valve (PV) or a temperature control valve (TCV) or level control valve (LCV).

The boundary between the IAS and a front-line system occurs at the junction between the air receivers and the local instrument air distribution system.

4.4.9 System Analysis Reports

In general, each system reliability analysis report contains the following information as a minimum:

a) The purpose and scope of the system analysis.

b) A brief description of the system design and operation, based on the technical description or specific system design manuals and flow sheets.

c) Identification of the fault tree top events to be analysed for the initiating event or mitigating system, and their names/labels.

d) The definition of success/failure criteria for the system.

e) Assumptions used in the analysis. These assumptions include system design and operation, as well as fault tree modelling assumptions.

f) The definition of system boundaries.

g) Reliability data - this includes primary event data, interfacing event data, human reliability data and generic C&I model data.

h) Fault tree quantification.

i) A discussion of dominant contributors.

j) Data tables.

k) Fault tree plots.

l) References (design manuals, flow sheets, etc.).

4.5 Dependent Failure Analysis

In risk analysis, the treatment of dependencies in the identification and quantification of accident sequences is called “dependent failure analysis.” Dependent events are those that are influenced by the occurrence of other events. In general, this means that the probability of a dependent event is based on whether or not the other events (which affect it) have previously occurred. Dependencies tend to increase the frequency of multiple, concurrent failures. Dependent failures are those failures that defeat the redundancy or diversity that is used to optimize the availability of some plant functions. Section 5 describes in detail the dependent failure analysis used in the GPSA.

4.6 Human Reliability Analysis

An important aspect of any PSA is the analysis of the human actions, commonly referred to as human reliability analysis (HRA). Given the high degree of hardware reliability and redundant design associated with nuclear power plant systems, human interactions with the systems are often significant contributors to system unavailability. The purpose of HRA is to identify potential human errors, and to quantify the most significant of these errors. The human actions of potential concern that are identified during the PSA process are analysed. Section 6 describes in detail the HRA used in the GPSA.

4.7 Database Development

4.7.1 Overview

In order to quantify the frequency of each accident sequence, reliability data are required for each basic event in the system fault trees. Some of these events are human errors, which are evaluated and quantified using the HRA techniques (see Section 6). Other events include initiating events, which are quantified using the methodology described in Section 4.2. The vast majority of events, however, consist of failures of components and unavailabilities that are due to testing and maintenance outages. Each component, in turn, may fail in several ways. The purpose of the database development task is to develop generic data, and where appropriate, develop plant-specific data for each failure mode, as well as for testing and maintenance unavailabilities, for all components in the front-line and support system fault trees.

4.7.2 Component Reliability Database

4.7.2.1 Sources of Information for Database

Component reliability data for CANDU 6/CANDU 9 PSAs is compiled primarily from operating CANDU plants. A large source of component reliability data, is the operating experience from Ontario Power Generation's generating stations. OPG was formally known as Ontario Hydro (OH). These data were compiled from both internal and external sources.

4.7.2.1.1 Internal Sources

The primary source of data builds on OPG Operating Experience.

4.7.2.1.2 External Sources

There are several other sources of published data available from industry sources. The following are the primary sources:

a) IEEE Standard 500-1984 (Reference 4-11), and

b) Nuclear Plant Reliability Data System (NPRDS) 1983 Annual Report of Cumulative System and Component Reliability (Reference 4-12).

The IEEE Standard (Reference 4-11) provides failure rates that correspond to various failure modes of electrical and C&I components, including detailed classification with respect to type, size, etc. However, for some components, the failure rate data are not available for all type or size classifications.

The NPRDS Annual Report (Reference 4-12) presents data that spans eight years of experience with commercially operated US nuclear power plants through 1982. The report provides component failure information such as the total number of failures, the population, total component operating times, and failure modes.

It is noted that data collection in the above manner has led to the inclusion of failures due to human error for some components, but not for others. Since human errors are explicitly modelled, this may lead to some double counting. However, this method is conservative.

4.7.3 Treatment of Data

The component reliability database contains the average failure rates of components, unless there have been no failures. In the latter case, values that correspond to the one-sided, 50% upper confidence limit are given.

a) Failure rates

The average failure rate (λ) for a component type is estimated using the following equation:

$$\lambda = \frac{1000\eta}{T}$$

where λ = failure rate in occurrences per 1000 component operating years,

η = total number of reported failures of the component type, and

T = total component operating time in years.

In the database, the average value of λ is given, unless there have been no failures. In the latter case, the value that corresponds to the 50 percent upper confidence level is given.

The one-sided upper confidence limit, λ_u, is calculated by:

$$\lambda_u = \{\chi^2(\propto,2n + 2)/2T\} * 1000$$

where $\propto$ = specified one-sided upper confidence level, and

$\chi^2(\propto,2n + 2)$ = the value of the chi square at the $\propto$ percentile of the chi square distribution, with (2n + 2) degrees of freedom.

b) Mean Time to Repair

The MTTR is calculated as follows:

$$\text{MTTR} = \frac{1}{k}\sum_{i=1}^{k} t_i$$

where t_i = the observed repair time, in hours, of the i^{th} failure, and

k = number of failures for which repair times were recorded.

The value for MTTR is given in hours and is rounded to the nearest integer. In the case where no failures have occurred, an estimate that is based on a similar component is used.

4.7.3.1 Presentation of Data

Reliability data for the generic CANDU 6 and CANDU 9 component reliability database will be organized alphabetically by type code, and will include the following items for each component:

a) Type code—a six-digit code, which includes the component type code, class code and failure mode code that is associated with the component –(see Section 4.4.5).

b) Failure rate—failure rates in the CANDU 6/CANDU 9 component reliability database will be expressed in failures/year.

c) Description of component and failure mode.

d) Source of data.

e) Mean time to repair (MTTR).

f) Error factor (EF).

g) Uncertainty distribution (lognormal).

4.7.3.2 Restoration Time

The restoration time is estimated, by adding the administration time and the time required to return the component to service, to the MTTR. The minimum restoration time is MTTR + one 8-hour shift, except where the Technical Specification (TS) or the operating policies and procedures (OPPs) specify a shorter period. For these cases, the period specified by the latest documents should be used.

4.7.3.3 Limit of Resolution

The establishment of the (internal) limit of resolution of the analysis is the process of selecting the smallest subsystem or component that will be treated as a discrete entity in the analysis. The limit of resolution must, as a minimum, extend to the component level for which sufficient data are available.

The definitions given in Appendix A explicitly identify the component boundaries to which the failure rates in the database apply. The analysts should use these boundaries when establishing the limits of resolution for their fault trees.

4.7.3.4 Component Boundaries

A component is defined as an assembly of interconnected parts with specific boundaries that constitutes an identifiable device, instrument or piece of equipment. A component can be disconnected, removed as a unit, and replaced with a spare. It has a definable performance characteristic, which allows it to be tested as a unit.

Relay contacts are not components as per the above definition; however, they are modelled separately, to ensure that dependencies are revealed in the risk assessment models.

4.7.3.5 Uncertainty

For uncertainty analysis, the component reliability database contains two fields; one for the Distribution Type (DIST), usually lognormal, and the other for the EF associated with each failure event.

4.7.3.6 Limitations

The following limitations of the data are to be considered when reviewing the qualitative results of the fault tree analysis:

a) Experience-The reliability data, in some cases, are based on limited experience in terms of component population size, average in-service time per component, or the number of observed failures.

b) Generic Nature of the Data-For the most part, the failure rate data are generic. However, generic data may not always be representative of a specific application (e.g., generic pump data may not be applicable to all pumps).

c) Restoration Time-These times are based on estimates rather than observed results. Also, in general, component repair times are given for only the "all modes" failure mode, and not specifically for each failure mode.

d) External Data-Some of the failure rate data are from non-CANDU experience, and are based on judgement rather than observed results.

4.8 Accident Sequence Quantification

4.8.1 Outline

Accident Sequence Quantification (ASQ) is undertaken to estimate the frequency of the PDS following an initiating event.

As mentioned in Section 4.3.4, event tree logic is developed to a final plant state within the containment boundary. The endpoint or final state of an event tree sequence is either a plant success state where fuel cooling is maintained with no radiation release into containment, or a PDS, with radiation release into containment and possible impairment of one or more containment systems. For each individual event tree sequence that ends in an undesirable plant condition or PDS (see Section 4.9), an assessment is required to determine the frequency.

The objective is to merge the fault trees for all the decision branch points that lead to the accident sequence under study. The frequency estimate for the sequence takes into account any modelled failures that are common between systems. ASQ yields an estimate of the frequency for individual accident sequences by solving for the event tree top logic and system fault trees. The frequencies of the cutsets that result in SCD may be summed to obtain the overall or SCDF of the plant.

ASQ is performed on the event trees. For some cases, the plant response to different initiating events is the same; therefore, only one event tree is developed and quantified. In other cases, initiating events are grouped as one event and are solved.

4.8.2 Methodology

The objective of ASQ is to provide an evaluation of the impact and contribution of individual accident sequences to the frequency of PDSs. This objective is met by the straightforward solution of the event tree top logic and system fault trees.

ASQ will be performed using the CAFTA and PRAQUANT (Reference 4-13) computer codes. Figure 4-4 shows the sequence of analysis and the computer codes used to perform the ASQ. The event tree is first constructed using the event tree computer code ETA-II. The system fault tree logic is then developed using the CAFTA fault tree editor. Next, the supporting (high level) logic for each accident sequence that is generated in the event tree is developed, by converting the event tree accident sequence logic to a fault tree format using the CAFTA fault tree editor.

Once all the fault trees and other supporting files are prepared, they are merged into one large fault tree using the fault tree editor. The merged fault tree is then used to generate an input file for the CAFTA cutset generator, for each accident sequence, using the CAFTA fault tree editor. The cutsets for each accident sequence are generated using the CAFTA cutset generator.

Since the cutsets for some sequences may contain success logic, it may be necessary to condition these cutsets, by deleting the success logic. In addition, mutually exclusive cutsets, such as a combination of all pumps in a system being maintained at the same time (a situation that is not permitted by operating procedures or technical specifications), must be deleted. These steps are performed using the code PRAQUANT.

Before accident sequence cutsets can be generated, several preliminary tasks must be performed. Each of these tasks is described below.

4.8.2.1 Generate and Review Front-Line System Cutsets

The front-line system models, along with the required support system logic, are evaluated, and cutsets are ranked by probability. Once the cutsets are generated, they are reviewed by the system analyst and the PSA team leader. In addition to checking the model probability, the analyst needs to review the support system interface, identify mutually exclusive events, and identify and define any flags that are included in the model.

4.8.2.2 Prepare Accident Sequence Logic Files

Accident sequences to be evaluated are converted into fault tree logic, as described in Section 4.8.2. The failure branches and initiating events are logically “AND”ed, and the success branches are “OR”ed. In order to “AND” the failure branches, any logic loops between supporting systems must first be solved—see Section 4.8.2.3.

When converting the event trees to a fault tree format, some changes may be required to make them consistent with the fault tree systems. In some cases, flags may have to be added, for example, to the RRS to toggle setback and stepback. In other cases, logic may be required to join systems together, for example, the RS top event consists of SDS1, SDS2 and the RRS, “AND”ed together.

When all the fault trees are completed and the circular logic is solved, these files are merged together into one large file (file extension .CAF), with associated files (file extensions .BE and .GT). These files become the basis for solving the various ASQ sequences. All the mitigating systems that are needed to perform ASQ are found in these files.

The success branch logic is used to remove cutsets that violate the success criteria of the sequence. Only those success systems that have events in common with failed systems need to be included in the success sequence logic. The determination of the accident sequences that require evaluation, along with the logic for these sequences, is the responsibility of accident sequence and system analysts.

4.8.2.3 Remove Logic Loops

Logic loops may become apparent after merging the support systems with the front-line systems. An example of such a loop would be the Class III AC electrical power, which is required to start and run the Class III diesel generator (DG) support systems. If the raw service water system is not available due to the loss of Class III AC, then the DGs are functionally unavailable, and cannot supply Class III AC. Any such loops that are found should be broken at some point, because the code will not be able to solve fault trees with loops. This action should be done carefully to ensure that no cutsets are lost in the process.

4.8.2.4 Develop Flag File

Some of the system models may contain flags that will be set to true or false, depending on the initiating event or sequence that is being quantified. The flags are similar to conditioning events, and can be toggled "on" by setting the flag to TRUE (logic 1), or "off" by setting the flag to FALSE (logic 0), during the integration process. The purpose of the flags is to modify the existing mitigating system fault trees to suit specific accident sequences. Depending on the initiating event and the plant response, some specific equipment may or may not be available. If the equipment is not available for a particular accident sequence, then it cannot be credited in that sequence.

For each event tree that will be analysed, there will be a file, which includes all the flags that are pertinent to that event tree. The flags will be set to true or false in the file, depending on the accident sequences. Each event tree will have its own flag filename, if it is different from the standard case (the standard case will have a default with appropriate flags).

4.8.2.5 Develop Mutually Exclusive Events File

Two events may often appear in an accident sequence cutset that cannot occur simultaneously. For example, initiating events are assumed to be mutually exclusive, as well as maintenance events on separate trains of the same system. These cutsets could be removed through the use of NOT logic, but this introduces a significant amount of additional work on the part of the cutset generation codes. It is easier and less time-consuming to remove these cutsets from the cutset results, by using the mutually exclusive event files. The PRAQUANT code provides the function to delete the mutually exclusive events from the generated cutsets.

4.8.2.6 Modularization

The functional modularization technique serves to reduce the time that is required to evaluate large fault tree models. This process will be used less and less with the availability of ever more powerful personal computers. Modularization combines events that cause similar losses of system function and that are independent of each other, the analyst can greatly reduce the time required to evaluate the models. This technique is called functional modularization, because each module now represents a failure of functionally related events. The module logic can be evaluated to produce module probabilities and cutsets. The resulting module failure probabilities are then stored in the basic event database. When the main fault tree is evaluated, the module is treated as a single event, using the result from the module evaluation stored in the database file. The combined events in a module should be independent from the rest of the fault tree. The use of modules is usually limited to large multi-system models.

In addition to reducing the time needed to evaluate the models, this modularization process can also reduce the time spent reviewing the cutset results. The review process identifies the important risk contributors; however, it is often difficult to identify these contributors, as they may appear within hundreds or thousands of cutsets. By implementing the modularization technique, the analyst can greatly reduce the number of cutsets that require review. Due to the large-size fault trees and event trees associated with CANDU 6 and CANDU 9 systems, this modularization technique can be used in the PSA.

4.8.2.7 Frequency Truncation

It is expected that the frequency of individual sequences that cause beyond-design-basis accidents, i.e.: SCD, will be 10^{-6} events/year or less. Therefore, a cutset truncation limit of 10^{-10} is selected for ASQ and is used for the majority of the sequences, in order to ensure that all significant contributors to the sequence are included in the generated cutsets. Also, the use of the frequency truncation technique limits the number of cutsets to a manageable quantity.

4.8.2.8 Recovery Analysis

After the number of cutsets for the sequences that result in the PDS are minimised, recovery analysis is performed. Recovery factors are incorporated into the cutsets using the CAFTA cutset editor, in order to produce the final results of the analysis.

Recovery analysis is performed on sequences that have a frequency greater than 10^{-9} events/year, and on cutsets within a sequence that have a probability greater than 10^{-10}, where applicable. Since many sequences have to be reviewed for recovery analysis, and since recovery actions are applied to many cutsets, several programs have been developed to facilitate the work.

Two programs are available, one written in visual Basic (ADD1V1_0.EXE) and the other in C++ (RECOV.EXE). These programs automatically add recovery actions, which are determined by rule-based functions, to certain cutset combinations in a sequence. The programs check each generated cutset, to see whether or not some conditional cutset is included. If the generated cutset contains the conditional cutset, then the recovery action is added to those cutsets. For

example, if a cutset contains GRID-TRIP and a running failure of a diesel generator, then the program adds the basic event OR-CL4-12H to the cutset, to reflect the recovery action. The programs add this recovery action to all cutsets in a particular sequence.

In this manner, the PSA analyst determines the cutsets that require recovery actions, and then runs the programs to add them to all cutsets within a sequence automatically.

Both programs can handle NOT logic. For example, if X and Y exist but not Z in a cutset, then add recovery basic event A to the cutset. Several different combinations are possible, up to a maximum of six combinations.

The RECOV program has been integrated with the CAFTA software for ease of use. In this way, the analyst begins with a *.CUT file, and ends with a new *.CUT file, which contains the recovery actions that are applied to all the cutsets in the sequence.

4.9 Plant Damage State Analysis

The event tree analysis yields a large number of internal events accident sequences that can result in significant fission product releases to the containment. The objective of grouping (binning) these numerous event sequences is to collapse the spectrum of design-basis/core-damage accident scenarios into a manageable set of PDSs, in order to simplify the subsequent containment performance analysis.

For containment analysis, the assumption is made that each PDS can be represented by one event sequence that is chosen to be representative of the category as a whole. Within each of the PDSs, a single assessment of the containment response and fission product release pathways can be made, for which source terms are estimated.

The range of accident sequences covered by the PDSs is defined by the overall scope and level of detail utilised in performing the Level II PSA and CET analysis (see Section 10). This range is bounded at the higher consequence threshold by events that lead to SCD and the failure of containment systems.

The range is bounded at the lower consequence threshold for significance by a loss of moderator fluid to containment, followed by a corresponding release of tritium or a LOCA without fuel failure, which shows a release of activity from the coolant. Although fuel damage is not likely, the events are considered to have the potential for some radioactive releases and economic consequences, due to plant shutdown for clean-up.

4.9.1 Basis for Classification of Plant Damage States

By definition, a PDS is a group of accident sequences that have similar characteristics with respect to the accident progression and containment performance. Accident sequences allocated to a PDS have similar characteristics not only in the degree of fuel damage, but also in other characteristics that influence the release of fission products to the environment. These characteristics are associated with the conditions of the HTS core cooling. These influences

include the impact of the status of the ECCS on the timing of the fission product release from the primary HTS (PHTS) and the implications of the initiating event on the PHTS pressure. Therefore, the PDS categories can be defined in terms of the performance of certain safety-related systems.

All accident sequences that require classification can be described by one of the following general PDS definitions, which are arranged in order of decreasing potential for a large magnitude fuel damage and/or fission product release:

a) Early (rapid) loss of core structural integrity - PDS0.

b) Late loss of core structural integrity with high PHTS pressure - PDS1.

c) Late loss of core structural integrity with low PHTS pressure - PDS2.

d) Loss of core cooling with moderator required early as sustained heat sink. - PDS3 (e.g. due to LOCA plus loss of ECC).

e) Loss of core cooling with moderator required late as a sustained heat sink - PDS4 (e.g. due to LOCA plus loss of ECC).

f) Loss of cooling/inadequate cooling in one or more core passes following a large LOCA with successful initiations of ECC - PDS5.

g) Power cooling mismatch in a single channel with direct discharge into containment - PDS6.

h) Power cooling mismatch in a single channel terminated by discharge into the reactor core - PDS7.

i) Loss of cooling to fuelling machine - PDS8.

j) Loss of PHTS integrity/small LOCA with successful initiation of ECC - PDS9.

k) Deuterium deflagration in calandria vessel and/or release of moderator into containment (fuel cooling is maintained) - PDS10.

The containment performance, i.e.: the containment status before and during core degradation, and the containment systems performance has not been considered in the initial definition of the PDSs. The individual PDSs are discussed briefly below.

4.9.2 Definition of Plant Damage States

PDS0, PDS1 and PDS2 are all very low probability events.

4.9.2.1 Loss of Structural Integrity – PDS0, PDS1 and PDS2

These PDSs contain all events that have the potential to cause a loss of core structural integrity. This loss can occur as a result of the failure of the moderator to act as a heat sink when required, as a result of a failure to shutdown, or as a result of the severe overstressing of the calandria structures. All such losses of core structural integrity are assumed to have the potential to lead to SCD.

The three sub-categories of the loss of core structural integrity are:

1. PDS0 - Early loss of core structural integrity.
2. PDS1 - Late loss of core structural integrity with high PHTS pressure.
3. PDS2 - Late loss of core structural integrity with low PHTS pressure.

Each of the above PDSs is discussed in more detail below.

4.9.2.1.1 Early Loss of Core Structural Integrity - PDS0

This SCD event is a low probability power excursion event. The initiating event is postulated to be an event at full power that leads to an imbalance between the power generated and the power removed by the coolant, e.g., decreased coolant flow, LOCA, or loss of reactivity control. All the control and shutdown systems are then assumed to fail. This includes the failure of the RRS with both stepback and setback functions, the failure of the fast shutoff rod system SDS1, and the failure of the fast poison injection system SDS2. The shutdown of the reactor is then caused by displacement of the moderator as the result of steam discharge from fuel channel failure.

4.9.2.1.2 Late Loss of Core Structural Integrity with High PHTS Pressure - PDS1

A key CANDU-specific heat sink is the cool, low-pressure moderator that surrounds the fuel channels in the core. The moderator system is cooled to remove nuclear heat that is continually transferred to it. If the primary heat sinks fail, then the moderator provides an inherent heat sink, which limits fuel temperatures and hence releases. With continued moderator cooling, the fuel temperatures are limited, so that no fuel melting occurs.

A complete loss of heat sinks, with the HTS at high pressure, and a failure of ECC and MHS to remove decay heat lead to loss of core structured integrity, PDS1. A description of a core melt progression for this plant damage state (PDS1) is given in Reference 4-16.

4.9.2.1.3 Late Loss of Core Structural Integrity with Low PHTS Pressure - PDS2

This category involves accidents with a late loss of core structure caused by a complete loss of heat sinks, with the heat removal system at low pressure, successful initiation of ECC, a failure of ECC recovery and a failure of the moderator to remove decay heat

4.9.2.2 Loss of Core Cooling Requiring the Moderator as a Heat Sink - PDS3, PDS4

Any LOCA beyond the capability of the D_2O feed system requires the initiation of the ECCS. Failure of ECC results in a loss of cooling of the fuel and eventual fuel damage. If the moderator is available as a heat sink and meets the necessary criteria, then no loss of core structural integrity will occur, although fuel damage and structural distortion of the fuel bundles may occur within the fuel channels.

This set of accident sequences involve LOCAs combined with a loss of emergency core cooling (LOECC), either on demand (PDS3) or during the mission time (PDS4), with the moderator acting as an emergency heat sink. For these scenarios, some pressure tubes may strain and contact their associated calandria tubes, in which case the moderator provides a heat sink.

PDS3 represents significant fuel damage—up to 30% of the core equilibrium fission-product inventory may be released from the fuel.

The magnitude of fuel damage associated with PDS4 is quite small, and largely represents an economic rather than a public health risk.

For the transient events where all heat sinks are lost, followed by pressure tube rupture and ECC initiation the PDS category is considered to be PDS4.

4.9.2.3 Loss of Cooling/Inadequate Cooling in One or More Core Passes Following a Large LOCA with Successful Initiation of ECC - PDS5

For a large LOCA with loss of Class IV power, the PHTS pumps run down early, and are therefore not available to assist in core refill by ECC injection. In some cases, this can lead to longer refill times than with the pumps running during the refill procedure. Although thermalhydraulic calculations do not indicate severe fuel heating, for conservatism in the safety analysis, fission product releases from fuel in the core are assumed to pass downstream of the break (critical core pass), and are assumed to be the same as in the loss of ECC injection analysis. While this gives an overestimate of expected releases, dose limits are still met.

4.9.2.4 Loss of Cooling in a Single Channel - PDS6 and PDS7

A number of failure modes can be identified that may result in damage to a number of fuel bundles, up to a maximum of twelve in a single channel. The magnitude of potential fission product release is of the same order for all failure modes, depending on the precise nature of the associated fuel cooling assumptions.

In determining the appropriate number of PDSs to adequately represent the potential consequences of single channel events, the associated thermalhydraulic behaviour and its impact on containment response are the main considerations. Since all breaks that result in single channel events fall in or below the small break range, the major issue affecting dose consequence is whether or not sufficient steam pressure is generated to pressurize the containment structure, and initiate isolation automatically.

The single channel event is subdivided into the following two categories:

- Out-of-core events such as an end-fitting failure, with the ejection of fuel into the reactor vault. For these events, it is assumed that containment is pressurized and the PDS is defined as PDS6.

- In-core events such as a fuel channel failure, as a result of severe channel flow blockage, in which the fuel is ejected into the moderator inside the calandria. In this case, containment is not pressurized and the PDS is defined as PDS7.

4.9.2.5 Loss of Cooling to Fuelling Machine - PDS8

A CANDU fuelling machine can accommodate up to ten fuel bundles at a time; however, for most of the time, it transfers a maximum of eight bundles. Therefore, the analysis is based on eight bundles. The magnitude of potential fuel damage is thus comparable to the single channel events. Nonetheless, a separate PDS has been defined for this event, for the following reasons:

- There is no pressurization of containment.
- Since fuel heat-up is slow, fuel damage is not expected to occur before 30 minutes.
- No break occurs in the PHTS, so the potential for economic consequence is reduced.

4.9.2.6 Loss of PHT Integrity/Small LOCA with Successful Initiation of ECC - PDS9

A break in the PHTS that results in the operation of the ECCS but that does not cause fuel damage is nevertheless considered to have the potential for significant economic consequence. Such an event results in the release of radionuclides (tritium, noble gases, radioiodines) from the coolant, and necessitates the recovery of the downgraded D_2O coolant.

4.9.2.7 Deuterium (D_2) Deflagration in Cover Gas and Release of Moderator into Containment - PDS10

This PDS encompasses events that may result in a release of moderator fluid into containment, with an associated release of tritium. No fuel damage is postulated for these events. This category may be divided into the following three sub-categories:

1. Deuterium (D_2) deflagration in cover gas - PDS10-1,
2. Fast release of moderator into containment (fuel cooling is maintained) - PDS10-2, and
3. Slow release of moderator into containment (fuel cooling is maintained) - PDS10-3.

4.10 Uncertainty Analysis

4.10.1 General

Many types of quantitative reliability techniques exist for analyzing the performance of a system. The end result, e.g., system unavailability prediction, is an estimation of actual, real-life performance. There is, however, some uncertainty as to how well the prediction will match the actual situation.

This section discusses the sources and treatment of uncertainty in a PSA. Uncertainty in the analysis is encountered in every step of the process. Uncertainty can be both qualitative and quantitative in nature, and arises from the database used to determine parameter values, modelling assumptions, and the completeness of the analysis.

4.10.2 Sources of Uncertainty

The following is a list of some of the major sources of uncertainty encountered in a PSA:

a) the completeness of the analysis,

b) the modelling of physical processes or systems and their interactions, including phenomenological issues, and

c) parameter value uncertainty.

Ultimately, the only reliable way to assess the overall uncertainty in a risk estimation process is to compare predictions with actual experience. Where such an option is unavailable, various methods may be employed to incorporate the effects of uncertainty, by making conservative assumptions, or by estimating the magnitude of the uncertainty and by taking the uncertainty into account when interpreting the results of the risk estimates.

4.10.3 Treatment of Uncertainty

4.10.3.1 Uncertainties with Respect to the Completeness of the Analysis

Uncertainties in the conceptual understanding of systems, processes and their interactions, which can lead to the omission of potential contributors to risk or to the inclusion of unrealistic contributors, is often referred to as the issue of completeness. The primary concern is that potentially important sequences that contribute to risk may be omitted, due to a lack of knowledge, understanding, experience, or a combination of all three. On the other hand, it is also possible that some identified sequences may be given more significance than is warranted due to conservative assumptions in defining system failure criteria. Obviously, the scope and limitations of the PSA will have an important bearing on the issue of completeness.

Uncertainties in this category cannot be quantified; however, efforts can be made to minimize their impact, e.g., by adopting a highly systematic approach to event identification, as discussed in Section 4.2. This approach, in addition to accumulated knowledge acquired from other risk assessments, worldwide operating experience, and a thorough review process, provides a degree of assurance that important sequences will not be omitted.

4.10.3.2 Modelling Uncertainties

Modelling uncertainties reflect the limitations of knowledge regarding the phenomenological progression through the plant systems, and the human response to abnormal conditions.

Most of the information that is used to assess plant transient behaviour, core damage, and fission product release and transport is the result of some form of modelling. Certain features of failure rate estimation also involve models, in particular that of HRA. Uncertainties are introduced, when the physical processes and systems are represented as mathematical or logical models, and when simplifications are required, in order to make the modelling process manageable.

It is recognized that there is uncertainty associated with all physical processes or systems, e.g., fuel failure, channel rupture or failure of moderator cooling. Also, the uncertainty of some or all of the phenomenological issues that are associated with containment analysis can have an important effect on containment.

These uncertainties are generally addressed, by making conservative modelling assumptions in the safety analysis.

4.10.3.3 Parameter Value Uncertainty

This type of uncertainty refers to parameters that possess a significant natural random variability, and whose characteristics can be represented probabilistically. Sources of parameter uncertainty include the lack of data regarding component failure modes, the interpretation of data and component performance records, and the use of generic data for plant-specific analyses.

The parameters of interest are those of the probability models for the accident sequence logic. These parameters include failure rates, component unavailabilities, initiating event frequencies, and human error probabilities.

4.10.4 Approach to Uncertainty Quantification

The performance of uncertainty analysis is based on UNCERT program (Reference 4-14). This computer program is used to determine the uncertainty of system failure probabilities (including module probabilities) or accident sequence frequencies for the PSA, based on model input uncertainties. A Monte Carlo technique is used for the calculations.

The UNCERT code is designed specifically to calculate the uncertainty that exists in the quantification of a model, due to the uncertainty in the values that are used for the basic event probabilities. The code calculates this by propagating throughout the model the user-defined probability distributions for each basic event. The propagation of the basic event probability distributions results in a range of uncertainty for the entire model. Essentially, a new distribution is developed for the top event, based upon the individual input distributions.

Uncertainty analysis can be applied to any quantitative modelling technique, including fault tree analysis, reliability block diagram analysis, and event tree analysis. The UNCERT program requires only that the model be reduced to cutsets, or a cutset-like form i.e.: to a form that is a Boolean sum of products.

The Monte Carlo method selects random numbers, based upon the distribution of each individual basic event. The cutsets that are loaded into UNCERT are used to form a Boolean equation that

calculates the top event probability. The calculation of the top probability is repeated using several samples. The more samples taken, the greater the precision of the top event probability.

4.10.5 Uncertainty Fundamentals

The top probability is calculated from the cutsets using a user-defined calculation method. These methods apply different equations, in order to calculate the top probability. There are three common methods that are used to calculate the top probability in UNCERT. The first method calculates the module probability, by summing the cutset probabilities found in the module, as follows:

$$P(TOP) = \sum_{i=1}^{n} P_i$$

where P_i is the cutset probability, and n is the number of cutsets.

The second method uses the Min-cut Upper Bound calculation, as follows:

$$P(TOP) = 1.0 - \prod_{i=1}^{n} (1 - P_i)$$

The third method will uses the inclusion/exclusion principle, as follows:

$$P(TOP) = \sum_{i=1}^{n} P_i - \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} P_i P_j + - + ... + (-1)^{n-1} P_1 P_2 P_{3...} P_n$$

The first method is a rather straightforward method that involves adding each cutset probability to obtain a module probability. The third method is the most precise calculation, and requires significant calculation time. The second method gives an upper bound value of the module probability (which yields a conservative result), and provides the best combination of accuracy and speed. In general, the second method will be used to calculate the top event probability.

Once UNCERT begins sampling, it stores the calculated result (either internally or to the disk) for each sample. From these stored sample values, the fifth, median, ninety-fifth and various other statistics can be obtained. UNCERT also uses the stored values to produce plots of the cumulative probability, the probability density and uncertainty bars (bars that have the fifth, median, ninety-fifth and mean displayed).

4.11 Sensitivity Analysis

4.11.1 Purpose

Sensitivity analyses are carried out with the following objectives in mind:

a) to test the sensitivity of PSA results to certain changes in key input assumptions (different maintenance practices, testing procedures, mission times, etc.); and

b) to optimize the design by highlighting systems or subsystems that are especially large contributors to risk (e.g., human reliability model).

Objective (a) above involves the re-running of parts of the PSA work, with a modification made to a particular assumption or set of assumptions (e.g., revised definition of a fault tree top box). If results are shown to be especially sensitive to the particular assumption, then these results will be reflected in the operating and maintenance procedures.

Objective (b) above involves the calculation of importances for various systems or subsystems. The intent would be to initiate operations enhancements, if practical, on those systems that are especially large contributors to risk.

4.11.2 Scope and Methodology

The sensitivity of results (PDS frequencies) is tested for key aspects of the analysis, i.e.: different maintenance practices, testing procedures and mission time. This activity involves the re-running of parts of the PSA work (revised accident sequence quantification for the relevant sequences).

Initially, all the accident sequence frequencies in the specific PDS are summed. The impact of different maintenance practices, testing procedures and mission time on the summed frequency of each PDS is determined.

4.11.2.1 Items Covered in the Sensitivity Analysis

It is difficult to provide a detailed list of items to be covered in a sensitivity analysis for a generic methodology, since the ASQ analysis will generally be plant-specific. Sensitivity analysis will be performed when the initial ASQ for a given project is complete. Most items that are expected to be analyzed in the sensitivity analysis are related to the operating policy of the plant, e.g., maintenance practices, testing procedures and operating procedures.

4.11.2.2 Criteria Used for Identifying the Sensitive Items

When ASQ is completed, importance analysis is performed using the selected code. Based on the result of the importance analysis, items that are considered important will be selected for the sensitivity analysis.

4.11.2.3 Feedback of Sensitivity Analysis

Most items that are expected to be covered in the sensitivity analysis are related to the operating policies of the plant being analyzed. When an item is shown to be important as a result of sensitivity analysis the procedure dealing with the item is expected to be prepared, incorporating the recommendations from the PSA. The PSA is not expected to be updated to reflect the result.

4.12 Quality Assurance

The quality of the PSA is assured by using the following methods:

a) the analyst's informal day-to-day record keeping,

b) project operating instructions,

c) a review of PSA work, and

d) an update of PSA methodology,

e) archive the results for repeatability where possible.

4.12.1 Analyst's Informal Day-to-Day Record Keeping

Each analyst is required to maintain an informal record of his or her analysis, which will contain pertinent information such as descriptive material, correspondence, and notations regarding assumptions and supporting rationale. Each task in the PSA (e.g., system reliability analysis) will have associated with it a readily retrievable set of information that consists of entries made on a routine basis, as the analysis progresses. Examples of entries include the following:

a) design information used,

b) fault tree "top event" detailed descriptions,

c) assumptions used,

d) revision control,

e) outstanding or unresolved issues, and

f) comments.

While this record will not itself form part of the formal PSA documentation, it will be used in report preparation and as a means of verifying the steps of the analysis at a later date. This record must be submitted to a records management system, to be filed under the appropriate project and BSI/GSI number for archiving and retrieval.

4.12.2 Operating Instructions

Several operating instruction documents are typically prepared to ensure consistent application of methods by analysts. Examples of such project instructions include the following:

a) Rules for fault tree event labelling, and

b) Management of component reliability database.

4.12.3 Review of PSA Work

An on-going review of the work, rather than a review upon the completion of the study, is the most effective approach to assuring quality. It is also important that each major task of the PSA

be reviewed by people from different disciplines or with different perspectives, in order to ensure a high quality product.

A thorough review by the team leader of all aspects of the PSA work is required. One of the responsibilities of the team leader is to pay particular attention to assumptions that are made in the analysis, and to ensure consistency among different analysts, in addition to ensuring the accuracy of the analysis.

4.12.3.1 Familiarization with CANDU Design

A review of the plant design will focus on evaluating the success of the integration of the design information, the selection and grouping of initiating events, and the identification of success criteria for front-line systems. Adequate documentation to support the choice of success criteria will be provided.

Design personnel will review the analyses to ensure that the modelling is consistent with the particular CANDU design.

4.12.3.2 Event Tree Analysis

Event trees are reviewed, with particular attention being paid to the appropriateness of event headings and to the proper reflection of system and phenomenological dependencies in the event tree structure. Assumptions that are made in this regard are carefully documented and reviewed.

A standard procedure is used to initiate thermalhydraulics or other deterministic analyses that are required to confirm key assumptions made in the event sequence or event tree analysis. In this document, this analysis is referred to as a PSA support analysis. This required support analysis will be identified by the PSA team and documented in an analysis basis document for disposition by the safety analysis group. For each event that requires analysis, the analysis basis document will describe, as a minimum, the event sequence, success or failure criteria and system assumptions. The analysis requests are documented in the company's filing system.

4.12.3.3 Fault Tree Analysis

Fault trees are generally reviewed in their entirety; however, particular attention is paid to the top logic of the fault tree. It is in this portion of the tree that major logic errors may arise. The top events of fault trees are checked to ensure correspondence with the failure criteria defined in the event trees. Fault tree development is terminated at a level that is consistent with the available data.

4.12.3.4 Human Reliability Analysis

A review of the human reliability task ensures that potential sources of human error are taken into account. Each component that is placed in an inoperable position during testing, or is removed from service during maintenance, should also model human errors (which are

associated with the failure to restore the component to an operable state) in the appropriate fault tree, unless the probability of such errors is so low as to be insignificant.

4.12.3.5 Accident Sequence Analysis

During this review, particular attention is paid to truncation limits. Truncation is performed at the cutset level. Dominant accident sequences are reviewed to ensure that

a) the cutsets will actually cause the sequence to occur,

b) each event in the dominant cutsets is properly quantified, and

c) recovery factors reflect an understanding of the actions to be taken, as well as the plausibility of these actions under accident conditions.

4.12.3.6 Uncertainty and Sensitivity Analysis

A review of the uncertainty and sensitivity analysis ensures that proper ranges of values are used for the data, and that the major assumptions made in the analysis are addressed. Insights that are developed will reflect major findings associated with the dominant accident sequences and any plant design peculiarities identified in the study.

4.12.3.7 Review Process

The review and comment process complies with the project procedure for Analysis Reports. In particular, the review of the PSA will include the following:

a) Internal review (within the specific project and other projects)
   1) by PSA analysts, and
   2) by relevant system designers (e.g., AECL, and third party designers); and

b) External review (outside the specific project)
   1) by other experts within AECL.

4.12.3.8 Final PSA Report

The final PSA report is reviewed to ensure that

a) the findings of the study are clearly stated (and supported by the analysis),

b) the assumptions that are inherent to the analysis in general, and are related to systems or sequences in particular are clearly stated, and

c) information that is pertinent to the calculation of the frequency of dominant and near dominant sequences is presented in sufficient detail to allow the reader to duplicate these calculations.

4.13 Reporting of Results

4.13.1 Overview

The final step in performing the PSA is to integrate the data obtained in the various tasks of the analysis, and to interpret and present the results in a clear, concise and understandable way. The final report, including the presentation and communication of insights gained from the PSA study, is important and requires a considerable amount of time to prepare. This, however, is time well spent. A well—prepared, thorough analysis report serves as a reference for future analyses, and will enhance decisions on the part of the designer (AECL) and the utilities.

This integration of the analysis work into the final report will include the tabulation of frequencies for accident sequences that are important to safety and the development of distributions that reflect the uncertainties associated with accident-sequence frequencies.

The events from the generic list in the applicable revision of CNSC Consultative Document C-6 (References 4-2 and 4-3) are reviewed to show compliance with the dose limits given for each event.

To provide a focus for the assessment, the results are analyzed to determine the plant features that are the most important contributors to risk. These engineering insights constitute a major product of the analysis. Insight into the relative importance of various components and the relative importance of various assumptions to the results may be developed from the uncertainty and sensitivity analyses. A discussion of these insights provides additional perspective to the analysis.

4.13.2 Documentation

The following description of the documentation of a PSA is based on the Probabilistic Safety Analysis Procedures Guide, NUREG/CR-2815 (Reference 4-15), and is modified where necessary to conform to CANDU practice and needs. In particular, the PSA summary is briefer than that described in Reference 4-15, and is not intended for use in a high-level peer review.

The following subsections discuss the contents and documentation requirements of the PSA report in more detail. Portions of the following discussion have been taken verbatim from Reference 4-15.

There are several needs to be met by the documentation of a PSA. The assessment should:

a) communicate its essential results to the community of reactor safety specialists,

b) lend itself to high-level peer review,

c) permit detailed technical review, including substantial recalculation, and

d) accommodate extensions or adaptations of its basic models. In other words, it must be possible to build on the assessment.

The report should contain the following three major divisions:

a) an executive summary, which communicates the essential results and conclusions at a level that is useful to a wide audience of reactor safety specialists;

b) the main report, which integrates the entire study and detailed descriptions of the tasks and associated methodology, as well as conclusions that are presented in sufficient detail to support (together with the appendices) a detailed technical review; and

c) a collection of appendices that contain detailed computations and data to support the models and analyses presented in the main report.

4.13.2.1 Summary of a Probabilistic Safety Assessment (PSA)

The executive summary of the PSA should communicate the purpose, scope, tasks, results and conclusions of the study, with brief descriptions of each topic. These topics are discussed individually below.

4.13.2.1.1 Purpose

The purpose or objectives of the PSA should be clearly stated, with reference to the acceptance criteria of the study.

4.13.2.1.2 Scope

The treatment of scope should include the following items:

a) the major tasks of the PSA,

b) a summary of the location where the tasks are treated in the main report,

c) a description of the PSA team, including the name of the team leader and the names of the analysts responsible for the various tasks of the PSA, and

d) a description of the steps taken to monitor the technical quality as the study was performed (e.g., external review at major milestones).

4.13.2.1.3 Report Organization

In addition to providing an overview of the report's organization, this section should provide a link that relates the sections of the summary to the corresponding sections in the main report.

4.13.2.1.4 Tasks

The major tasks of the PSA are presented, with a brief description of their associated methodologies, relationships to each other, and interfaces with each other.

4.13.2.1.5 Essential Results and Conclusions

The results of the PSA should include the following:

a) confirmation that the design meets the frequency and dose requirements,

b) confirmation that all special safety systems meet the reliability requirement,

c) a list of the dominant accident sequences,

d) engineering insights into the relative importance of various system components and their overall effect on safety,

e) a list of design changes identified by the PSA, which require implementation to optimize overall plant safety and

f) the summed core damage frequency.

4.13.2.2 Main Report of a Probabilistic Safety Assessment (PSA)

The main report, together with the appendices, provides the information necessary for the detailed technical review. The inputs and outputs of the various tasks are a major part of the main report.

4.13.2.2.1 Report Integration

The main report should include a section that presents the overall organization of the study. This section would include

a) the purpose, objectives and scope of the PSA,

b) acceptance criteria with which the results can be compared,

c) a description of the structure of the study in terms of tasks and subtasks, and inputs and outputs for each task, and

d) a cross reference between the sections of the main report and the appendices.

4.13.2.2.2 Task Description

This portion of the report describes each task in depth, including a summary of the inputs and outputs for each task, and a detailed methodology for each task.

4.13.2.2.2.1 Input Data for Each Task

The information requirements for each task should be summarized. The source of each input should be defined, i.e.: the inputs that come directly from other tasks in the study, the inputs that are generated through iterative loops with other tasks, and the inputs that originate outside the study.

Inputs that are generated outside the PSA should be included either in the main report with specific sources cited, or in the appendices. Inputs that are generated within the PSA as outputs of other tasks are to be listed in the appropriate task section.

The limitations and assumptions of the available information and databases for each task should be discussed in the appropriate task section.

4.13.2.2.2.2 Methods for Each Task

Methods for most (but not all) of the tasks to be performed for a CANDU PSA are described in more or less detail in this GPSA methodology document. In some cases, reference is made to other documents for more detail regarding the methodology of particular tasks. The methodology section of the PSA should discuss the methods used to perform each task and subtask, as defined in this GPSA document, along with any additional tasks that are defined by the report.

The descriptions should be sufficient to permit the assessment, by a peer reviewer, of the adequacy of the methods for the purposes of the PSA. If special techniques or deviations from the specified methodology are developed during the process of performing the study, then these should be highlighted in the appropriate sections.

In general, the methodology for each task should cover the following:

a) The general methodology should be outlined, with comparisons being made to methodologies used in other accepted probability risk assessment (PRA) or PSA studies, if considered necessary. This is especially necessary where the methodology is new, or differs from accepted PRA or PSA methodologies.

b) Inherent limitations or assumptions of the methodology, or practical constraints encountered during implementation should be defined and discussed.

User manuals for computer codes should be referenced and a brief discussion of the code, consistent with the above methodology, should be provided.

Uncertainties that are associated with the limitations of the methodology should be quantified to the extent necessary to support the decision-making goals of the PSA.

4.13.2.2.2.3 Outputs of Each Task

The products or outputs of each task can be viewed as “results” of the PSA that are comparable in importance to the final core damage frequencies. Each task can be viewed as a “stepping stone” on the path to the final results of the PSA. For future users of the model, the intermediate results of the various tasks are as important as the final results. Moreover, a clear presentation of the intermediate steps is a prerequisite for a successful detailed technical review.

It is recommended that a table that lists the products or outputs of the various tasks and subtasks, similar to Table 7.2 in the Probabilistic Safety Analysis Procedures Guide (Reference 4-15), be provided.

4.13.2.2.3 Display and Interpretation of Results

In the presentation of results, the dominant accident sequences require special emphasis. A narrative description of each dominant accident sequence should be provided. This narrative should briefly discuss the nature of the initiating event, and the mitigating system failures involved in the sequence. The major contributing failures associated with each system failure should be presented. Any significant dependencies between the events involved in the sequence should be discussed. It is also useful at this stage to compare the dominant sequences with those of comparable plants.

The activities that are undertaken to ensure the completeness of the models should be addressed, with special attention being paid to the initiating events, the identification of failure modes associated with each event tree heading, and the identification of dependencies.

4.13.2.3 Appendices of a Probabilistic Safety Assessment

The appendices contain material of sufficient magnitude and level of detail to warrant its separation from the main report. Examples of this material are the system detailed fault trees, plant technical specifications, system descriptions, flow sheets, elementary wiring diagrams, PSA support analyses, component reliability databases and tables that list accident sequence quantification cutsets and importance measures.

4.14 References

4-1. USNRC, 1983, PRA Procedures Guide - NUREG/CR-2300: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, USNRC Report, NUREG/CR-2300, Volumes 1 and 2.

4-2. CNSC, 1980, Requirements for the Safety Analysis of CANDU Nuclear Power Plants, CNSC Consultative Document, C-6, Revision 0.

4-3. CNSC, In preparation. Requirements for the Safety Analysis of CANDU Nuclear Power Plants. CNSC Consultative Document, C-6, Revision 1, this revision is under review from the industry and is a Draft.

4-4. CNSC, 1987, Requirements for Reliability Analysis of Safety-Related Systems in Nuclear Reactors, CNSC Consultative Document, C-98, Revision 0.

4-5. DS&S, 1993, ETA-II Users' Manual for Version 2.1d, Data Systems & Solutions, Los Altos, Ca. Proprietary.

4-6. USNRC, 1990, Analysis of Core Damage Frequency: Internal Events Methodology, USNRC Report, NUREG/CR-4550, SAND86-2084, Volume 1, Revision 1.

4-7. CNSC, 1983, The Use of Fault Trees in Licensing Submissions, CNSC Consultative Document, C-70.

4-8. USNRC, 1981, Fault Tree Handbook, USNRC Report, NUREG-0492.

4-9. DS&S, 1993, CAFTA User's Manual for Version 2.3, Data Systems & Solutions, Los Altos, California. Proprietary.

4-10. DS&S, 1990, SAIPLOT User's Manual for Version 2, Data Systems & Solutions, Los Altos, California Proprietary.

4-11. IEEE, 1984, Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, Mechanical Equipment Reliability Data for Nuclear Power Generating Stations. IEEE Standard, 500.

4-12. SRI, 1983, Nuclear Plant Reliability Data System 1982 Annual Reports of Cumulative System and Component Reliability, Southwest Research Institute, San Antonio, Texas. Proprietary.

4-13 DS&S, 1993, Accident Sequence Quantification Using PRAQUANT, Data Systems & Solutions, Los Altos, California, Proprietary.

4-14. DS&S, 1992, UNCERT User's Manual Version 2.0, Data Systems & Solutions, Los Altos, California, Proprietary.

4-15. USNRC, 1994, Probabilistic Safety Analysis Procedures Guide - NUREG/CR-2815, Department of Nuclear Energy, Brookhaven National Laboratory Report, BNL-NUREG-51559.

4-16. D.A. Meneley, C. Blahnik, J.T. Rogers, V.G. Snell and S. Nijhawan, 1995, Coolability of Severely Degraded CANDU Cores, AECL Report, AECL-11110.

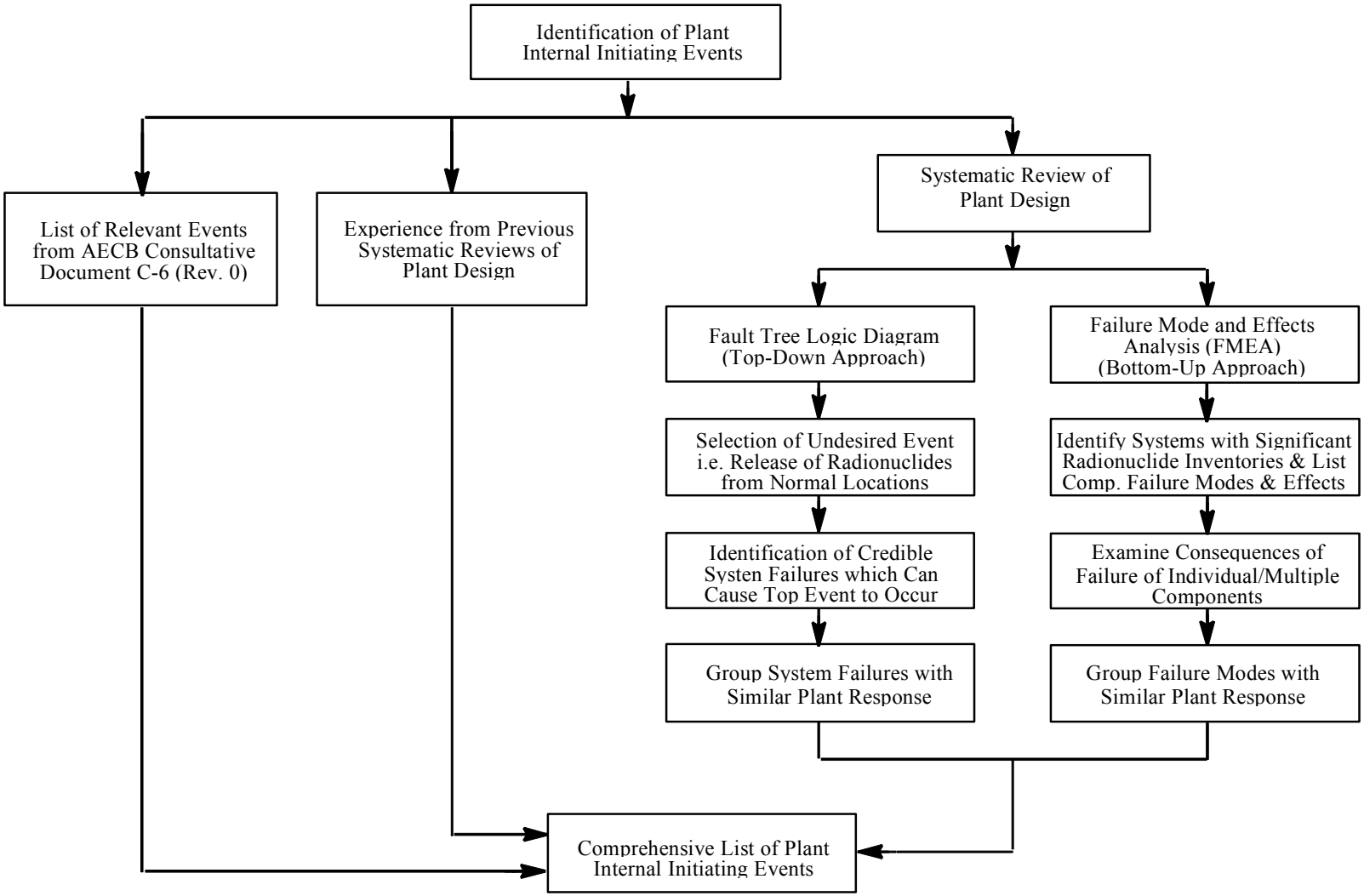


Figure 4-1 Plant Internal Event Identification

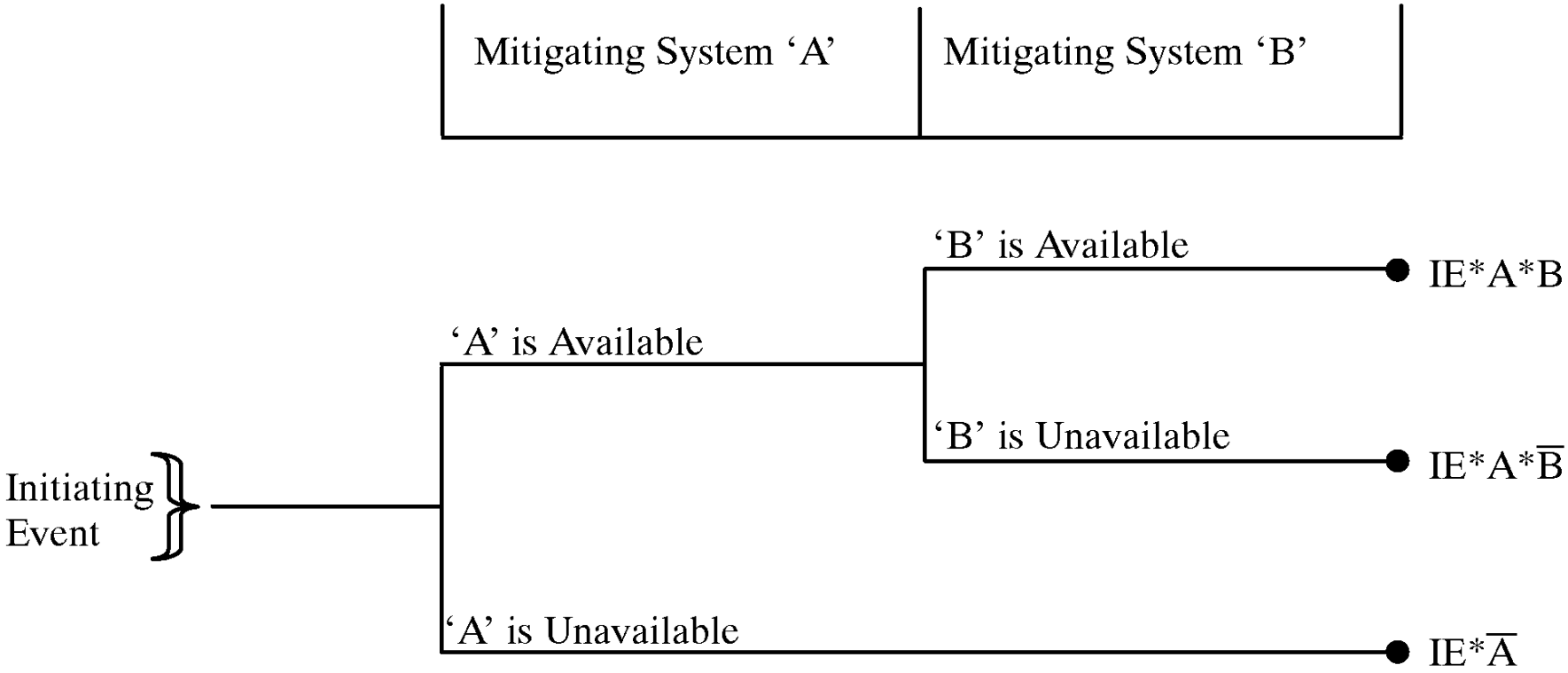


Figure 4-2 Simplified Example of an Event Tree

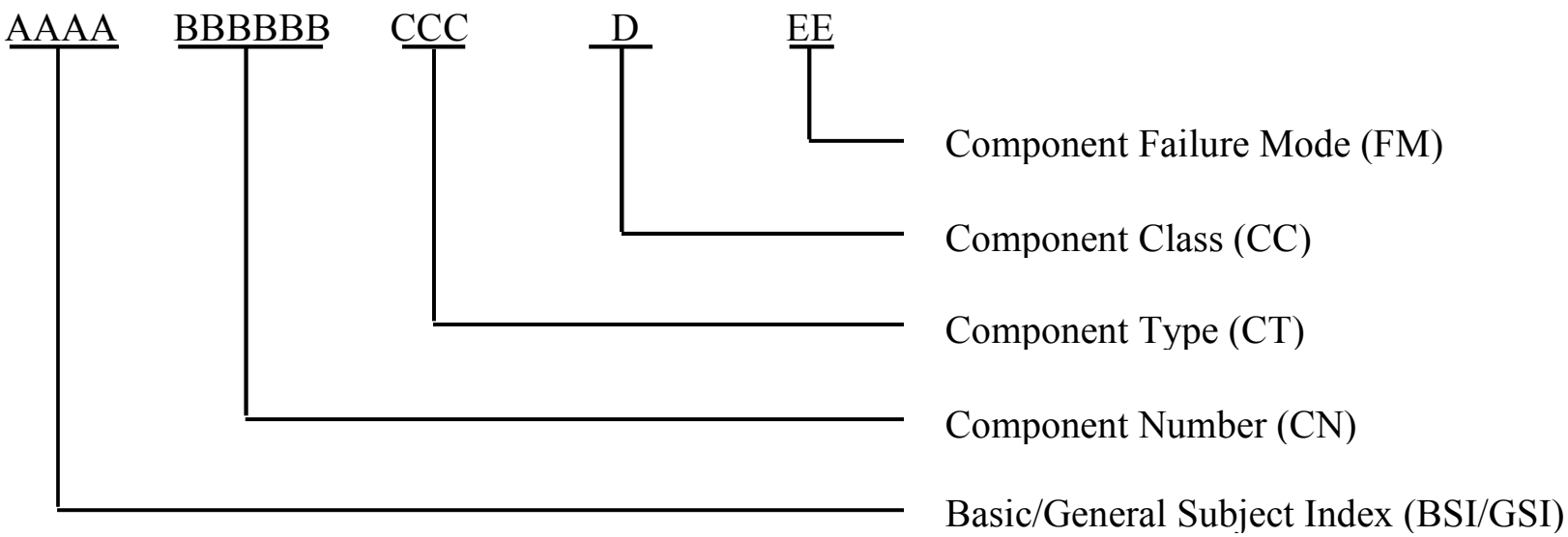


Figure 4-3 CAFTA Labelling Scheme for CANDU 6

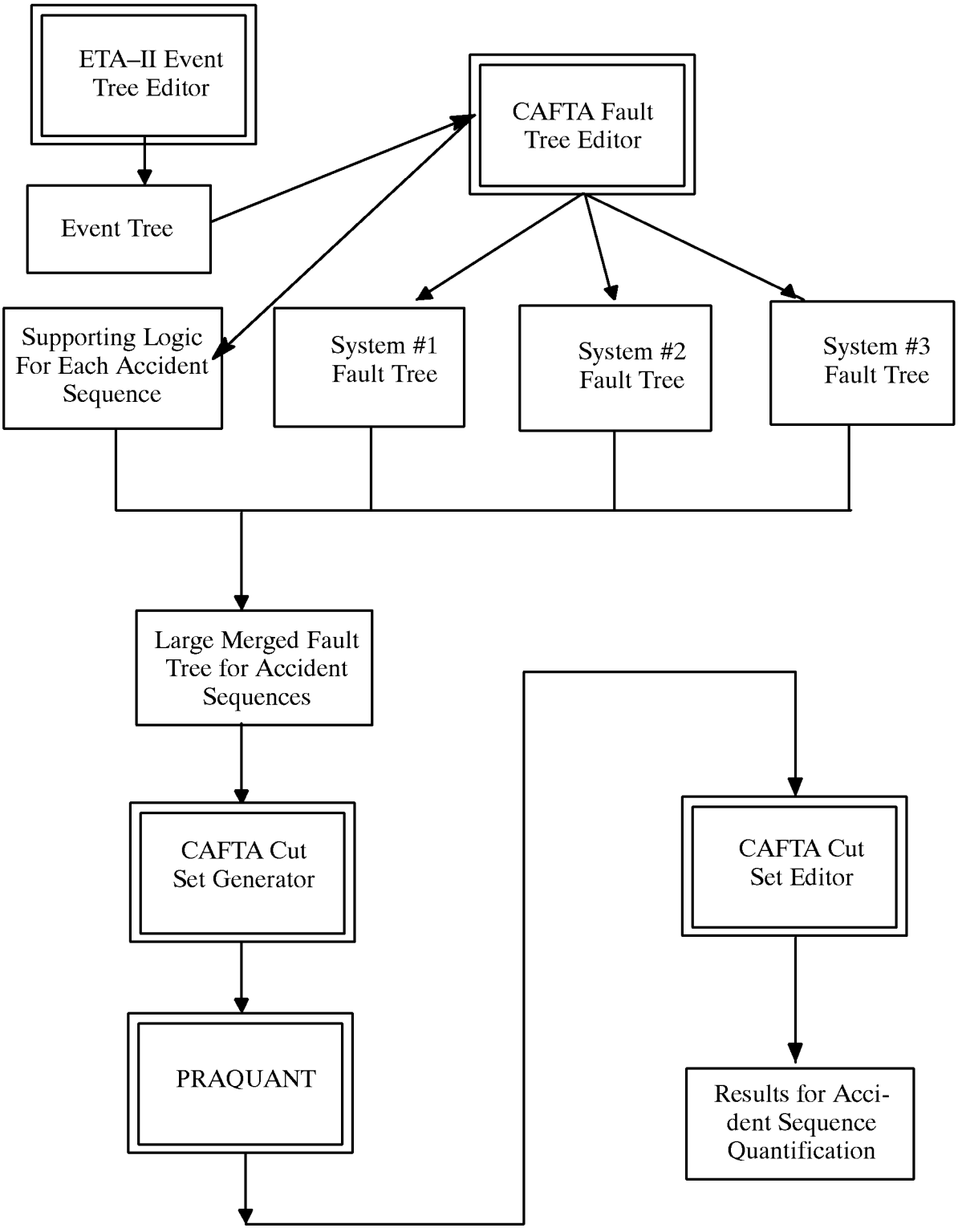


Figure 4-4 Analysis Procedure Using DS&S Codes

5. DEPENDENT FAILURE ANALYSIS

5.1 Introduction

In risk analysis, the treatment of dependencies in the identification and quantification of accident sequences is called "dependent failure analysis". Dependent events are those that are influenced by the occurrence of other events. In general, this means that the probability of a dependent event depends on whether or not the other events, which affect the dependent event, have previously occurred. Dependencies tend to increase the frequency of multiple, concurrent failures. Dependent failures are those failures that defeat the redundancy or diversity that is used to optimize the availability of some plant functions. This section describes the dependent failure analysis used in the GPSA.

Dependent failures involve two types of relationships: (1) explicit dependencies between components or systems, and (2) failure mechanisms that affect more than one component, but that are not explicitly identified in the systems analysis.

Numerous explicit dependencies are taken into account in the processes of event tree development, system reliability analysis and ASQ. These dependencies can be broken down into the following main categories:

a) Functional dependencies

These are dependencies among systems or components that follow from the plant design philosophy, system capabilities and limitations, and design bases. In some cases, a system or component is not used or needed unless other systems or components fail. For example, certain pumps may be held in a standby mode, ready to operate upon the failure of running components. Another example is a system or component that can only function in conjunction with the successful operation of other systems. Failures within support services, such as instrument air or service water, can cause multiple failures in front-line systems that are functionally dependent on them. Many dependencies result from other types of equipment sharing. For example, components in different mitigating systems are, in some cases, fed from the same electrical bus.

Obvious functional dependencies are modelled explicitly in the event trees. A simple example is the low-pressure recirculating mode of ECC, which is only credited after the success of the high pressure and medium pressure injection modes. More subtle dependencies are explicitly modelled, when fault trees are merged during ASQ. Consistent application of the fault tree event labelling scheme among different mitigating and support systems ensures that dependencies are properly treated during the Boolean reduction.

b) Physical interactions

Physical phenomena that can impact multiple systems and components are, in many cases, explicitly considered. For example, mitigating systems that are not environmentally qualified for severe environmental conditions created by an initiator such as a LOCA, are not modelled in the event trees for that initiator. Similar dependencies are analysed in the seismic, internal fire and flood analyses, where the initiating event itself can render multiple

systems inoperable. For the treatment of seismic, fire and flood events, see Sections 7, 8 and 9 respectively.

c) Human interactions

These are post-accident operator actions that are usually modelled in the event trees, and pre-accident actions that are modelled in the fault trees. Various mitigating systems depend on manual initiation by the operator. An operator's failure to diagnose an event or perform certain critical tasks to start a system may increase the likelihood of operator failure on subsequent tasks. In some situations, undamaged systems, which could be called upon to mitigate an accident, may be initiated too late or not at all, because of previous operator errors. Pre-accident action dependencies are based on the same premise—a mistake made on one task increases the probability of failure on later tasks that are performed closely in time. For example, a single individual could potentially miscalibrate three redundant components during a single shift. The probability of this event would be higher than the product of each individual error, if considered independently.

Many CANDU systems incorporate redundant components to increase reliability. Apart from the explicitly modelled dependencies described above, historical component reliability data indicate that a variety of additional causes can render multiple redundant components simultaneously unavailable. Often, these types of failure can have a significant effect on system reliability, because they inherently defeat redundancy. Examples include such things as common design faults, or local, non-energetic harsh environments. Due to the rarity of these so-called "common cause failures" (CCFs), it is difficult to obtain frequency of failure estimates for each cause. Furthermore, it is difficult for the systems analyst to ensure that all possible causes are individually taken into account, and it is impractical to include many CCF events in the fault trees. For these reasons, CCFs are modelled implicitly, in the sense that a single fault tree basic event is used to capture all of the possible causes. Identically labelled CCF events are introduced as inputs to an "OR" gate, adjacent to each redundant component's independent failure modes, in order to model the failure dependency. The failure rate for these events is usually based on the total component failure rate and a number of additional parameters that are derived from generic CCF data and expert judgments.

5.1.1 Selection of CCF Analysis Method

The Unified Partial Method (UPM) (Reference 5-1) is a method that enables CCFs to be quantified either at the system level by estimating a system cut-off probability, or at the component level by estimating a beta-factor for sets of similar components. The "unified" part of the method title refers to the unification of the cut-off system level approach and of the partial beta component level approach. UPM requires the analyst to examine the potential vulnerabilities of a system (or of sets of similar components within the system) to CCF in a systematic and thorough way. Thus, UPM forces the dependent failure analyst to carry out a thorough qualitative analysis of a system, while quantitatively estimating the probability of CCF. The benefits of a coherent approach that incorporating both qualitative and quantitative analyses are thus realised. One of the main conclusions from the Common Cause Failure Reliability

Benchmark Exercise (CCF-RBE) (Reference 5-2) stated that it is essential to combine qualitative and quantitative methods when performing CCF analysis.

Numerous alternative approaches to the quantifying of CCF probabilities exist. Each approach has its own inherent advantages and disadvantages, in terms of ease of use by the analyst and adaptability to CANDU system reliability analysis. Ideally, any technique would be able to incorporate CANDU-specific CCF data into the calculation of CCF basic event probabilities. However, since CANDU data for CCFs have never been explicitly collected, it is necessary to rely on CCF data from other sources, such as PWRs and BWRs. The UPM is calibrated to this type of generic CCF data, and allows the analyst to take credits or penalties for design features and maintenance/operating practices that alter the potential for CCFs, by assigning beta-factors within a certain range. Since its results are tailored to the system being analyzed, the UPM is preferable to using published data for the parameters of other CCF models, such as the Multiple Greek Letter (MGL) technique. Although a rigorous methodology for obtaining more relevant parameters for MGL or other methods is presented in NUREG-CR-4780 (Reference 5-3), it is necessary to have access to CCF event reports, and the methodology is best suited to situations in which generic MGL parameters can be subjected to Bayesian updating with plant-specific information. Therefore, the UPM has been selected over other CCF models for use in the GPSA.

5.1.2 Background of UPM Methodology

UPM is a development of the Partial Beta Factor method for assessing CCFs at the component level (Reference 5-4). The Partial Beta Factor method was originally proposed as a way of decomposing the overall assessment of a simple beta factor into a series of judgments relating to identifiable topics, which all have an impact on redundant component vulnerabilities to CCF. A total of 19 such topics were included. The analyst was required to assess a partial beta factor for each of these topics. The value that was selected had to be between a specified minimum and unity, based on the features of the set of components under review. An overall beta factor was then calculated, by multiplying all 19 partial beta factors together. The minimum partial beta factors were adjusted, so that there was a lower limit of beta = 0.02 for systems with identically redundant components, and a lower limit of beta = 0.001 for systems that incorporated engineering diversity.

UPM represents a development of the original partial beta method. The 19 topics requiring assessment in the original model have been consolidated into eight causal groups. This consolidation reduces the amount of analysis and time required. Also, instead of assessing a value for a particular partial beta factor between the stated minimum and unity, the UPM requires the analyst to choose one of five system definitions that most closely matches the system under review. This feature means that consistency between different analysts is easier to achieve, although specific guidance on the interpretations of the system descriptions may still be required for a particular project. Finally, a partial cut-off approach has been developed and incorporated within UPM. This approach uses the same model structure as that for the partial beta factor approach, except that it calculates a system cut-off, or limiting CCF probability, by modifying the factor definitions and the calibration appropriately.

5.2 Main Features of UPM

The Unified Partial Method has the following features:

- UPM provides a framework, within which qualitative and quantitative assessment can be combined. This is essential when carrying out a CCF assessment.
- The method in UPM builds on and refines previous models and analysis. UPM is a development of the Partial Beta Factor method and includes a means of calculating a system cut-off, if this is the required output of the analysis.
- UPM provides a means of examining the potential vulnerabilities of a system (or set of components) to CCF, and records the judgments that have to be made in the assessment. Therefore, an auditable trail of these judgments is produced as an integral part of the CCF assessment.
- The quantitative aspects of the method are calibrated to historical data from the civil nuclear power industry. By examining a system's defences against CCF, the most relevant parts of this historical data are used. It is possible to recalibrate the weighting factors if suitable plant-specific data are available; this process is discussed in Appendix C of the UPM workbook (Reference 5-1).
- UPM allows both system level cut-off assessments and component level beta factor assessments to be carried out.
  a) For multi-train systems, a system level assessment is undertaken if detailed fault tree models are not available. Basically, an overall system reliability is estimated, based on the assumption that it is dominated by CCFs. The system reliability estimate is therefore based on a qualitative comparison of the features of the system being modelled and historical experience and judgement of the reliability of multi-train systems.
  b) When detailed fault tree models are available, a component level assessment is used. This approach produces "beta factors", which are applied to the failure probabilities of redundant components. CCF events are added to the fault trees to reflect the failure dependency of the components in the group. Unlike standard beta factor techniques, credit may be claimed within the assessment for levels of redundancy that are beyond duplicity. Therefore, for a situation in which one out of three components must operate for success, the calculated CCF probability is lower than it would be for a simple dual redundancy case.

Although UPM deals with the CCF subset of dependent failures, it is not claimed to be a 'universal' dependent failure assessment methodology, but rather a "practical approach for standard systems". The UPM workbook (Reference 5-1) specifically mentions the following limitations, which are common to most CCF assessment methodologies:

- The method does not aim to assess dependency between multiple human operators, or between operator actions on multiple systems. However, it can be used to assess the human element in dependency between hardware failures. For further discussion of this issue, see Section 5.3.6.3.

- The method is not intended to account for functional dependencies. Where equipment operation depends on the functioning of common service systems, these shall be modelled explicitly.
- The special case of systems that incorporate software is specifically placed outside the scope of UPM.

The UPM workbook (Reference 5-1) guides the analyst through the steps of the method, and includes specific advice on the correct interpretation of the various subfactors that are considered. The structure of the UPM workbook has been designed to try to ensure the consistent application of the method for all of the subfactors involved. A brief description of each of the sub-factors is provided below. More detailed explanations can be obtained from the workbook.

1. Redundancy (and diversity): Increasing levels of redundancy result in a reduced likelihood that all the components in a group will fail. Diversity among redundant components will guard against many causes of multiple component failures.
2. Separation: Increased separation among redundant components makes them less vulnerable to certain environment-related CCFs.
3. Understanding: The intention of this sub-factor is to address the fact that certain CCF mechanisms or non-obvious functional dependencies will likely be missed at the time of design, particularly if a system is novel or complex.
4. Analysis: If designers are aware of CCF issues and receive feedback from reliability analysts at the time of design formulation, then credit may be taken for reduced CCF probability.
5. Man Machine Interface (MMI): This sub-factor is used to account for the possibility of human actions affecting multiple components. Better procedures, limitations on human interaction, and the checking and testing of maintenance actions all serve to reduce the CCF probability. See Section 5.3.6.3 for a discussion of this category in the context of the larger PSA.
6. Safety Culture: The level of staff training affects the probability of human actions that result in failures of multiple components, especially those actions that may be contrary to the express policies and procedures of the plants.
7. Environmental Control: The less human or machinery traffic that exists in an area, the less likely it becomes that a CCF will be induced. Also, by limiting the number of local sources of potential environment-related CCFs (e.g., temperature, moisture), the probability of such failures is reduced.
8. Environmental Testing: Here, emphasis is placed on the benefits of verifying manufacturers' claims for environmental qualification. Lower CCF probabilities are claimed, when for example, units are subjected to a variety of tests to the point of failure.

5.3 Application of the Unified Partial Method for CCF Analysis

5.3.1 Selection of Common Cause Component Groups

The most important, and perhaps the most difficult task in a component-level CCF analysis is the definition of the component groups. The importance of this selection process is related to the final results of the analysis. The inclusion or exclusion of different types of components in the scope of the CCF modelling, and the number of components encompassed by each CCF basic event in the system logic model can have a very large influence on the predicted system reliability. This influence is expected to be much larger than the particular CCF model (e.g., UPM vs. MGL) employed in the analysis. The difficulty arises because no matter how systematic or detailed a CCF group selection procedure may be, it is always subject to the judgment and experience of the analyst using the procedure. Therefore, inconsistency between analysts is always possible, both in the identification of CCF groups and in their quantitative evaluations. However, some general guidelines can be put forward to minimize inconsistencies. The following guidelines are adapted from NUREG-CR-4780 (Reference 5-3), with some additional points:

- When identical, functionally non-diverse and active components are used to provide redundancy, these components should always be assigned to a conceptual common cause group for analysis purposes. In general, as long as there are common cause groups of identical redundant components that are already identified (within the same system), the assumption of independence among diverse components is a good one, and is supported by operating experience data. In other words, very few CCF events have been observed for diverse components, so any groups of identical components dominate in terms of overall system unavailability. When diversity is present in a CCF group, the UPM allows credit to be taken for that diversity in the form of a lower beta factor.
- When diverse redundant components have piece parts that are identically redundant, the components should not be assumed to be fully independent. One approach, in this case, is to break down the component boundaries and identify the common piece parts as a common cause component group. This should not be an issue for CANDU system reliability analysis, as the fault trees will have a high degree of resolution.
- In systems reliability analysis, it is frequently assumed that certain passive components can be omitted, based on arguments that active components dominate. In applying this principle to common cause analysis, care must be exercised to not exclude such important events as debris blockage of redundant pump strainers, etc.

The identification of potential members of a CCF group is facilitated by examining system flow sheets or existing fault trees for redundant components. Also, a search for common attributes among components may be of some use. These attributes might include such things as:

- component type, e.g., pneumatic valve, radiation monitor,
- component use, e.g., system isolation, parameter sensing,
- component manufacturer,

- component internal conditions, e.g., pressure range, temperature range, normal flow rate, power requirements, etc.,
- component external environmental conditions, e.g., temperature range, humidity range, barometric pressure range, etc.,
- component location,
- component initial state or operating characteristics,
- component testing procedures and characteristics, e.g., test interval, test configuration, etc., and
- component maintenance procedures and characteristics, e.g., planned, preventive maintenance frequency, maintenance configuration, effect of maintenance on system operation, etc.

Once the analyst has identified potential groups of similar components based on the recognition of parallel trains on flow sheets or similar characteristics, the components must be formally grouped for inclusion in the system fault tree. Even though two components may be of similar type, use and manufacturer, they should not necessarily be assigned to a CCF component group. The essential question that must be answered is, "Are they in fact redundant?" If either component can, by itself, cause a system failure, then there is no need to create a CCF basic event for both components, since the independent failures of both will dominate the CCF probability. In determining the number of components that should be included in a given CCF group, a good rule of thumb is to include as many identical components as are sufficient to cause system failure. In other words, the CCF basic event should usually be a minimal cutset. Therefore, the ANDed independent failures of the components in the group result in a system failure. The inclusion of more components will result in irrational CCF modelling assumptions and optimistic results, as shown in the following example.

Consider four pneumatic valves, designed to isolate two separate lines that are located at opposite ends of a building. The isolation function of each line has dual redundancy (valves in series), as shown in Figure 5-1.

System failure is defined as the failure to isolate either of the two lines. If a common cause component group ABCD is selected, then there are more valves in the group than are necessary to give a minimal cutset. If a beta factor is worked out for the four-valve combination, then credit will be taken for the large separation between AB and CD. However, this is misleading, because the failure of just CD (or AB) will result in system failure, and these two valves are quite close together. Intuitively, one expects that a CCF event that causes two nearby valves to fail open is more likely than one that fails four separated valves. As a result, it is more sensible to assign the valves to separate groups AB and CD. In the case of the ABCD grouping, the results would be optimistic, even if no credit were taken for the enhanced separation. This result is optimistic, because there would only be one minimal cutset, whereas with the two-valve grouping, there would be two independent cutsets of equal probability.

There are also pitfalls that are associated with the inclusion of an insufficient number of components in a CCF group. The air supply to valves A and B from the previous example can

be used to illustrate. Each valve is supplied through redundant solenoid valves, which are pneumatically connected in series as shown in Figure 5-2.

From the standpoint of a single pneumatic valve, there is dual redundancy. However, the failure of SV-1 and SV-2 will fail only valve A, and not the entire system. Since any root cause of multiple component failure is likely to affect all four of the closely-spaced solenoid valves, the appropriate grouping is SV-1234. This grouping will also be conservative, compared with the alternate groupings of SV-12 and SV-34. For this grouping to be non-conservative, the sum of the probabilities of the second order cutsets SV-12*B, SV-34*A and SV-12*SV-34 would have to be higher than the probability of the first order cutset SV-1234. This condition will not be satisfied in this and most analogous situations, unless the independent failure probabilities of the isolation valves are orders of magnitude above those of the solenoids.

It should be noted that the loss of the physically meaningful second order cutsets (e.g., SV-12*B in the above example) is an artefact of all beta factor CCF techniques. MGL and other methods have the advantage of preserving such combinations, by taking into account partial CCFs out of a larger group. However, this can lead to a proliferation of cutsets, without significantly altering the calculated system reliability.

5.3.2 Fault Tree Construction Considerations

Once the common cause component groups have been identified, it is, of course, necessary to incorporate the appropriate basic events into the fault tree logic model. The easiest means of doing so is to add *identically named* CCF events that are adjacent to each basic event; each basic event represents the independent failure of a redundant component. An example is shown in Figure 5-3, where the event “E,F FAIL - CCF” is OR’d with the independent failures of both “E” and “F”. In some cases, it may be possible to restructure the fault tree in a logically equivalent fashion, such that the CCF event need only appear once. However, this is not recommended, because it does not follow the principle of immediate cause and can make the logic more difficult to trace. It is preferable to show CCF as a failure mode of each component, as in Figure 5-3.

The output of the UPM is a beta factor, which may be multiplied by the component total random failure probability to obtain the CCF failure probability:

$$P_{CCF} = \beta P_{TOTAL}$$

where $P_{TOTAL} = \lambda T$ (running failure)

$$P_{TOTAL} = \lambda \frac{T}{2}$$ (dormant failure)

As shown, the total random failure probability is a function of the total random failure rate, λ, and a time parameter, *T*. The time *T* is equal to the mission time for running failures. For dormant failures, it is the test interval. When two components that are part of the same CCF component group have different test intervals, the UPM workbook (Reference 5-1) suggests that one of the two values be used. When the CCF component group is not a dominant contributor to

system unavailability, it is simple and conservative to use the longer test interval. Otherwise, the geometric mean of the test intervals should be used, in order to obtain a better estimate for P_{TOTAL}:

$$T = \sqrt{T_1 T_2} \quad .$$

When the fault tree structure shows the failure of a component being broken down into various failure modes, it is necessary to sum the probabilities of each mode to obtain the total random failure probability, P_{TOTAL}. However, if it is felt that the beta factor should be different for different random failure modes, or that different failure modes are tested for at different intervals, then two or more CCF basic events will have to be created next to each independent failure event. Also, note that other causes of component unavailability are to be excluded from the CCF analysis. If, for example, unavailability due to maintenance is modelled for redundant components, then it makes little sense to apply a separate beta factor to these events or to include them in the failure probability sum. The beta factor is meant to be applied to the total *random* failure probability only. This is not to say that multiple redundant components cannot be unavailable due to personnel oversights during maintenance, but rather that this remote possibility is taken into account within the beta factor that is applied to the random failure probability.

Another point to consider is that the failure rate data in AECL's databases likely counts both single, independent failures and CCFs. Therefore, the use of these failure rates to obtain the independent component failure probabilities represents double-counting, wherever CCFs are modelled. In theory, the independent failure probability, P_{INDEP}, should be calculated as follows:

$$P_{INDEP} = (1-\beta)P_{TOTAL} \quad .$$

Since β is typically less than 0.1, the effect of using P_{INDEP} instead of P_{TOTAL} on the overall system unavailability will be minimal, because the CCF events will be dominant. As the change would require an enormous amount of editing to existing fault trees or databases, it is recommended that P_{INDEP} be taken to be equal to P_{TOTAL}.

5.3.3 Fault Tree Event Labelling Scheme

As described in the previous section, the beta factor shall be applied to the total random failure probability. In some parametric CCF methods, the beta factor is instead applied to the failure rate. The reasons for using the probability and not the failure rate are related to the nature of the UPM, and the fault tree event labelling scheme and software used at AECL.

The main problem with creating CCF failure rates is that the UPM produces beta factors that are very specific to the component groups being examined. Consider six identical valves, assigned to two common cause component groups having two and four valves, respectively. The levels of redundancy and separation among the valves in each group may be quite different, so different beta factors would be assigned to each group. Therefore, a variety of CCF failure rates would be necessary, even for the same type of component. Since there is not much flexibility to devise CAFTA-type codes for each of these failure rates, it is much easier to just create basic events with assigned probabilities in the fault trees.

A related issue concerns the method for labelling the CCF basic events in the fault trees. Ideally, the labels should identify all of the components within the group for better clarity. Basically, the labelling scheme for CCF divides the CAFTA 16 character event label into 3 fields. These are the Basic Subject Index (BSI), Component Number (CN) and Failure Mode (FM) fields. A CCF event may encompass several failure modes; therefore, it is proposed that the FM field be increased to three characters, invariably containing the characters "CCF". This will make it easy to pick out CCF events from printed basic event listings. Note that the increase to three characters is only conceptual, and does not imply a change to the CAFTA parameter files. Since the CCF events will have assigned probabilities, the event labels can be arbitrarily assigned. Therefore, none of the characters in the CCF event label shown below are automatically linked with the CAFTA type code database:

BSI				CN									FM		
—	—	—	—	—	—	—	—	—	—	—	—	—	C	C	F
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

The last character (#13) of the CN field can be used to differentiate between different types of failure, as is done in the standard labeling scheme. In this way, separate CCF events for both starting and running failures can be included, if required. The standard symbol for mission unreliability is "+", and the symbol for dormant unavailability is "$". Note that in the CCF event label, these are not intended to indicate the CAFTA calculation type. All CCF events have assigned probabilities. However, implicit in every CCF event are the underlying independent basic events, which usually represent either running or dormant failures. If only one failure mode exists and it is obvious from the context or event description, then character #13 may be used as part of the component identification. A few examples illustrate the approach.

Example #1: SDS2 quick opening valves PV-1G, PV-1H and PV-1J fail to open on demand, due to a CCF.

BSI				CN									FM		
3	4	7	1	P	V	1	G	/	H	/	J	$	C	C	F
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Example #2 Standby diesel generators SG1 and SG2 fail to start on demand, due to a CCF.

BSI				CN									FM		
5	2	1	1	S	G	1	/	2	-	-	-	$	C	C	F
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Example #3 Standby diesel generators SG1 and SG2 fail to run during their mission, due to a CCF.

BSI				CN									FM		
5	2	1	1	S	G	1	/	2	-	-	-	+	C	C	F
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Where there are high levels of redundancy, it may be difficult to itemize all of the component numbers in the group under the "CN" field. In such cases, it is left to the analyst to decide how they may be best described in the space available. A listing of the components that are included in the group should be reported in the documentation that is produced.

5.3.4 Calculation of Beta Factors

5.3.4.1 Screening Analysis

Having identified a common cause component group and created an appropriate fault tree basic event, the analyst must then calculate a beta factor, and hence, a basic event probability. Since the UPM incorporates an in-depth qualitative assessment for each component group, the time required by the analyst to document his or her assumptions, and to fill out the UPM "judgment tables" to arrive at a beta factor may be substantial. Therefore, a quantitative screening shall be performed before applying the UPM directly.

NUREG-CR-4780 (Reference 5-3) suggests using a quantitative screening value of β=0.1 for each CCF basic event. This value should be conservative for most situations, although conservatism is not the main objective of the screening. The intent is to help the analyst to identify the common cause component groups that contribute most to the top event unavailability of a given fault tree. This determination can be made by examining the top 100 minimal cutsets or, alternatively, by examining the importance measures of the fault tree solution. Then, the probabilities of the selected CCF events can be refined using the UPM procedure, and the fault tree can be re-evaluated.

5.3.4.2 Detailed Analysis

The UPM must be applied to those component groups that survive the quantitative screening. The method is structured to provide a framework that allows the analyst to first carry out a structured assessment of the vulnerability of a system to CCF, and secondly, to record the process of the assessment in an auditable manner.

There are five main steps to the UPM, as detailed in the manual (Reference 5-1):

1. The system to be analyzed must be clearly defined. It is necessary to define the physical boundary of the system, i.e.: the components and parts of the system that are to be considered in the analysis. See Section 5.3.1 for further discussion of this step, which is not unique to the UPM.
2. The level of assessment must be established. Is the CCF analysis to be carried out at a system (cut-off) level, or at a component (partial beta factor) level? For CANDU 6 and CANDU 9 PSAs, a component level assessment is appropriate, because system reliability calculations will be made using detailed fault trees. See Section 5.2 for further information.
3. The judgement tables must then be consulted for each subfactor. Each table relates to a different aspect of system design or operation, including its effectiveness in defending

against CCF. Out of the five system descriptions that are listed in the tables, the analyst must choose the description that most closely matches the system under consideration. The justification for the choices must be recorded in tables for each CCF component group, using the format shown in Table 5-1.

4. The estimation table, which summarizes the judgements made in the previous step, must then be filled in. This step can be combined with step three, by obtaining the numerical values for each subfactor from the UPM estimation table, and by entering the information in Table 5-1. This step constitutes the bulk of the analysis.
5. Finally, the value of the system cut-off or component beta factor is to be calculated, as appropriate.

After obtaining the beta factor, the CCF probabilities should be calculated, and the values should be incorporated into the fault tree, in order to replace the screening values. The fault tree should then be re-evaluated to obtain the final result.

5.3.5 Component Types and Boundaries

The types of components listed in Table 5-2 are to be modelled as part of CCF analysis. They have been selected, based on the criteria listed in Section 5.3.1. That is, these components are active, and appear in non-diverse, redundant structures within CANDU plants. Passive components are also considered in a few limited cases. The entries in this table are not intended to be an exhaustive listing for all projects, but rather a minimum requirement based on the types of components for which generic beta factors have been collected (References 5-5, 5-6, 5-7, 5-8).

In order to reduce the number of basic events that are added to the fault trees during CCF analysis, the component boundaries shall be enlarged, if practical, to encompass a larger number of parts. For example, rather than introducing three basic events that represent the mechanical failures, motor failures and C&I failures of redundant pumps, a single basic event shall be generated. In calculating the CCF probability, the analyst must be careful to sum the failure probabilities from each of these sources, while excluding the contributions from external support services (e.g., power supplies, cooling water). Contributions from control logic may be obtained by creating modules in the fault tree to obtain the unavailability of intermediate gates. Table 5-2 lists the expanded component boundaries, where applicable.

For the special safety systems (SDS1, SDS2, ECC and containment), detailed modelling shall be performed for instrumentation that initiates trips on the various 2 out of 3 channels. The intervening relay logic that is to be activated between instrumentation and the components should be grouped into a single CCF basic event, if possible.

Figure 5-4 shows an example of the way in which the CCF events may be added for components with expanded boundaries. The example shows a subtree of the shutdown cooling system normal mode fault tree, in which running failures of pump P1 are modelled. The logic is repeated elsewhere in the fault tree for the redundant pump, P2. The subtrees for the two pump sets are “ANDed” in the higher-level logic. Two CCF events are shown under the subtree “top”, “33410 PUMP SET 1 FAILS WHILE RUNNING”. Running failures of P1 and P2 are modelled

by the CCF event labelled "B". The failure probability for this event is derived from the sum of the failure probabilities of the basic events labelled "A" and the appropriate beta-factor. CCF event "D" represents spurious failures of motorized valves, which can cause flow bypasses in both pump loops. The basic events labelled "C" are included in the CCF probability estimate for event "D". In this example, the calculation is simple, because generic C&I models have been used for the pump and motorized valve control circuitry.

For CCF events that survive the quantitative screening process, application of the UPM may be complicated for some components, since their physical locations may be separate from their C&I locations. Therefore, different beta factors might be assessed for C&I failures and mechanical failures. If the contribution from C&I is less than an order of magnitude below the mechanical failure modes, then it is sufficient to apply the UPM only to the mechanical failures, and retain the screening value for the C&I parts. Otherwise, more than one beta factor should be generated, and the contributors to the CCF basic event should be documented with separate judgment tables (see Section 5.3.4.2).

5.3.6 Additional Considerations

There are a number of additional aspects of CCF analysis using the UPM that are open to interpretation by the analyst. The topics presented in this section are meant to provide some guidance on various issues that are not discussed in detail in the UPM workbook.

5.3.6.1 Running/Standby Systems

For running/standby systems, the question arises as to whether the beta factor should be applied to the dormant failure probability of the standby component, or to the mission unreliability of the running component. The UPM manual suggests that the calculation is complex, since two sequences of failure can be postulated: (1) the running item fails with the standby item having failed since its last test, or (2) the standby item fails and propagates the failure to the running item. However, since neither of these sequences would seem to represent a likely CCF, a fairly simple methodology for running/standby CCF events is proposed here.

According to the UPM manual, a CCF is defined as "a dependent failure event where simultaneous or near simultaneous multiple failures result from a single shared cause." Although the definition of what constitutes "near simultaneous failure" is somewhat arbitrary, sequence (1) does not appear to meet the definition. If the mission reliability of a mitigating system is being evaluated, then the fact that the running item is assumed to be working at the beginning of the event is evidence that a CCF is not present at that time. Therefore, any failure of the standby item before the initiating event must be an independent failure. The exposure time for the CCF event is therefore the mission time, and the beta factor shall be applied to the mission unreliability.

Another possibility is a mitigating system with redundant standby components that are not activated until after an initiating event. In this case, there are two apparent CCF events. One is the failure of both redundant standby components to start, in which case the beta factor is applied to the dormant unavailability. The other CCF event probability would be derived from the

mission unreliability, and would involve the running item's failure and impairment of the starting/running of the second standby item.

Sequence (2), as described at the beginning of this section, is rather implausible, because it implies that a de-energized standby component can cause failures of running items. The reverse case is much more likely, since a running item may be a source of fire, flood or missiles. However, these types of dependency are usually taken into account in special analyses for the fire, flood and seismic events, and are therefore beyond the scope of the UPM or other CCF methods.

Running/standby component CCFs will be modelled according to the following rules:

a) If one or more CCF components are running prior to the initiating event, then one CCF basic event shall be created. The CCF probability will be based on the running failure rate, mission time and beta factor.

b) If the running/standby components are dormant prior to the initiating event, then both the failure to start and the failure to run shall be modelled, requiring two CCF basic events. The failure-to-start CCF probability will be based on the dormant failure rate, test interval and beta factor. The failure-to-run CCF probability will be calculated from the running failure rate, mission time and beta factor.

5.3.6.2 Initiating Events

One instance in which a beta factor may have to be applied to a failure rate is in the calculation of an initiating event frequency. This application is necessary if a CCF of multiple running components or running/standby components can itself be an initiator. Therefore, when creating fault trees to calculate initiating event frequencies, CCFs must be modelled.

5.3.6.3 Interface with Human Reliability Analysis (HRA)

The UPM attempts to quantify the human contribution to CCFs through two of its subfactors; the MMI and safety culture subfactors. As there is a potential overlap with HRA methodologies within the MMI subfactor, the analyst must take care to avoid double counting.

The MMI subfactor is derived from two evaluations. One is performed for maintenance actions, and the other is performed for operator actions. The more pessimistic result of these two categories becomes the subfactor used in the beta factor estimation. However, if all credible pre-accident human errors are modeled explicitly in the fault tree and a dependence model exists for these errors, then there is no need to also account for these failures in the CCF analysis. If this is the case, then only the operator action evaluation is relevant to the MMI subfactor.

The operator action aspect also requires some scrutiny. Since the UPM is designed for CCF analysis at both the system level and the component level, certain explanations in the manual are ambiguous. The text that refers to operator actions is very much geared to systems, because extensive mention is made of written procedures for system operation and checklists. The intent of the category is to account for the possibility of the operator inadvertently making a system or

redundant component unavailable, by using manual overrides or by performing other errors of commission, presumably in a post-accident situation. In cases where components perform their function without any interaction being required of the operator and without any possibility of being overridden by the operator, it makes little sense to assign a non-zero M.M.I subfactor. At least for these components, the presence or absence of written procedures for operating or monitoring the system has no relevance.

HRA is typically used to model obvious human errors that can result in the unavailability of components. However, there is some possibility that an unforeseen human action can render redundant components unavailable. An example might be the use of incorrect fuel in diesel generators, or the temporary cross-tying of redundant components, such that a functional dependency is introduced. Also, actions that are contrary to the policies and procedures of the plant are typically outside the scope of HRA. It is assumed that these types of errors are adequately captured by the lightly-weighted safety culture subfactor of the UPM.

Human actions that can cause unavailability of redundant components shall be modeled explicitly using HRA methods. Therefore, the M.M.I. sub-factor shall be assigned a value of zero.

5.3.6.4 Interface with External Events PSA

It is very important to distinguish root causes of multiple component failures that are included in the CCF analysis from those components that are not included. When a full-scope PSA includes some internal events (fire, flood) and external events, component unavailability due to certain causes is modelled explicitly, in order to arrive at plant damage frequency estimates. Ideally, then, these failure causes should be screened out from the CCF analysis to avoid double counting. Unfortunately, the nature of the UPM makes it difficult to do so. Since the subfactors are not generally based on cause, but instead on CCF defences, it is difficult to break down the beta factor, in order to eliminate these events as contributors. A solution might be to scale down the separation and/or environmental test subfactor values by some constant. The aim would be to reduce the CCF unavailability of a given set of components by an amount that is equal to the calculated unavailability due to all external events. However, this may not be easy to justify, since it is unclear to what extent the generic CCF data that underlies the UPM's beta factors includes failures due to these causes.

From another perspective, it may not even be desirable to attempt to screen out some external events. For example, small fires that do not lead to initiating events can nevertheless cause component unavailability. If this is not modelled as part of the fire PSA, then the CCF analysis can cover these events, albeit in a non-rigorous, non-deterministic fashion.

A conservative approach shall be taken, in that no attempt will be made to screen out any overlap between the CCF analysis and the internal and external events analysis. The UPM will be applied without modification.

5.3.6.5 Staggered Testing

One effective means of defending against CCFs that is not addressed in the UPM is the use of staggered testing on redundant components. The benefits of staggered testing can be illustrated with a simple example. Consider two redundant components, A and B, each tested every two months. If they are tested simultaneously, then the exposure of the components to CCF is the same as the exposure to independent failure—exactly two months. However, the exposure time to CCF can be reduced if testing is staggered, as shown below in Table 5-3.

If component A is found to have failed at month 3, *and there is a procedural requirement that the redundant item B should be checked after the first failure is found,* then the actual exposure time to CCF is one half of the exposure time to independent failure. Accordingly, the CCF basic event probability in the fault tree can be reduced by a factor of two. If the redundant component is not checked, then the modelling is complicated by the fact that it is unclear whether or not a CCF event has occurred. Even if component A is repaired, component B may be unavailable until it is tested at month 4. If there is no checking of the second component, then it is best to assume the same CCF and independent failure probabilities as for simultaneous testing. For cases in which there are three components with staggered testing and checking, a factor of three reduction in CCF probability is possible; for four components the factor is four, and so on.

5.3.6.6 High Levels of Redundancy

A contentious issue in CCF modelling involves the treatment of high levels of redundancy. By its very nature, the UPM models only those CCF events for which all components in a group are assumed to have failed. The particular *m* out of *n* success criterion affects the beta factor calculation (under the redundancy subfactor), but the fault tree model does not explicitly contain combinations of lower order failures. That is, if 7 out of 16 is the success criterion, the only fault tree CCF event will still be for all sixteen items being failed. There will be no minimal cutsets that show just 10 items failed or cutsets consisting of two CCF events, each with five items failed. To further complicate matters, the subfactor classification is not designed to handle large *m* and *n*. The manual suggests mapping *m* out of *n* to 1 out of (*n*-*m*+1), but only for $n \leq 5$. Ignoring this restriction, the 7 out of 16 example gives a result of 1 out of 10, which is presumably an optimistic number. However, if the redundancy is assumed to be equivalent 1 out of 2, then this is tantamount to saying that the probability of two identical components failing in a set-up with dual redundancy is similar to that of sixteen components failing simultaneously. Therefore, it would seem that the reliability estimate from the UPM would be unduly conservative.

It may be tempting for the analyst to divide up a large CCF group into several smaller subgroups. Diversity and increased separation between the subgroups might be used as arguments to support the claim that separate CCF events are appropriate. However, subdivision may be difficult to justify without a very strong rationale. A cutset that includes two CCF events for identically redundant components implies that the root cause of each event in the cutset is different (e.g., one CCF is maintenance related, the other is due to a harsh environment). The likelihood of this occurring would seem to be negligible, when compared with one root cause impacting all of the

components. A possible exception, which might allow for separate CCF groups, would be some sort of asymmetry among the components. If the most likely cause of CCF were to be environmental degradation, then periodic replacement or refurbishment of some fraction of the components would be an effective defence. Then, it might be argued that separate groups are acceptable, perhaps with a limited CCF probability attributed across the groups. Otherwise, the analyst has little recourse but to use the UPM in its present conservative form.

5.3.6.7 Re-Assignment of SubFactor Categories

For each subfactor, the UPM requires the analyst to select the category description that most closely resembles the components being studied. There are five categories from which to choose (A through E) in the manual (Reference 5-1), except for the redundancy subfactor, which has seven categories. However, there is no particular restriction that limits the number of categories, as long as the extreme values for categories A and E remain unchanged. The intermediate categories can therefore be freely reassigned, or new categories can be interpolated between the existing ones. For example, this might be useful if the analyst feels that the required two-metre separation between components in special safety systems warrants a slightly better subfactor for separation than the worst case category A value. The subfactor values for each category are fitted to an exponential function:

$$y = k \exp^{mx} .$$

Given an arbitrary set of equally spaced *x*-values to represent the categories, it is a simple matter to use the known *y*-values shown in the UPM manual's partial beta factor estimation table to determine a set of constants *k* and *m*. The *y*-value for a new category (e.g., A+) can then be calculated, by choosing an appropriate *x*-value, and by substituting into the above expression. An example of how this may be done is shown for Table 5-4, in which it is desired to interpolate an A+ category midway between the A and B categories.

a) Write two equations with two unknowns:

$$y_A = 2400 = k \exp^{mx_A} = k \exp^{m}$$

$$y_B = 580 = k \exp^{mx_B} = k \exp^{2m}$$

b) Solve for *k* and *m*:

$$k = 9931$$

$$m = -1.4202$$

c) Calculate y_{A+}:

$$y_{A+} = 9931 \exp^{-1.4202(1.5)} = 1180$$

5.3.6.8 Plant Safety Culture

The safety culture of the plant is addressed in one of the UPM subfactors. For a plant that has not yet gone into operation, the eventual, "steady-state" management conditions and the levels of

staff training and experience must be assumed. It is reasonable to assess the median, category C level, which is described as "Simulator training of normal operations OR dedicated staff and evidence of good safety culture including a systematic training program."

It is expected that this choice is conservative, given that simulator training is also conducted for emergency conditions at CANDU plants. The existence of such training is a prerequisite for assigning the best-case category E level for the safety culture subfactor.

If the UPM is to be applied to an established, operating plant, then the analyst should assess the safety culture level, by comparing actual training levels and plant safety records with the judgment tables.

5.4 Conclusions

This Section has described the basic features of the UPM and how it will be applied in AECL PSA studies. The analysis for all PSA projects shall be carried out at the component level. This will allow greater flexibility to perform sensitivity studies, in order to see the effects of design changes. The resulting CCF probabilities for the various sets of similar equipment that are assessed shall be included on the fault trees for the unavailability analysis of the system under consideration. This document provides guidance on the application of UPM and general CCF modelling; however, it will be necessary for analysts to reach a consensus on any outstanding issues. Reports on the unavailability analysis shall contain all the judgment tables, a listing of CCF basic events and their probabilities, and any additional discussion that is used to justify the judgments and assumptions made in the CCF analysis.

5.5 References

5-1. AEA Technology PLC. (Nuclear Division under Serco Assurance), 1996, UPM 3.1: A Pragmatic Approach to Dependent Failures Assessment for Standard Systems, SRD Association Report, SRDA-R13, AEA Technology PLC, Cheshire, UK. Proprietary.

5-2. Commission of the European Communities Joint Research Centre, 1987, CCF-RBE: Common Cause Failure Reliability Benchmark Exercise, Final Report, Commission of the European Communities Joint Research Centre Report, EUR 11054 EN, Ispra, Italy.

5-3. USNRC (prepared by Pickard, Lowe and Garrick, Inc.), 1989, Procedures for Treating Common Cause Failures in Safety and Reliability Studies, USNRC Report, NUREG/CR-4780, Washington, D.C.

5-4. SRD Association Report. 1986. A Method of Assessment of CMF - The Partial Beta Factor Method. Publisher Report, SRD/RTS/86/133. Propietary.

5-5. USNRC (prepared by EG&G Idaho, Inc.), 1983, Common Cause Fault Rates for Pumps: Estimates Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants, January 1,1972 through September 30, 1980, USNRC Report, NUREG/CR-2098, Washington, D.C.

5-6. USNRC (prepared by EG&G Idaho, Inc.), 1983, Common Cause Fault Rates for Valves: Estimated Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants, 1976-1980, USNRC Report, NUREG/CR-2770, Washington, D.C.

5-7. USNRC (prepared by EG&G Idaho, Inc.), 1983, Common Cause Fault Rates for Instrumentation and Control Assemblies: Estimates Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants, 1976-1981, USNRC Report, NUREG/CR-3289, Washington, D.C.

5-8. USNRC, 1981, A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants, USNRC Report, NUREG-0666.

Table 5-1
Judgment Table Format

Sub-Factor	Judgement Decision	Category/ Numerical Value	Comment
Redundancy			
Separation			
Understanding			
Analysis			
Human Factors		N/A	see Section 5.3.7.2
Safety Culture			
Environmental Control			
Environmental Testing			
Total Numerical Value (summation of sub-factors)			
Beta Factor (β) = /50000 (See partial β-factor estimation table in the UPM manual)		**β =**	

Table 5-2
Component Types and Boundaries for CCF Analysis

Component	Present Boundary	Additional Comp in CCF Event
Motorized Valves (MV)	Includes contribution from motor, but not power supply to the motor operator. Includes contribution from failure of associated limit and torque switches.	Motor starter, any additional C&I components
Pneumatic Valves (PV)	Includes contribution from actuator, but not air supply to the actuator. Includes contribution from failure of associated limit and torque switches.	Solenoid valves, C&I components
Pumps	Includes all intake and discharge piping associated with the pump and internals up to but excluding the flange or weld. Includes shaft/impeller-driven lube oil pumps, but excludes auxiliary lube oil pumps. It does not include pump motor failures or electrical cable terminations to the motor.	Pump motor, C&I components
Air Compressors	Includes contribution from motor failures. It does not include contribution from loss of power supply to the motor.	C&I components, if applicable
Air Coolers	Cooling coil, fan/motor set modelled separately.	Combine coil, fan/motor, C&I components, if applicable
Heat Exchangers	Vessel up to inlet and outlet nozzles, including all subcomponents such as tube bundle, divider plates and baffles.	None
Batteries	Battery cells, interconnecting links and supporting structures. Does not include outgoing cables with their connections.	None
Diesel Generators	Includes motor and generator.	None
Pressure Switches/Transmitters Level Switches/Transmitters Temperature Sensors/Transmitters Flow Switches/Transmitters	Component, including all subcomponents up to the first fitting, flange where applicable. Does not include electrical connectors.	None

Table 5-3
Staggered Testing Example

	Month 1	**Month 2**	**Month 3**	**Month 4**
Component A	Test - OK		Test - Failed	
Component B		Test - OK	Check?	Test

Table 5-4
Category Interpolation Example

	Category					
	A	A+	B	C	D	E
y	2400	?	580	140	35	8
x	1	1.5	2	3	4	5

Figure 5-1 CCF Grouping Example #1

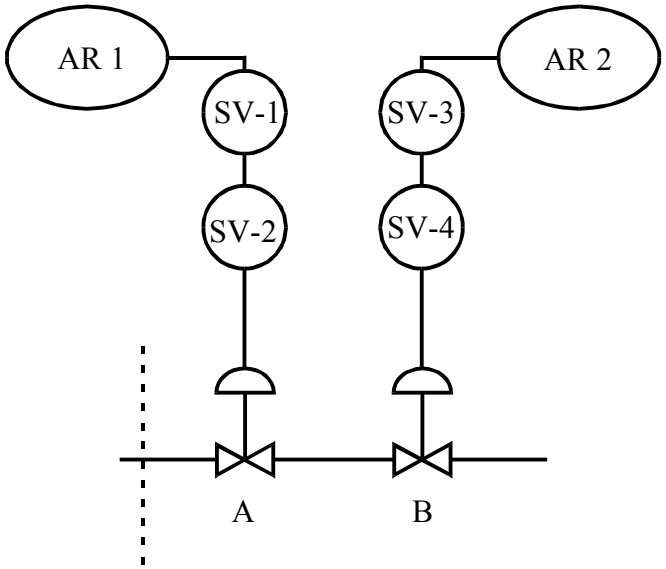


Figure 5-2 CCF Grouping Example #2

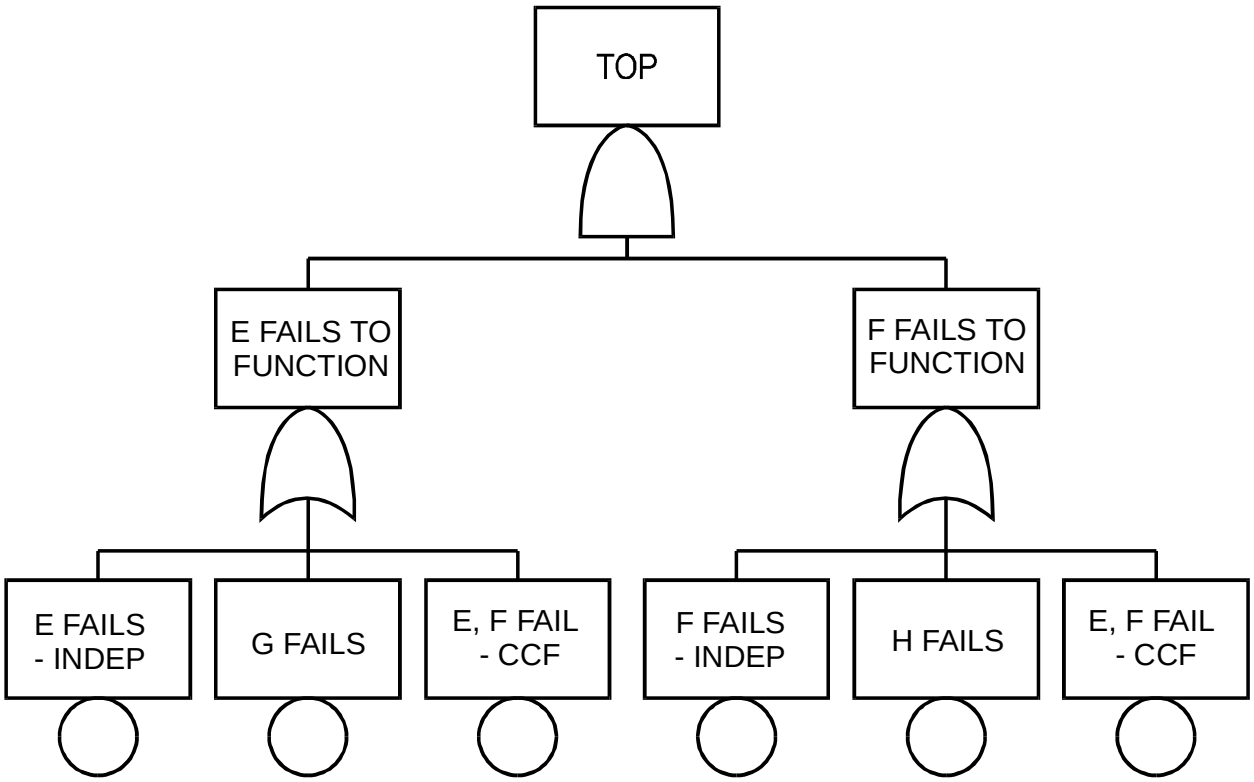


Figure 5-3 Addition of CCF Basic Events to Fault Tree

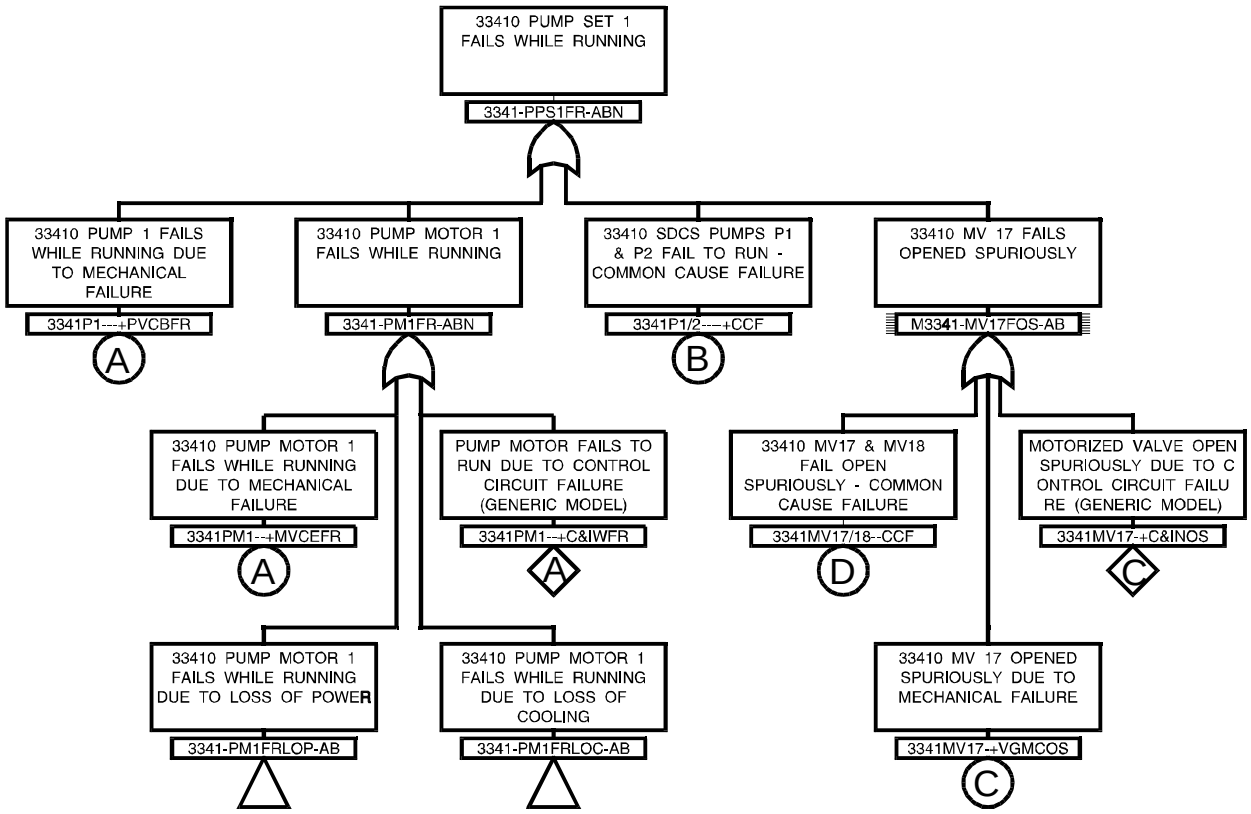


Figure 5-4 Component Boundaries Example - Shutdown Cooling System

6. HUMAN RELIABILITY ANALYSIS

6.1 Introduction

An important aspect of any PSA is the analysis of human actions, commonly referred to as human reliability analysis (HRA). Given the high degree of hardware reliability and redundant design associated with nuclear power plant systems, human interactions with the systems are often significant contributors to system unavailability. The purpose of HRA is to identify potential human errors, and to quantify the most significant of these. This investigation covers the analysis of the human actions of potential concern that are identified during the PSA process. This section describes in detail the AECL HRA methodology.

The procedures for incorporating human interactions into PSA studies, and the associated data requirements, are well documented and studied. However, it is recognized that no strong consensus exists on the best methods to perform HRAs, in order to quantify the potential contribution of human error to accident sequence frequencies. All methods have merits and limitations, depending on the particular circumstances in which they are applied. The HRA methodology described in this report is based on previous work performed within AECL in this area, and on industry accepted methods and guidelines.

For pre-accident and post-accident diagnosis, and, in part, for recovery human actions, HRA methodology is based on the experience accumulated during the PSA analyses for CANDU plants. Particular attention is given to modelling the post-accident execution errors in accordance with international practice, based on the ASEP procedure (Reference 6-1).

This report also includes the modelling of human error probabilities (HEPs) for recovery actions that are based on the methodology for the quantification of post-accident operator errors. Operator actions that are credited in the recovery analysis are based on equipment and component failures (or other failures) at the sequence cutset level.

6.2 Classification of Human Actions and Tasks In PSA

6.2.1 Classification of Human Actions

A review of several PSA studies has indicated that it is necessary to account for different types of human actions; some that may mitigate the consequences of an accident, and some that may increase the severity. These reviews identified five basic types of generic human actions that are common to nuclear power plants. In general, these five basic types of human actions can be grouped into the three major categories listed and discussed below:

a) Category A actions, i.e.: pre-accident human actions (pre-initiators),

b) Category B actions, i.e.: human actions that lead directly to initiating events (initiators), and

c) Category C actions, i.e.: post-accident human actions (post-initiators).

These categories facilitate the incorporation of HRA results into the PSA structure, and are determined by the way in which they are generally analyzed in practice in a PSA.

6.2.1.1 Category A - Pre-initiators

Category A actions occur prior to an accident, and are associated with maintenance, testing, calibration and repair errors that degrade system availability. They are referred to as pre-accident human actions/errors in this document. Prior to an initiating event, plant personnel can affect availability and safety by inadvertently disabling equipment during calibration, testing, or maintenance. This type of human error can occur and remain undetected until the system is required to operate following an initiating event, or until the next test of the system.

The benefits of testing and maintenance are modelled by the selection of repair times, and test and maintenance intervals in the equipment unavailability calculations. The factors that degrade system availability are modelled as test and maintenance outages, based on the associated downtime.

The pre-accident human actions (errors) are explicitly incorporated as basic events in the fault trees.

6.2.1.2 Category B - Initiators

These actions, either by themselves or in combination with equipment failures, contribute to initiating events or plant transients. They are generally implicit in the selection of initiating events, and contribute to their total frequency. Category B initiators may be due to control room actions/errors during normal operations, or maintenance/test errors. An example of an initiating event caused by human error is a reactor trip that is initiated by an error in following testing procedures. Category B actions are not modelled explicitly in the methodology. They are presumed to be included in initiating event frequencies based on operating experience.

6.2.1.3 Category C - Post-Initiators

Category C actions occur after, and in response to the accident or initiating event, and are called post-accident human actions/errors. They can occur either in the control room or locally in the field. The post-accident operator actions are complementary to automatic mitigating actions. These actions can be further subdivided into three different types for incorporation into the PSA.

a) Type 1 - Procedural safety actions

   These operator actions involve success or failure in following procedures or rules, in response to an accident sequence. By following procedures during the course of an accident, plant personnel can operate standby equipment that will terminate the accident. These actions are generally incorporated explicitly in the event trees; however, a few may be included in the fault trees. These actions include diagnosis and execution tasks.

b) Type 2 - Aggravating actions/errors

These actions are a special set of post-accident commission errors, in which the operator, in attempting to follow procedures, significantly aggravates the situation or fails to terminate the accident. An example of this type of interaction is the case where the operator misdiagnoses the event, and subsequently performs the right actions for the wrong event. Another example of a Type 2 error occurs when the operator correctly diagnoses the event, but chooses a non-optimal strategy for dealing with it.

This type of human interaction (known as errors of commission) is the most difficult to identify and model, and is not considered in the HRA. Also, this methodology does not address sabotage, poor safety culture, etc. Only a few PSA studies have attempted to include this kind of interaction, and only to a limited degree.

c) Type 3 - Recovery actions

A recovery action is an action taken to recover from (i.e.: cope with) some abnormal event. By improvising, the operator can operate and/or restore initially unavailable equipment, in order to terminate an accident. These interactions consist of recovery actions, which are generally included in accident sequences that dominate risk. These actions may include the recovery of previously unavailable equipment, or the use of non-standard procedures to mitigate accident conditions. Recovery actions are considered in the methodology.

6.2.2 Classification of Tasks

A task classification scheme is required for identifying different types of human action or behaviour and the associated error mechanisms, and is suitable for PSA purposes. A well-known task classification scheme, presented in Section 2 of the ASEP HRA procedure (Reference 6-1), is adopted. This model distinguishes between three types of behaviour.

a) Skill-based behaviour

Skill-based behaviour does not depend directly on the complexity of the task, but rather on the level of training and the degree of practice in performing the task. Highly practised activities that can be performed with little apparent thought, such as driving a car along a familiar route, typify skill-based behaviour.

While different factors may influence the specific behaviour of a particular individual, a group of highly trained operators are expected to perform skill-based tasks efficiently or even mechanically, with a minimum of mistakes. This also applies to those actions that must be taken quickly following an initiating event, such as a LOCA, and that are supposed to be committed to memory by the operating personnel.

b) Rule-based behaviour

Human actions that require the performance of less familiar tasks, which demand more conscious mental effort than skill-based tasks, are usually described as rule-based tasks. Although more demanding, these tasks are still within the experience and ability of the individual, and are usually executed by following written rules (procedures). The distinction

between skill-based and rule-based actions is often arbitrary, but the primary difference is the amount of thought that is required.

An example of rule-based behaviour is the performance of most test and calibration procedures. Rule-based tasks are usually classified as step-by-step tasks.

c) Knowledge-based behaviour

Behaviour that requires the performance of novel tasks, where familiar patterns and rules cannot be applied directly, and where a high degree of cognitive activity is required, is described as knowledge-based behaviour (e.g., operator actions for accident situations that have not been previously included in operating procedures or training programs).

A post-accident HRA deals with all three categories—mostly rule-based and knowledge-based behaviour in the diagnosis stage, and skill-based and rule-based behaviour in the execution stage. For a more detailed description of this task classification scheme, see Section 2 of the ASEP HRA Procedure (Reference 6-1).

6.3 Pre-Accident Human Reliability Analysis

6.3.1 Introduction

The pre-accident tasks of interest consist of routine and corrective maintenance, calibration, surveillance tests, and restoration tasks. A typical restoration task consists of the opening or closing of manual or motor operated valves following a repair or test, in order to restore these valves to their normal operating position or status. These tasks are usually performed by operations personnel, I&C personnel, and maintenance personnel, under non-accident conditions. Pre-accident tasks can affect the availability of safety systems that are required to mitigate an accident sequence.

In the evaluation of pre-accident tasks for an existing plant design, the calibration, test and maintenance procedures and practices are reviewed for each front-line and support system. This review identifies critical instrumentation for which miscalibration could prevent system function, and identifies components that could be removed from service and inadvertently left in an inoperable or incorrect state.

Pre-accident human errors are modelled at lower levels in the individual fault trees, usually at the basic event level. Typically, a human error is modelled alongside its corresponding hardware failure. Both types of errors are then input into “OR” gate logic as contributors to the specified undesirable state of the component. Each human error basic event that is modelled in the fault trees is labelled so that operator errors can easily be identified in cutset analysis and sorted for separate event reporting.

Although pre-accident tasks may include elements of skill-based, rule-based or knowledge-based behaviour, typically only rule-based behaviour is modelled for PSA purposes, when assessing pre-accident tasks. That is, the HRA considers the ability of people to understand and implement rules (usually written rules).

6.3.2 Basic Human Error Probability

The ASEP HRA Procedure (Reference 6-1) presents a simplified model of human behaviour for pre-accident tasks. The model includes a generic basic human error probability (BHEP) that can be used for all pre-accident tasks, as well as rules to adjust this BHEP for the effects of dependence and recovery factors. The BHEP has a value of 3×10^{-2} for the performance of pre-accident actions, exclusive of any recovery factors (RFs). Therefore, for each key action that must be accomplished, e.g., the restoration of a valve to its normal operating position after maintenance, or the performance of a critical step in a calibration procedure, a total BHEP of 3×10^{-2} is used. This value is based on the assumption of at least average quality written instructions and restoration procedures, and associated administrative control. For comparison, the IAEA suggests a basic HEP of 1×10^{-2} (Reference 6-3).

6.3.3 Performance Shaping Factors

Any factor that influences human behaviour is referred to as a performance shaping factor (PSF) and may be external to the operator, or part of his or her internal characteristics.

PSFs, other than recovery factors, dependence effects and radiation, are implicitly included in the BHEP and assume average, or better human factors or conditions. The effects of PSFs are also implicitly taken into account, to some degree, in the uncertainty bounds for the various HEPs. If it is considered to be necessary, the BHEP of 3×10^{-2} may be re-assessed upward (larger HEP) on the basis of a more detailed analysis of the administrative procedures, and their method of implementation; however, no downward adjustment of the BHEP should be made.

Radiation is explicitly considered as a PSF in the pre-accident screening HRA. When a human action takes place in a radiation area, the procedure assumes that the probability of human failure is doubled. That is, the basic HEPs are multiplied by a factor of 2.

6.3.4 Recovery Factors

An RF is defined as a factor that prevents or limits the undesirable consequences of a human error. One of the most common RFs is human redundancy. Other RFs are applicable to the effects on human performance of component status displays in the control room (especially those that are annunciated), the effects of post-maintenance or post-calibration tests, and the effects of periodic inspections (especially those involving the use of written checklists). It should be noted that these RFs are not part of the post-accident recovery analysis discussed in Section 6.5.

In the ASEP HRA Procedure for pre-accident tasks (Reference 6-1), no RF credit is given for the use of written checklists, unless the users of these checklists have been instructed to check off each listed item of equipment inspected, once the prescribed check has been completed. In the HRA, RFs will be credited for written checklists, on the assumption that these checklists are available and are required to be checked off.

The procedure distinguishes between basic conditions, in which no RFs are assumed to be available, and optimum conditions in which allowable RFs are present. Each basic condition has

its complementary optimum condition. For a case where all basic conditions apply, a BHEP of 3×10^{-2} is assumed. The following recovery factors are applied:

a) Indication in the MCR or SCA Unavailable component status is indicated in the MCRSCA by an annunciator, CRT alarm or other indicator, when the maintenance or calibration task or subsequent test is finished, or before normal power operation can be resumed.

   An RF of 1×10^{-4} is assessed for the failure to detect the unavailable status of a component due to a compelling signal, i.e.: a signal that demands the same kind of attention from an operator as an annunciator.

   An RF of 1×10^{-2} is assessed for the failure to detect the unavailable status of a component due to all other forms of indication in the control room, such as a CRT alarm or panel indicating lights.

b) Post maintenance (PM) or post calibration (PC) test Component status is verified by a PM or PC test. If performed correctly, then full recovery of any related error is assumed. An RF of 1×10^{-2} is assessed for the failure to perform the test correctly (including failure to do the test), based on the ASEP HRA Procedure (Reference 6-1).

c) Written verification There is a requirement for (1) a second person (checker) to directly verify the component status after the completion of a maintenance or calibration task, or (2) the original performer to make a separate check of the component status at a different time and place from his or her original task performance. No credit is given for either check, unless a written checklist is used during the check.

   An RF of 1×10^{-1} is assessed for the failure of the checker to detect the unavailable status of the component, due to an error by the original task performer. This RF is based on the ASEP HRA Procedure (Reference 6-1).

d) Periodic check/inspection There is a requirement for a periodic check (inspection) of component status (inside or outside the control room) using a written checklist. An RF of 1×10^{-1} is assessed for the failure of such a check to detect the unavailable status of the component. The RF is based on the ASEP HRA Procedure (Reference 6-1).

The determination of the applicable RFs for the specific activity under review is presented in Table 6-1, which is based on the ASEP HRA Procedure, Table 5-3 (Reference 6-1).

6.3.5 Dependence Effects

The dependence between two tasks or activities refers to the situation in which the probability of failure for one task is influenced by the success or failure that has occurred for the other task. The dependence may exist between two tasks performed by the same person (within-person dependence), or between the same tasks performed by different persons (between-person dependence). For the same pair of activities, the level of dependence may differ for errors of commission and errors of omission. For a detailed discussion of dependence, see Chapter 10 of NUREG/CR-1278-F (Reference 6-2).

The BHEP of 3×10^{-2} must be modified for the effects of dependence. As noted in Section 6.3.4, between-person dependence is already included in the HEPs for the RFs. Rules are therefore developed for assessing the effects of within-person dependence, i.e.: dependence between the activities performed by the same person.

In the ASEP approach and in this document, dependence effects for RFs and for original task performance are treated differently. For RFs, dependence effects are not specifically considered because of the rule, which states that for any group of tasks, each RF will be applied only once, and because even in the exceptions for periodic checks, independence can be assumed.

For original task performance, dependence effects for series systems and parallel systems are treated differently. A parallel system is one in which system failure occurs only if all the human actions in a set are performed incorrectly, and system success occurs if at least one human action is performed correctly. A series system is one in which system success occurs only if all human actions in a set are performed correctly, and system failure occurs if any one human action in a set is performed incorrectly.

6.3.5.1 Levels of Dependence

Although dependence is a continuum, it is discretized for practical reasons into a number of levels, which vary from two levels (zero dependence and complete dependence) in the ASEP HRA Procedure (Reference 6-1), to five discrete levels in the Handbook of Human Reliability (Reference 6-2).

In this report, the dependence is discretized into four levels, from zero (no) dependence to complete dependence. This is a conservative simplification.

The levels of dependence in this model are

a) zero dependence (ZD)

b) moderate dependence (MD)

c) high dependence (HD)

d) complete dependence (CD)

6.3.5.2 Assessment of Dependence

For pre-accident errors, the modelling of dependent errors in the fault trees is affected by the level of dependence that is assigned between the errors. Equations for the calculation of the conditional failure probabilities that are associated with different levels of dependence are shown in Table 6-2. These equations are taken from Table 10-2 of NUREG/CR-1278 (Reference 6-2), and are based on the positive dependence model. Guidance for the assessment of dependences is given in Figure 6-1 (Reference 6-1). Dependencies will be analyzed only at the system level and not at the sequence level, so that the cutset truncation limit is 10^{-10}.

For each level of dependence, the logic structure of the system fault trees is revised, if necessary, as follows:

a) Zero dependence (ZD)

All human actions that are identified as being completely independent (zero dependence) are modelled in the fault trees as individual basic events, each with its own unique label. In general, for the case of zero dependence, the original fault trees will not require modification.

b) Low to moderate dependence (MD)

Where each dependent event appears, an additional dependent failure event is added to the fault tree, in a similar way to the addition of a CCF event for hardware failures. In this report, low and moderate dependence are combined in a single level, and the higher level, i.e.: moderate dependence, is always used. For two tasks A and B, the probability for the dependent event (P_D), modelled in the fault tree, is a product of the probability of the independent event P_A and the conditional probability $P_{[B|A]}$:

$$P_D = P_A * P_{[B|A]} .$$

c) High dependence (HD)

High dependence is treated in a similar manner to moderate or low dependence, i.e.: an additional basic event is added to the fault tree.

d) Complete dependence (CD)

All errors identified as being completely dependent are modelled by using the same basic event label in the fault tree. The fault tree analysis software then treats the dependent errors as the same error.

6.3.6 Quantification

The purpose of this section is to assess the failure probabilities of Category A (pre-accident) human actions, including the influence of RFs and within-person dependence for multiple errors. RFs already include between-person dependence. The following steps are used to determine the nominal human error probability (NHEP):

a) Basic human error probability

A total BHEP of 3×10^{-2} is assigned for each critical action.

b) Performance shaping factors

The only explicit PSF, excluding RFs and dependence effects, that is considered in the calculation of the pre-accident NHEP is radiation. If the critical action is performed in a radiation area, then the BHEP is multiplied by a factor of 2 (see Section 6.3.3).

c) Recovery factors

Assign credit for all permissible RFs. This is the total RF credit from Table 6-1 for each applicable case.

d) Dependence effects

1) Series system (ZD)

Zero dependence (ZD) is assessed for the critical human actions that are related to series systems (see Figure 6-1, dependence model). For this case, the NHEP is approximated by the following equation:

$$\mathbf{NHEP = n[BHEP * T_{RF}] = n[3E\text{-}2 * T_{RF}]}$$

where the BHEP has a value of 3×10^{-2}, T_{RF} is the total recovery factor credit, and n is the number of components in the system.

2) Parallel system (ZD)

If zero dependence is assessed for the critical human actions in a parallel system, then the NHEP is approximated by the following equation:

$$\mathbf{NHEP = [3E\text{-}2 * T_{RF}]n .}$$

3) Parallel system (CD)

For complete dependence between the critical human actions in a parallel system, the NHEP is approximated by the following equation:

$$\mathbf{NHEP = 3E\text{-}2 * T_{RF} * [1.0]n\text{-}1 = 3E\text{-}2 * T_{RF}}$$

where 1.0 is the conditional HEP, assuming complete dependence, for the second or subsequent human actions following the basic HEP (see Table 6-2 for the calculation of conditional failure probability for complete dependence).

4) Parallel system (HD)

For high dependence between the critical human actions in a parallel system, the NHEP is approximated by the following equation:

$$\mathbf{NHEP = 3E\text{-}2 * T_{RF} * [0.5]^{n-1}}$$

where 0.5 is the conditional HEP, assuming high dependence, for the second or subsequent human actions following the basic HEP (see Table 6-2 for the calculation of conditional failure probability for high dependence).

5) Parallel system (MD)

For moderate dependence between the critical human actions in a parallel system, the NHEP is approximated by the following equation:

$$\mathbf{NHEP = 3E\text{-}2 * T_{RF} * [0.15]^{n-1}}$$

where 0.15 is the conditional HEP, assuming moderate dependence, for the second or subsequent human actions following the basic HEP (see Table 6-2 for the calculation of conditional failure probability for moderate dependence).

6.3.7 Additional Credit for Human Error Probability Calculation

In some cases there are surveillance programs and/or checks conducted on equipment in between tests. To take credit for these programs and checks, instead of applying the Table 6-1 as described in Section 6.3.4, the following equation can be used (Reference 6-2):

$$\mathbf{U_{HEP} = (E \times R \times D) / T}$$

Where

U_{HEP} = HEP taking into account additional credit,

E = the basic HEP (3×10^{-2}),

R = the probability of failing to recover from the error that causes the component to be in the failed condition,

D = the mean downtime, i.e.: the average time within a given time period, within which the component or system is unable to operate given that a human error has induced a failed condition, and

T = time period of interest when estimating unavailability.

When checks are made between tests, the general equation for calculating the total average downtime (D) is

$$D = H_1 + C_1H_2 + C_1C_2H_3 + \ldots C_1C_2 \ldots C_{m-1}H_m$$

where

m = the number of checking intervals between the two tests;

H_1, H_2, H_3 and H_m = the number of hours (or any other time unit) between the first test and the first check, the first and second checks, the second and third checks, and the last check and the next test, respectively; and

C_1, C_2, and C_{m-1} = the probabilities of non-detection of the error at the first, second and last checks performed between the two tests, respectively.

In determining D, credit will be taken for these steps if sufficient data are available; otherwise, conservative numbers will be used that are based on judgement.

6.4 Post-Accident Human Reliability Analysis for Internal Events

6.4.1 Introduction

Post-accident human actions typically pertain to activities that are performed by reactor operators who are stationed in the MCR, and that take place after the onset and annunciation of an initiating event. Post-accident tasks are divided into diagnosis (perception, discrimination, interpretation, diagnosis and decision-making) and post-diagnosis (execution) tasks, both of

which are intended to implement mitigation measures for ensuring or maintaining adequate fuel cooling.

Post-accident operator actions are required in the following cases:

- failure of the automatic actuation of the mitigating systems;
- successful automatic actuation of a mitigating system, with a requirement for operator action to ensure continuing operation (e.g., replenishing of water inventories for Group 2 feed water after 8 hours); and
- the absence of design features for automatic mitigating action.

Diagnosis is the identification and evaluation of an abnormal event to the level that is required, in order to identify those systems or components whose status can be changed to mitigate or eliminate the problem. In other words, diagnosis means the determination of appropriate actions when an abnormal event has been recognized—within the allowable time constraints. Diagnosis includes interpretation and, when necessary, decision-making. Diagnosis also involves knowledge-based behaviour, i.e.: behaviour that is applied to unfamiliar situations in which personnel have to interpret, diagnose or use some level of decision-making.

Post-diagnosis actions are activities that are indicated by, and which logically follow, a correct diagnosis of the abnormal or initiating event. These actions involve skill-based and/or rule-based behaviour, and must be performed correctly within the allowable time constraints.

6.4.2 Modelling

Post-accident operator actions are generally modelled in the event trees as separate decision branch points (top events), and are usually placed just before the top event of the associated system that requires manual initiation.

In some cases, post-accident operator actions are modelled in the system fault trees. This is usually restricted to cases where only one system or subsystem is affected by the operator action, as, for example,

- the interconnection of the Class III odd and even 4.16 kV buses to restore auxiliary feed water to the steam generators;
- the transfer of power between odd and even buses to 480 V Class III motor control centres 5433-MCC 17A, MCC 18C, and MCC 19B via manual transfer switches; and
- manual transfer from the unit service transformer (UST) to the system service transformer (SST).

As a result, a prerequisite for the systematic identification of post-accident human actions is the accident sequence event trees for each initiating event. In addition to the event trees, the analyst reviews emergency procedures that are associated with each accident sequence, accident analyses and reports, and any relevant information. A list of operator actions to be performed for each system and sequence is then compiled.

For post-accident operator actions, both diagnosis errors and execution errors are modelled. In some situations, following a correct diagnosis, execution errors or system failure will mean that success criteria for the particular operator action are not met. The operator is assumed to correctly monitor the state of the plant and realize the occurrence of a failure. For the subsequent operator action in this case, a new diagnosis HEP will be considered, unless this failure possibility is already included in the procedure being followed by the operator, which clearly specifies the next required action.

6.4.3 Time Relationship between Diagnosis and Execution Tasks

One of the simplifications that is employed in the post-accident screening analysis is the division of the total estimated time available for coping with an abnormal event into two artificially independent parts. The total allowable time for coping with an abnormal event is specified by the systems analyst, and is divided into an allowable diagnosis time and an allowable execution (post-diagnosis) time. The procedure for estimating the diagnosis time is described below.

First, assuming that a correct diagnosis has been made, the time to perform the execution tasks required in response to the initiating event is estimated. Once the time to perform the execution tasks is determined, this time is subtracted from the total allowable system response time estimated by the systems analyst. The time left after this subtraction is the allowable diagnosis time. The diagnosis time is expressed as

$$\mathbf{T_d = T_m - T_a}$$

where

Tm = the estimated maximum allowable time for the correct diagnosis of the abnormal event and for the completion of the required post-diagnosis actions (execution tasks), in order to meet system success criteria established by the systems analyst.

Td = the estimated allowable time for a correct diagnosis, with sufficient time to perform the required post-diagnosis actions within the maximum allowable system response time Tm.

Ta = the estimated time to get to the appropriate locations and to perform the required post-diagnosis actions, following a correct diagnosis.

6.4.4 Human Error Probability for Diagnosis Tasks

The BHEPs for diagnosis tasks are given in Table 6-3 as a function of the available diagnosis time. In assessing the diagnosis time, the time starts from the receipt of first alarms and indications by the operator of the off-normal condition, and specifically excludes the time taken to execute the specific corrective action required (see Section 6.4.3). The model retains the assumption that no operator action is credited within the first 15 minutes following an abnormal event (HEP=1). No HEPs are assigned for a diagnosis time greater than 8 hours, since it is assumed that after 8 hours, the diagnosis will always be successful.

The diagnosis model represents the performance of a typical team of people, who are expected to be in the control room following an abnormal event.

6.4.5 Human Error Probability for Execution Tasks

The operator's response in coping with an abnormal event may be classified as either dynamic or step-by-step. A step-by-step task is a routine, procedurally guided set of steps that is performed one step at a time on one particular task at a time, without a requirement to divide the operator's attention between the task in question and other tasks. Post-accident step-by-step tasks are generally classified as Category C, Type 1. However, with high levels of skill and practice, a step-by-step task may be performed reliably, without recourse to written procedures.

A dynamic task is one that requires a higher degree of interaction between the people and the equipment than step-by-step, procedurally guided tasks. Dynamic tasks may include decision making, monitoring and/or the controlling of several functions, or any combination of these. Category C, Type 3 tasks (recovery actions) are generally classified as dynamic tasks.

Post-diagnosis actions are also assessed as being performed under moderately high stress or extremely high stress levels. A moderately high stress level is a level of disruptive stress that will result in a moderate deterioration in the performance effectiveness of system-required behaviour for most people. The onset of an abnormal event that is indicated by annunciators or other compelling signals is usually classified as resulting in at least a moderate stress level.

An extremely high stress level is defined as a level of disruptive stress that causes the performance of most people to deteriorate drastically. The occasion of a large LOCA is assessed as resulting in extremely high stress to operating personnel. For example (Reference 6-4), extremely high stress is assessed for the operator if one or more of the following conditions apply:

a) the maximum time available is less than two hours,

b) a single channel flow tube blockage occurs, or

c) more than two safety-related systems fail.

The NHEPs for post-accident execution errors are quantified based on ASEP methodology (Reference 6-1). The common practice for determining the NHEP is to use the median values for HEP (Reference 6-4), which include the effects of stress and complexity of the task. The HEPs assessed for the type of task and stress level are based on the values in Table 8-5 of Reference 6-1 and in Table 7.3-14 of Reference 6-4, and are presented in Table 6-4. The original performer (OP1) is the operator performing the task. In the case when the recovery of OP1 errors is still possible at the point of error action, the HEP for the related task and stress categories for the second person in the operating crew (OP2) are to be used. Also, a third operator can be credited for verifying the emergency actions and for taking recovery actions during an abnormal state of the plant. Verification may consist of checking and monitoring the adequacy of the heat sink configuration.

If there are RFs other than human redundancy (checkers), then the influence of these RFs will be assessed separately. Credit to the second and/or third operator (checker) can be given. The HEP for the third operator (checker) is the same as that for the second operator (checker) given in Table 6-4. Credit for the second and third operator is also conditioned by the following criteria.

For the tasks performed in the MCR,

a) if the allowed time is greater than 30 minutes, then credit for the second operator is given;

b) if the allowed time is longer than 60 minutes, then credit for the second and for the third operator is generally given.

For the tasks performed locally (in the field), including the SCA:

a) if the allowed time is shorter than 60 minutes, then credit for the second operator is not given;

b) if the allowed time is longer than 60 minutes, then credit for the second and for the third operator is given.

The total failure probability of the execution task is the product of HEPs for OP1, OP2 and OP3. The HEP values for each activity are then added for each task. This yields the total HEP for the activity under investigation. For the tasks, for which there is insufficient time to execute the task, the operator is not credited (HEP=1).

6.4.6 Dependencies for Post-Accident Actions

For zero dependence, consecutive operator actions are simply assigned the calculated HEPs. For complete dependence, the second and subsequent operator actions (branch points) are assigned a probability of 1.0 (certain failure) on the failure branch of the first operator action, and are generally not modelled in the event tree. For moderate dependence (MD) and high dependence (HD), the conditional failure probability equations are given in Table 6-2.

6.4.7 Quantification

The total failure probability for a post-accident operator action is taken as the failure of the operator to correctly diagnose the event or the failure to correctly execute the actions that must be taken within the total allowable time. Thus, the total failure probability for the combined diagnosis and execution tasks is given by the following equation:

$$\mathbf{P_t = P_d + P_e - P_d \times P_e}$$

where

P_t = total post-accident probability

P_d = probability of diagnosis error

P_e = probability of execution error

In this report, it is conservatively considered that $P_d \times P_e$ is small, compared with $P_d + P_e$, such that the combined failure probability is

$$P_t = P_d + P_e.$$

6.5 Recovery Analysis

Recovery analysis deals with the probabilistic evaluation of recovery actions, and is usually performed after ASQ at the cutset level. Recovery analysis will be performed on sequence cutsets for a PDS, if the probability of that core damage state is higher than anticipated. The operator actions that are credited during recovery analysis are based usually on component or equipment failure at the cutset level.

The following steps are involved in recovery analysis:

a) Obtain information for post-accident analysis.

b) Identify recovery actions that are included in event trees and fault trees.

c) Develop accident sequence descriptions.

d) Determine sequence and cutset timing.

e) Identify potential recovery actions.

f) Determine the available operator time.

g) Determine the operator performance time.

h) Select viable operator actions.

i) Determine the HEP.

6.5.1 Obtain Information for Post-Accident Analysis

The information for the recovery analysis is based on the plant response that is modelled in the accident sequence event tree analysis.

6.5.2 Identify Recovery Actions Included in Event Trees and Fault Trees

Post-accident operator actions are generally modelled in the event trees. In some cases, post-accident operator actions are modelled in the system fault trees. This is usually restricted to cases where only one system or subsystem is affected by the operator action. An example is the interconnection of the Class III odd and even 4.16 kV buses to restore auxiliary feed water to the steam generators, transfer power between odd and even buses to 480 V Class III motor control centres 5433-MCC 17A, MCC 18C and MCC 19B via manual transfer switches, and manually transfer from UST to SST.

6.5.3 Develop Accident Sequence Description

The accident sequences that are relevant for the recovery analysis are identified, and the following information is retained:

- initiating event and event tree number,
- event tree sequence number,

- sequence designator, and
- accident type and subsequent PDS.

6.5.4 Determine Sequence and Cutset Timing

The accident sequence is defined by the initiating event and the set of system successes and failures leading to plant damage. The dominant cutsets for recovery analysis are chosen among those having a frequency that is generally three orders of magnitude lower that the expected frequency of the core damage state. Thus, for the severe core damage states, the truncation limit for the cutset frequency is 10^{-10}.

For the selected sequence, the mission time is determined. This will define the approximate start time and end time, and the approximate sequence duration. The cutset failure time is determined based on information in steps a) and c)—see Sections 6.5.1 and 6.5.2. This is defined as the time at which the last failure in the cutset occurred. For demand cutset failure, the cutset failure time is zero. For running (mission failure) cutset failure, the cutset failure time is the midpoint of the mission phase interval.

6.5.5 Identify Potential Recovery Actions

The potential recovery actions in the cutset are determined among the equipment and component failures in the cutset. These potential recovery actions are usually applicable to one specific failure in the cutset.

6.5.6 Determine Available Operator Time

The time available to perform a recovery action is the amount of time from the point at which the affected equipment or component failed, to the time when the heat sink is lost (plant damage occurs).

For various sequences, the available action time is between 30 minutes and 40 hours, depending on the parameter that tripped the reactor, and whether or not feed water and condensate train is available. For events that jeopardize end shield cooling, the available operator action time depends on the calandria tubesheet thermal stress, and not on the feed water supply to the steam generators.

6.5.7 Determine Operator Performance Time

The operator performance time is the time required by the operator to execute the recovery action. If the action is simple and is performed in the MCR, then it may require only a few minutes. If the action is performed in the SCA, then another 15 minutes are to be added to the operator action time.

6.5.8 Select Viable Operator Action

A recovery action is considered to be viable if the time required to perform the action is smaller than the amount of time that is available to perform the action. If more than one operator action is capable of restoring core cooling, then the recommended order in which these actions are to be initiated is

- restore feedwater
- restore shutdown cooling
- start EWS

6.5.9 Determine Human Error Probability (HEP)

HEPs for recovery actions include the contribution of diagnosis errors and of execution errors, which are calculated according to the methodology for the quantification of post-accident operator errors, described in Section 6.4. HEPs for recovery actions during seismic or fire events will also consider the factors defined in Sections 7 and 8, respectively.

At the cutset level, the maximum credit for the human error composite should not be greater than 10^{-5}, when the time available is between 4 to 8 hours, and should not be greater than 10^{-4}, when the operator has between 2 to 4 hours to act.

For dominant sequences which contain operator error actions, the sequences may be re-evaluated using Reference 6-2 to re-calculate the HEP. Alternatively, the paired comparison/expert judgement method, NUREG.CR 3688 (Reference 6-5) may be used.

6.6 References

6-1. USNRC (prepared by Sandia National Laboratories), 1987, Accident Sequence Evaluation Program Human Reliability Analysis Procedure, USNRC Report, NUREG/CR-4772, SAND86-1996, Albuquerque, NM.

6-2. USNRC (prepared by Sandia National Laboratories), 1983, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (Final Report), USNRC Report, NUREG/CR-1278-F, SAND86-1996, Albuquerque, NM.

6-3. IAEA, 1989, Guidelines for Conducting Human Reliability Analysis in Probabilistic Safety Assessment, IAEA Report, report number, Draft No. 1.

6-4. USNRC (prepared by Sandia National Laboratories), 1990, Analysis of Core Damage Frequency: Internal Events Methodology, USNRC Report, NUREG/CR-4550, SAND86-2084, Volume 1, Rev. 1.

6-5. USNRC (prepared by M.K. Comer et al.), 1984, Generating Human Reliability Estimates Using Expert Judgement, USNRC Report, NUREG/CR-3688.

Table 6-1
Application of Recovery Factors to Pre-Accident Tasks

Case (1)	BHEP (2)	Control Room Indication (RF1) (3)	Post-Mtce / Calib Test (RF2) (4)	Written Verification (RF3) (5)	Written Periodic Check (RF4) (6)	Total Recovery Factor Credit (7)	Total Failure Probability (8)	Error Factor
I	3E-2	—	—	—	—	—	3E-2	5
II	3E-2	—	—	1E-1	1E-1	1E-2	3E-4	16
III	3E-2	—	—	1E-1	—	1E-1	3E-3	10
IV	3E-2	—	—	—	1E-1	1E-1	3E-3	10
V	3E-2	1E-4/1E-2**	—	—	—	1E-4/1E-2**	NEG**	10
VI	3E-2	—	1E-2	—	—	1E-2	3E-4	10
VII	3E-2	—	1E-2	1.0*	1E-1	1E-3	3E-5	16
VIII	3E-2	—	1E-2	1.0*	—	1E-2	3E-4	10
IX	3E-2	—	1E-2	—	1E-1	1E-3	3E-5	16

1) See Table 5-3 in ASEP HRA Procedure (Reference 6-1), for the cases that are applicable to critical activities.

2) See Section 6.3.2 for comments on BHEP.

3) See Section 6.3.4, item a, for comments on compelling signals and/or other types of MCR indication.

4) See Section 6. 3.4, item b, for comments on recovery factors that are applicable to post-maintenance and post-calibration tests.

5) See Section 6.3.4, item c, for the requirements on recovery factors that involve written verification of component status following maintenance or calibration.

6) See Section 6.3.4, item d, for a description of the periodic check/inspection recovery factor.

7) The total RF credit is the product of all applicable RFs.

8) The total failure probability is the product of the BHEP and the total RF credit.

* The failure probability of 1.0 for RF3 for Cases VII and VIII indicates that no recovery credit is given for RF3, if the PM or PC test is not done, or not done correctly, as per Section 6.3.4, item b.

** A HEP of 1×10^{-4} is assumed for a compelling signal, and a HEP of 1×10^{-2} is assumed for all other types of MCR indication.

Table 6-2
Conditional Failure Probability Equations for Different Levels of Dependence

Level of Dependence		Equations of Conditional Failure Probabilities	Approximate Value *
Zero Dependence	(ZD)	$P[B\|A\|ZD] = P[B]$	P[B]
Moderate Dependence	(MD)	$P[B\|A\|MD] = (1 + 6\ P[B]\ ) / 7$	0.15
High Dependence	(HD)	$P[B\|A\|HD] = (1 + P\ [B]\ ) / 2$	0.5
Complete Dependence	(CD)	$P[B\|A\|CD] = 1.0$	1.0

Notes:

1) The above table gives equations for the conditional failure probabilities for Task "B", given the failure of the previous Task "A", for five levels of dependence. This table is based on Table 10-2 of NUREG/CR-1278 (Reference 6-2).
2) Task "A" = the first task.
3) Task "B" = the second task.
4) $P_{[B]}$ = the probability of failure of Task "B", assessed independently.
5) $P_{[B|A]}$ = the conditional probability of failure of Task "B", given the failure of the immediately preceding task (Task "A").
6) * This column represents the approximate value of conditional HEPs, when $P_{[B]}$ is 0.01.

Table 6-3
Diagnosis Model for Estimated BHEPs and Error Factors

Item	Diagnosis Time (T_d) (minutes)	Joint HEP (Control Room Team)	Error Factor (EF)
1	0-15	1.0	—
2	16-20	1E-1	10
3	21-30	1E-2	10
4	31-60	1E-3	10
5	61-240	1E-4	30
6	241-480	1E-5	30

Note: The HEPs in this table represent the joint HEP for the performance of the entire control room crew.

Table 6-4
Assessment of Nominal HEPs by Task and Stress Level for Post-Accident Execution Tasks

Post-Diagnosis Actions (Execution)	Step-by-Step Task Moderate Stress		Step-by-Step Task Extreme Stress		Dynamic Task Moderate Stress		Dynamic Task Extreme Stress	
Operator	HEP	EF	HEP	EF	HEP	EF	HEP	EF
Original Performer (OP1)	2E-2	5	5E-2	5	5E-2	5	2.5E-1	5
Second Operator (Checker) (OP2)	2E-1	5	5E-1	5	5E-1	5	5E-1	5

Notes:

a) The HEPs are for independent tasks or independent sets of tasks, in which the actions that make up the set can be judged to be completely dependent.

b) A HEP of 1.0 is assessed for the total failure probability of the post-diagnosis task (diagnosis + execution), if no written procedures are available for a critical skill-based or rule-based action.

c) The HEPs and EFs in this table are taken from Table 8-5 in the ASEP HRA Procedure.

d) Credit to second and/or third operator (checker) can be given. The HEP for the third operator (checker) is the same as that for the second operator (checker).

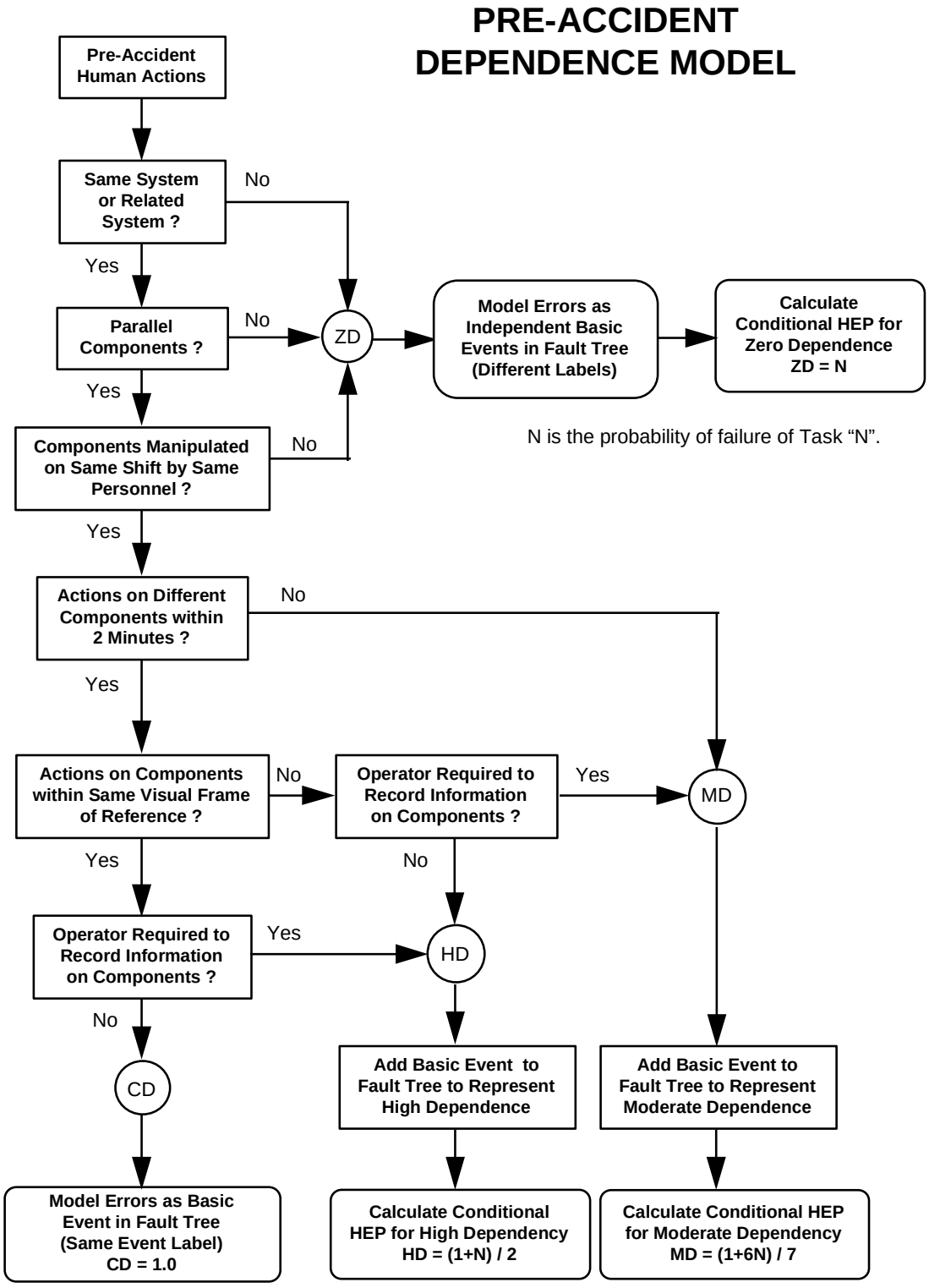


Figure 6-1 Model for Assessing the Positive Dependence for a Pre-Accident Task: Dependencies are Evaluated at System Level Only

7. SEISMIC EVENTS PSA

7.1 Introduction

Seismic events are one of several potential external events that may affect the plant. Seismic events need special consideration, because earthquakes cause upsets of the plant that require emergency systems and operator actions. Furthermore, earthquakes can cause failures that defeat system redundancy and diversity simultaneously, and can cause failures of "passive" components, such as tanks or structures. As well, during an earthquake, there may be additional stress on the operators.

International experience has shown that earthquakes may be a significant contributor to plant risk. It has been accepted that seismic events need to be included routinely in PSA. NUREG/CR-2815 (Reference 7-1) provides a general procedural guide for conducting a seismic PSA. NUREG-1407 (Reference 7-2) contains specific procedures and submittal guidance for conducting external event analyses, including seismic events. The report (Reference 7-2) was written for the Individual Plant Examination for External Events (IPEEE) for United States (US) Light Water Reactors by the US Nuclear Regulatory Commission. The report states that two assessment methods are acceptable—seismic margins or seismic PSA. The International Atomic Energy Agency has also issued a document that provides an overview of seismic PSA (Reference 7-3). CNSC's Consultative Document C-6 (Reference 7-4) lists the requirements for the safety analysis of CANDU nuclear power plants and lists a seismic event as a Class 3 event.

For the purposes of the Generic CANDU PSA the seismic PSA methodology is described in this section. Because of the large uncertainties in seismic hazard input, a PSA-based seismic margin analysis is considered an alternate method depending on the objectives of the PSA. A PSA based seismic margins assessment consists of similar steps to a seismic PSA but does not include the last step of integration of the hazard curve with the rest of the analysis. Due to the uncertainty in the hazard curve, AECL's expects to use PSA-based seismic margin analysis for future CANDU plants.

7.1.1 Scope

There are many steps to be followed in performing a seismic PSA. Figure 7-1 shows the typical steps involved in a seismic PSA. The following is a list of the major aspects that are associated with a seismic PSA:

a) the determination of the seismic hazard at the site, i.e.: the calculation of the frequency of earthquakes of various sizes and the type of motion,

b) the evaluation of seismic local ground motion and building motion,

c) the determination of responses of plant systems and components, spatial interactions and plant configuration (seismic walk-down),

d) a fragility analysis of components and structures,

e) a plant systems analysis and HRA,

f) an accident sequence quantification, and

g) uncertainty and sensitivity analyses.

7.2 Plant Design Information

PSAs are broad, integrated studies that require a considerable amount of information related to the plant design, analysis and operation. This applies to internal or external events PSA. The seismic PSA requires work that involves the analysis of the seismic hazard at each site, the identification of seismic initiating events and the fragility analysis of structures and components.

To assess the seismic capacity of the plant, the seismic design philosophy needs to be understood. This information is available in safety and engineering design guides, and in seismic Canadian Standards documents (References 7-6, 7-7, 7-8)

There are two seismic levels of earthquakes, which are defined in accordance with CAN3-N289.1 (Reference 7-6) as follows:

a) Design basis earthquake (DBE)

   The DBE denotes an engineering representation of the potentially severe effects of earthquakes that are applicable to the site, and that have a sufficiently low probability of being exceeded during the lifetime of the plant. The DBE effects on the site are described by the DBE ground response spectra (GRS). Its effects within structures at the site are described by the floor response spectra (FRS) or time histories that are developed for selected locations in each structure.

b) Site design earthquake (SDE)

   The SDE denotes an engineering representation of the effects at the site of possible earthquakes with an occurrence rate, based on historical records, of not greater than 0.01 per year.

A third earthquake level is defined by the National Building Code of Canada for application to systems and structures that are not required to be qualified to DBE or SDE.

A significant amount of information is required from almost every discipline that is responsible for the design of the nuclear and the BOP systems. This information must be organized and communicated to the PSA team in a fast, reliable and consistent manner. The purpose is to ensure that all the analysts consistently use the same information and the latest version of the information.

The following information is typically necessary:

a) CNSC regulatory document (e.g., Consultative Document C-6 Rev. 0 (Reference 7-4),

b) compliance document with regulatory documents,

c) licensing basis documents,

d) technical description,

e) safety design guides,
f) PSA methodology documents and design guides,
g) systematic review of plant design for initiating events,
h) internal events PSA,
i) design manuals,
j) system flow sheets,
k) safety analysis reports,
l) ground response spectra,
m) floor response spectra,
n) equipment, structure and support systems design criteria and descriptions,
o) equipment specifications—weight, material, capacity, size, power rating and manufacturer,
p) equipment outline and assembly drawings,
q) equipment installation specifications and drawings,
r) seismic qualification reports—analysis and tests,
s) concrete data—drawings, specifications and test data, and
t) anchorage drawings and specifications.

7.3 Seismic Hazard Analysis

7.3.1 Introduction

Seismic hazard analysis (SHA), also known as probabilistic seismic hazard analysis, is one of the main tasks of the seismic PSA. It is essential in the quantification process. The analysis provides the frequency of earthquake motions at various levels of intensity at the site. This output is known as the seismic hazard curve, and is expressed in terms of a particular measure of intensity (peak ground acceleration or spectral acceleration versus the annual probability of exceeding this level of intensity). This section highlights some of the important aspects of SHA. The general requirements and methods for SHA are provided in CAN3-N289.2 M81 R92 (Reference 7-7).

The SHA accounts for the variation due to randomness and uncertainties in earthquake magnitude and location, and in modelling techniques, respectively. Modelling uncertainties may occur in basic models or parameters that are used in the analysis, such as fault geometry, or ground motion attenuation.

The SHA has the following objectives:

a) to determine probabilities for earthquake scenarios,

b) to determine, for each earthquake scenario, a conditional probability of exceeding, at each site, the motion level of interest,

c) to provide a framework for synthesizing the probabilities for all scenarios into a single hazard result (curve), and

d) to provide input to the ASQ of the seismic PSA.

With the determination of the seismic hazard curve, seismic fragilities for individual components, equipment or structures may be merged with the curve to calculate the frequency of particular accident sequences. It is not necessary to know all the details and assumptions in the derivation of the seismic hazard curve in order to use it.

The seismic hazard curve is usually derived from the input of different experts in their respective fields - seismology, geology, etc. It is also influenced by methods that are used to solicit expert judgement. As was shown by seismic curves developed by EPRI and Lawrence Livermore National Laboratory (LLNL) in United States in the 1980's, the difference in method can be significant. The AECL approach is outlined below. Recent practices for the systematic development of hazard curves are available in NUREG/CR 6372 (Reference 7-9).

The AECL method used to obtain the seismic hazard is specified in CAN3-N289.2 M81 R92 (Reference 7-7) as described below.

7.3.2 Methodology

AECL follows the generally accepted worldwide practice for conducting a SHA. The SHA may be divided into four main steps (References 7-5, 7-6, 7-7, 7-8, 7-9, 7-10), as shown in Figure 7-2:

Step 1: Determine the seismic source characterization, i.e.: identify the seismic sources in the area around the site.

Prior to any analysis, it is first necessary to collect as much seismic information as possible about the region where the site is located. This includes information from past earthquakes, area geology, plate tectonics, paleoseismicity, etc. With this information and appropriate earthquake models, the seismic sources that affect the site can be identified.

Step 2: Calculate frequencies of occurrence of earthquakes of different magnitudes (recurrence).

The recurrence relationship is normally shown as a frequency versus magnitude (peak ground acceleration) relationship for a given seismic source (point, line, area). The original work on magnitudes - recurrence is given by the recurrence relationship of Gutenberg & Richter (Reference 7-11).

Step 3: Model ground motion attenuation.

The decrease in the intensity of ground motion with distance from the epicentre of the earthquake is called "attenuation". In other words, it is the relationship between ground motion versus distance for each magnitude. The attenuation of ground

shaking varies in different parts of the world. Some areas may attenuate much more rapidly than others.

Step 4: Produce a single seismic hazard curve.

The fourth step involves the integration of the information, in order to derive the seismic hazard curve. The curve is usually shown as frequency of exceedance versus a ground motion parameter. Figure 7-3 (Reference 7-12) show a typical seismic hazard curves for the Surry nuclear power plant.

Following the assessment of the seismic hazard for firm ground, the local ground and building motions have to be determined. Soft soils affect the frequencies and amplitudes of the ground motion entering the structures. These effects must be taken into account. For rock sites, it may be acceptable to assume that the base motions are the same as the free field.

Typically, for a site-specific seismic hazard, a computer program is used to calculate this seismic hazard. One such program is EZ-RISK, developed by 1997 Risk Engineering, Inc. of Boulder, Colorado, USA. This program, which is used by AECL, calculates the earthquake hazard at a site both probabilistically and deterministically under certain assumptions that are specified by the user. These assumptions involve identifying the location of the earthquakes, their potential characteristics, and the ground motions that they may generate. These assumptions are site-dependent. The assumptions will be specified in the appropriate design guide document. The results of the program's probabilistic calculations are annual frequencies of exceedence of various ground motion levels at the site of interest.

7.4 Seismic Fragility Evaluation

7.4.1 Overview

The seismic fragility evaluation calculates the seismic capacity of individual components and structures. The fragility of a component is defined as the conditional probability of failure for a given seismic input motion or response parameter, e.g., peak ground acceleration. This response is normally represented as a fragility curve. Guidelines for equipment and structure fragility calculations are described in Appendix B.

The objective of the fragility evaluation is to estimate the ground acceleration capacity of a given piece of equipment or structure.

There are two aspects to the calculation of fragilities: (*a*) the definition of the failure of the component, and (*b*) the determination of the seismic capacity. Components may have more than one failure mode, and each mode must be considered in the analysis. Therefore, there may be more than one fragility curve for a particular component, wherever different failure modes are possible.

Generally, for equipment, failure denotes the inability of the equipment to perform its safety function. Sometimes, the failure may be short term and may have no lasting damage, such as

relay chatter. The consequences of failure are also important. By reviewing equipment design, the failure mode that is most likely to occur as a result of a seismic event is identified. Three types of equipment failure are usually analyzed:

a) anchorage

b) structural

c) functional

For structures, failure usually means the collapse of the structure, which damages the equipment or interferes with the functioning of safety equipment, due to buckling or fracturing. The interactions between structures and equipment may be difficult to interpret from drawings. A seismic walk-down assists in this area.

To summarize, the following are some of the possible failure modes for different components:

- Structures - inelastic deformation that exceeds the operability limits of equipment.
- Piping - fracture or collapse of the pressure boundary, failure of supports, attachment failure.
- Equipment - structural: bending, buckling of supports, anchor bolt pull-out, etc; functional: binding of valve, excessive deflection, relay chatter.
- Soil - liquefaction, toe bearing, base slab uplift, slope instability.

7.4.2 Fragility of Components and Structures

A scaling method is used to derive the fragility of a component. The intent is to derive an actual response and capacity, as opposed to a design response and capacity of a component. This is estimated from information on the plant design basis, response calculations for the design basis or a reference level earthquake, as-built dimensions and actual material properties. Other information sources may be fragility test data, earthquake experience data and engineering judgement.

Three parameters characterize the fragility curve: the median ground acceleration, A_m, the logarithmic standard deviation reflecting randomness in the capacity, β_r, and the logarithmic standard deviation reflecting uncertainty in the median capacity, β_u. These parameters are estimated for each failure mode of the component, by taking into account the seismic design, qualification and installation of the component.

The failures modes of equipment that are assessed are their functionality, their structural integrity and their anchorage. In some cases, the weakest link only may be assessed. Some of the variables to take into account are the strength, inelastic energy absorption, spectral shape, damping, modelling, method of analysis and testing, combination of modes, combination of earthquake components, structural response, soil-structure interaction, and ground motion incoherence.

Some of the variables for the analysis of structures are strength, inelastic energy absorption, spectral shape, damping, soil-structure interaction, modelling, method of analysis and testing, combination of modes, and combination of earthquake components.

Figure 7-4 shows a typical fragility curve. A commonly used value that describes the seismic capacity of components is the high confidence of low probability of failure (HCLPF) value. This value typically represents the 5% probability of failure of a component, with a 95% confidence level, and is calculated using

$$\text{HCLPF capacity} = A_m \exp [-1.65(\beta_r + \beta_u)].$$

The HCPLF gives a good indication of the capacity of a component, and is also useful for the quantitative screening of components. This screening reduces the number of components that need to be included in the analysis. Typically, a screening value is selected, above which components are screened out.

7.4.3 Sources of Fragilities

Generic qualification test data may also be used, if the data can be shown to be appropriate for deriving fragility data. A source of generic fragilities for components was developed in the Seismic Safety Margin Research Program (SSMRP), NUREG/CR-3558 (Reference 7-13). Fragility functions for the generic categories were developed, based on a combination of experimental data, design analysis reports and an extensive expert opinion survey. Lawrence Livermore National Laboratory (LLNL) lists fragility medians, random uncertainties and modelling uncertainties for a wide variety of components that were analyzed in past seismic US PSAs (Reference 7-14).

Fragility testing of components has been conducted as USNRC-funded research. The testing was conducted by Brookhaven National Laboratory (BNL) and LLNL. BNL tested 18 component types, whereas LLNL tested 8 component types. The components of the BNL tests were manufactured as Class 1E, or Seismic Category I after 1975. The results of the testing are available in numerous NUREG/CR documents.

Another source of earthquake information is obtained from investigations that follow earthquakes. Many facilities have been surveyed for damage following earthquakes, including fossil-fuelled and hydroelectric power plants, electric distribution stations, petrochemical and other large industrial facilities. The facilities that have been surveyed represent a wide range of facilities in terms of age, operating configuration, manufacturer, local soil conditions and quality of construction and maintenance.

7.5 Seismic Walk-Down

A seismic walk-down is performed at a site to determine any as-built construction deviations, and to assist in the fragility analysis of components and structures. The objectives are

a) to identify all equipment items that are expected to have sufficiently high seismic capacities;

b) to clearly define failure modes for components that are not expected to have high seismic capacities;

c) to review and gather detailed information and measurements on equipment and structures for performing seismic fragility evaluations;

d) to observe and record any deficiencies (e.g., missing anchor bolts, loose mounting of relays, excessive cracking of concrete) that may reduce the seismic capacity of components;

e) to identify spatial interactions, e.g., equipment that is not DBE-qualified and that is situated above or beside DBE-qualified equipment, heavy equipment or ceiling fixtures;

f) to identify areas for potential seismic-induced fires (e.g., storage areas for flammable liquids or gases);

g) to evaluate the fire protection systems in the plant for inadvertent actuation (potential seismic-induced flooding) and the capability to mitigate against seismic-induced fires;

h) to evaluate the seismic capacity of other piping systems, e.g., recirculating cooling water (RCW) piping, and safety systems in the reactor building and other buildings that are designed to handle seismic-induced flooding.

Some other issues that pertain to components on the safe shutdown equipment list (SSEL) are listed in Section 7.6.2.

The most important part of a seismic walk-down is the assembling of the appropriate personnel that are necessary for such an undertaking. The team has to be multi-disciplinary. The team consists of

a) systems engineers who are familiar with plant design and operation,

b) plant operations personnel who are knowledgeable about operating procedures and abnormal accident response, and

c) seismic capability engineers who are familiar with walk-down and seismic qualification analysis.

The seismic review team must be knowledgeable about the failure modes, the performance of structures and equipment during an earthquake and nuclear design standards. The team must be experienced in determining the seismic capability of electro/mechanical equipment and performing fragility calculations. Finally, the team must have a general understanding of seismic PSA and systems analysis, as well as a general knowledge of plant systems functions.

The duties of the seismic review team include the assessment of components to be screened out (high seismic capacity components); the specification of failures to be investigated for non-screened items; the inspection of components for deficiencies; and the identification of system interactions to be evaluated.

Equipment is usually divided into classes, such as horizontal pumps, vertical pumps, fans, valves, motor control centres, cable trays, transformers, inverters, pressure and level sensors, diesel generators, and heat exchangers. In some cases, it is not necessary to check all components of each equipment type, but only to check a representative piece.

There are also a number of checklists that can be developed and used as required. Samples of the types of questions that are asked as part of a screening evaluation and a screening verification are shown in Table 7–1 and Table 7-2, respectively.

A typical equipment evaluation for anchorage may involve the following steps:

a) Observe and note the number, type, condition and size of anchor bolts, plug welds, or fillet welds.

b) Check anchor spacing, free edge distance, and concrete condition.

c) Check that all specified anchor bolts, plug welds, or fillet welds, as per design drawings, are present. Note any non-uniformity in the installation of anchorage, grout and concrete, and the condition of nearby concrete.

d) Verify that all nuts are present and are apparently tight on all bolts and/or that bolts are apparently tight on expansion anchors. Note that a torque test is not required, unless a bolt or nut is suspected to be loose.

e) Where visible, spot check that the gap under the base is less than ¼ inch for bolted anchorage.

f) Check that anchorage appears to be relatively stiff, and that there is no excessive prying action on anchors.

g) Determine whether or not excessive flexibility exists between tie-down anchorage and cabinet walls.

The identification of system interactions is another important aspect to be covered in a seismic walk-down. The issues to be dealt with are:

a) the potential for equipment to fall on seismically qualified equipment;

b) equipment proximity—specifically, the effects of the seismic motion of an item on an adjacent item, e.g., a pipe hitting a component;

c) seismic-induced floods, e.g., the failure of pipes or vessels; and

d) seismic anchor motion, i.e., differential building motion, e.g., flexible headers and a stiff branch, or vice versa, flexible or unanchored equipment and a stiff pipe.

A seismic walk-down provides information on the as-built plant, and provides relevant feedback to the seismic PSA.

7.6 Systems Analysis

7.6.1 Introduction

The safety objective for the design of a nuclear power plant is to protect the public and plant workers from adverse health effects due to the release of radioactive materials during normal plant operation and during accident conditions. The following general safety functions must be performed during accident conditions:

a) Shut down the reactor and maintain it in a safe shutdown condition.

b) Remove heat from the fuel (stored and decay heat).

c) Limit the release of radioactive material by maintaining a barrier.

d) Monitor the condition of the plant, and perform actions that are necessary to maintain the above safety functions.

Each of the above safety functions may be performed by several different safety related systems and structures, for example, there are two special safety systems to shut down the plant (SDS1 and SDS2).

Similar to the internal events PSA, the potential initiating events (IE) occurring from seismic events must be identified. In addition, any random or consequential events that result from the earthquake must be identified (e.g., flood). Once the IEs are identified, the mitigating functions that are required to respond to these events and the systems that provide these functions must be determined.

7.6.2 Safe Shutdown Equipment List

The first step in the analysis is to identify the SSEL. These are components that are necessary to perform the safety functions, and include both front-line and support systems. The support systems, such as electrical power, cooling water and instrument air provide services to the front-line systems. The SSEL also includes items that may fail during the earthquake, and that may lead to an IE. The IEs identified in the internal events PSA must be reviewed and taken into account to ensure that all potential IE events are covered in the seismic PSA.

The internal events PSA fault trees do not provide a complete list of equipment for the seismic PSA; structural items must be added to the list, e.g., electrical panels and cabinets, instrument racks, walls, buildings, etc. Structures containing PSA related items and other equipment identified must be identified. For each safety function, the safety system(s) must be identified, after which the necessary equipment is listed (see Table 7-3).

Generally speaking, manual valves, check valves, small relief valves and other passive equipment are not included on the SSEL. It is assumed that they are seismically rugged. However, during a seismic walk-down, these items can be checked. Solid state relays are also considered to be seismically rugged and are not included on the SSEL.

Various sources of information for the SSEL include the seismic qualification equipment list, purchase orders, the basic event list for the internal events PSA, design or operational flow sheets and elementary wire drawings. Component information that is needed for items on the SSEL includes the component identification, description, redundancy, component location (room and elevation), type/class of component, normal operating position, fail-safe position, manufacturer, power supply (control and power), and any other special conditions that may apply. Table 7-1 shows an example template for the collection of such information.

There are some other special considerations that need to be taken into account when compiling components on the SSEL:

a) Identify active components that are required for the isolation of potential diversion paths.

b) Identify inactive components that are required for the integrity of the system, e.g., HTS—a loss of integrity of the HTS could lead to a LOCA.

c) Identify unique plant features and special interaction items, e.g., fuel handling machine bridge, overhead cranes, control room ceiling, plant stacks, tall storage tanks.

d) Identify any hazardous materials storage containers, especially flammable or toxic gas.

e) Identify any block walls that may fall and fail safety equipment.

f) Identify sources of potential seismic fire and seismic flood interactions. Only gaseous or liquid combustibles need to be considered. Special attention should be paid to hydrogen handling, piping and storage.

g) Verify that all components that appear in the internal events PSA are included in the SSEL, or that there is a reason for exclusion. One obvious rationale is that some systems in the internal events PSA depend on offsite power, which may not be available after a seismic event.

h) Review abnormal operating manuals for the loss of offsite power, etc., to ensure that all equipment and instrumentation that are referenced in the procedures are on the SSEL.

i) Consider the results of initial discussions regarding general and specific plant practices and procedures that are related to system success and operator recovery actions.

It is necessary to be familiar with the electrical system—its layout, bus hierarchy and cabinet and panel naming conventions, etc.

7.6.3 Damage Correlation Issue

Earthquakes may cause multiple equipment failures at the same time. The likelihood of this occurrence of depends on the seismic capacity of the equipment and the intensity of the earthquake. It is rather difficult to fully account for these correlations, since the analysis methods are complex and are heavily dependent on judgement.

Several assumptions are made to simplify the process of taking into account correlations between equipment:

a) the response of identical equipment at the same elevation is assumed to be 100% correlated, i.e., if one set fails, then the other fails as well, that is to say their fragilities are the same, and

b) other response correlations are assigned zero correlation i.e.: they are independent.

Usually, sensitivity analysis studies are used to determine if these assumptions are critical. Partial dependency may be included in models, if necessary, by modifying the Boolean equations.

7.6.4 Screening of Equipment by Calculation

The purpose of screening is to reduce the amount of effort that is required to solve the event trees, and to reduce the number of components in the Boolean equations. The Boolean equations are the algebraic representation of the accident sequences of the event tree (see Section 7.6.11). The selection of an appropriate screening value depends on the seismic hazard level, the relative capacity of dominant components, and the DBE level. Either the median or HCLPF seismic capacity can be used. If a component contributes less than 10^{-6}/yr to core damage, then its contribution is considered minimal, and it can be screened out.

If the screening value is too high, then no components will be screened out, whereas if it is too low, then too many components will be screened out and the results will not be realistic. A sensitivity analysis can be performed to confirm the chosen screening value.

For equipment that is not screened out, an FMEA is conducted to determine the impact of the structure or equipment failure. The equipment that has been identified by the FMEA as having serious consequences is included in the quantification of the seismic event tree.

7.6.5 Seismic Event Tree Development

A seismic PSA includes the evaluation of accident sequences. The methodology that is used to develop event trees for plant seismic events and to perform accident sequence event tree analysis is described in this section. The methodology for developing seismic event trees is somewhat different from that of the internal events PSA.

The event tree structure describes the combination of system successes and failures that can result in the design basis accidents and/or core damage. The structure reflects system interrelationships and accident phenomenology that determine whether or not the sequences lead to severe core damage. In association with the seismic hazard curve and component fragility calculations, the seismic event trees are used to perform ASQ to derive the frequency of the final state (end-state) of a particular accident sequence. The mitigating systems for which the availability is explicitly questioned in the event trees, up to the point of severe core damage, are referred to as front-line systems (e.g., shutdown cooling, auxiliary feed water). Any system that provides a service (e.g., electrical power, cooling water, instrument air) to a front-line system is called a support system. Mitigating and support systems may fail at the same time, as a result of

the seismic event. In this respect, the methodology is different than for the internal events PSA, where the IE generally affects one component or system at a time, unless it is a support system failure.

Generally, accident sequence seismic event trees are developed as one master event tree, unlike the internal events PSA, which has many separate IEs with their own event trees.

Two sets of event trees need to be developed. The first set of event trees will be strictly used to define and quantify the Level I sequences that lead to SCD. As such, the sequences in the Level I event trees will terminate on either a success state, a damage state in which the reactor core has disassembled (SCD), or a relatively more benign state of damage, either to fuel bundles or to a limited number of channels within the core. The essential purpose of the Level I event trees is to easily determine the summed SCDF, and the frequencies of lesser damage states, if desired.

In order to interconnect Level I and Level II PSA activities effectively, there is a need to consider failures of containment systems, in addition to considering the status of the core. This is accomplished by creating a second set of event trees that also question the availability of containment systems, and that can affect the accident progression analysis. These trees are called extended Level I event trees. These event trees incorporate containment systems.

7.6.6 Event Tree Construction

Accident sequence event trees are usually bi-modal logic diagrams at the system level of detail, which describe the possible sequences of events that follow each initiator. The objective is to define all the possible combinations of successful and unsuccessful system responses to a seismic IE. The event tree starts with the IE, progresses through a logical set of decision branch points (mitigating system success or failure states), and concludes when stable conditions (with or without releases) are achieved, or when there are no more available mitigating systems.

A desktop-computer based event tree program called ETA-II (Reference 7-15) is used to produce the event trees. A typical seismic event tree for a CANDU 6 system is shown in Figure 7-5.

7.6.7 Event Tree Assumptions

To prepare the event trees, the physics, fuel, and thermalhydraulic response to each initiating event must be known. Most of the deterministic analysis that is associated with the above is normally documented in a safety report and can be considered, in general, as a PSA support analysis. Analysis is required to support assumptions that are made in the preparation of the event trees for a given PSA. In this document, any additional analysis that is required to support PSA assumptions is termed PSA support analysis, and is required for conditions that are beyond the scope of the safety analysis. PSA support analysis may be required in the following situations:

a) if the event has never been analyzed before,

b) if design changes in the plant of interest have an impact on the plant response, or

c) if other new information (e.g., more recent research and development results) on plant response becomes available.

7.6.8 Order of Events

The event order of the mitigating systems and operator actions in the seismic event trees depends on the results of the seismic capability of the systems. The most critical failures should be put at the front of the seismic event tree. The branch points should roughly correspond to the following order:

a) failures that result in SCD directly from the seismic event,

b) the loss of seismically qualified systems due to the seismic event,

c) the loss of support systems due to the seismic event,

d) the loss of other heat sinks due to the seismic event,

e) the loss of non-seismically-qualified equipment due to the seismic event, and

f) the loss of any remaining systems due to random failure.

In addition to these events, the extended Level I event trees will subsequently check the availability of containment systems for SCD sequences.

7.6.9 Operator Actions

Operator actions are included as far along in the event tree as possible, and are usually placed just before the system that is to be manually initiated. Operator branch points are modelled on a per-system basis, which means that more than one operator branch point could appear in the same sequence. Repeat operator action branch points (i.e.: the operator is called upon to mitigate his or her own previous failure) can be credited if there is time available for the subsequent actions, and if there are independent signals that indicate that the previous actions taken were ineffective. These signals might originate from the clear annunciation of abnormal conditions or instrumentation, which the operator is procedurally required to monitor to verify the successful operation of the initiated system. Another option involves placing the operator actions directly in the Boolean equations.

Details regarding the pre- and post-accident operator models are provided in Section 6.

7.6.10 Mitigating Systems

The top events for the mitigating systems, which appear in an event tree, symbolically represent a seismic failure of a system or a failure during mission. The IE is the seismic event itself.

The mission time for internal events is normally 24 hours if there are redundant systems. However, in the case of a seismic event, the damage may be more severe. Generally, a 72-hour mission time is considered. For the case of the loss of offsite power, it is assumed to not be recovered. The possibility of outside assistance is also not considered, since roads, bridges, etc.

may be damaged. A sensitivity study can be made to show the effects of different mission times.

Front-line and support systems that are credited to mitigate any IE that results in harsh environmental conditions must be environmentally qualified to operate in those conditions.

7.6.11 Quantification of Accident Sequences

ASQ is undertaken to estimate the frequency for individual accident sequences. The objective is to merge the seismic hazard curve and the fragilities of components and structures for all the branches in the seismic event tree. In so doing, the frequency combinations of different fragilities are taken into account. The ASQ process thus provides an accurate assessment of the summed core damage frequency. See Section 7.8 for further details.

Event sequence termination assists in reducing the amount of analysis.

The development of a typical accident sequence ends with the determination of the state of damage to the plant. Specifically, the outcome, or end-state (final state) of an event tree sequence is either a plant success state, where fuel cooling is maintained with no radionuclide release into containment, or a PDS, with a radionuclide release into containment. The methodology for determining the PDSs is described in Section 4.9. PDS define the status of the core, as well as those front-line and containment systems that have an impact on the subsequent accident progression, once radionuclide releases into containment occur.

The end-states for the Level I event trees are defined as follows:

a) Success states, where the plant is shown to be in a safe shutdown condition, with no releases for the entire duration of the accident repair time. The plant state label for these sequences is "S".

b) PDSs, where all pertinent front-line mitigating systems have been called upon in an effort to prevent releases to containment. If the sequence leads to SCD, (i.e.: all means of fuel cooling have been lost, including the moderator system),then the sequence is labelled "SCD". The PDSs will be explicitly categorized for these sequences in the extended Level I event trees.

The Boolean equations for the seismic event tree are generally evaluated from 0.02 g to 1 g peak ground acceleration. A check is necessary to ensure that the cut-off peak ground acceleration is not too low, by running the analysis at a higher "g" value.

Accident sequence nomenclature is described below.

A labelling scheme or nomenclature is developed for the accident sequences. Generally, the dominant sequences are tabulated, and the nomenclature is described as follows:

a) Sequence name, consisting of

   sequence number—each sequence is given a specific number, e.g., S1, S2, etc.

b) Plant damage state.

c) Sequence descriptor—nomenclature that describes the success or failure of the various mitigating systems that are involved, due to the seismic event and due to random failure.

The forward slash (/) in the sequence descriptor indicates the success of the mitigating system or operator action. The lack of the forward slash indicates the failure of the system or operator action. The asterisk (*) indicates that all the events in the sequence are "ANDed".

An example from Figure 7-5 for sequence number SCD-1 is:

SCD-1 = /RS*/GRP2*SLOCA*ECC, which represents the sequence of the reactor shutting down, Group 2 systems surviving the earthquake, a small LOCA occurring, and ECC failing seismically. In this case, it is assumed that the moderator system has also failed.

7.6.12 Reporting of Event Tree Results

Three items, all of which result from an accident sequence event tree analysis, are generally reported. These items, which are based on CANDU practice and are also listed in NUREG/CR-4550 (Reference 7-16) include

a) Assumptions

   Any assumptions that are made in developing the event trees are discussed, including the manner in which they could affect the final result.

b) Event tree

   Event trees are presented in graphic form to show all sequences that could be potentially dominant. As previously noted, the computer program ETA-II (Reference 7-15), is used to provide graphic representation of the event trees.

c) Accident sequences

   Each sequence or group of similar sequences is described. Sequences that are not completely developed should be explained. In CANDU practice, sequence descriptions include the following information:

   1) a brief description of the seismic initiating event,
   2) a description of the plant response (event sequence), and
   3) a brief description of each event tree heading (top event).

7.7 Human Reliability Analysis

7.7.1 Introduction

In general, the purpose of the HRA task is to identify potential pre-accident and post-accident human errors, and to quantify the most significant of these in terms of HEPs. This task covers the analysis of all human actions of potential concern that are identified during the PSA process. The HRA task also helps to identify and evaluate operator recovery actions under accident conditions.

It is recognised that there is uncertainty in the absolute values estimated by HRA methods. However, the primary value of including an assessment of human error within a PSA study is to identify the most important operator actions, and to help the operator to perform those actions as reliably as possible. Uncertainties in the HEPs that are included in the event trees and fault trees are quantified, and are included in the overall PSA uncertainty analysis.

7.7.2 Types of Human Error

The generic human actions that are common to NPPs can be grouped into the three major categories and discussed below:

a) Category A actions-pre-accident human actions (pre-initiators),

b) Category B actions-human actions that lead directly to IEs (initiators), and

c) Category C actions-post-accident human actions (post-initiators).

Category A actions occur prior to an accident, and are associated with human errors that degrade the availability of mitigating systems. In other words, these pre-accident tasks, if performed incorrectly, can result in the inability of systems or components to respond appropriately to an accident. Pre-accident errors include the miscalibration of instrumentation, and the failure to restore equipment to full operability, following test and maintenance activities.

Category B actions contribute to IEs or plant transients. They may be due to control room actions or errors during normal operations, or maintenance or testing errors. These errors are generally reflected in IE frequencies.

Category C actions are post-accident tasks that are required to cope with an abnormal event, i.e.: to return the plant or facility systems to a safe condition, following an IE. Post-accident errors include the failure of the operator to diagnose and respond correctly to accidents. Also considered under Category C are actions that may be taken to recover previously unavailable equipment, or the use of non-standard procedures to mitigate the accident conditions.

7.7.3 Approaches to Quantifying Human Error

The accurate prediction of the probability of human errors during the performance of a HRA for existing facilities is a difficult and complex task. In fact, in order to obtain even a reasonably accurate prediction of human behaviour, based on a thorough task analysis of every human action in a PSA, a large expenditure is required. Such detailed analysis involves visits to the site in question, and a detailed analysis of the facility's administrative control procedures and their implementation. The analysis includes the assessment of environmental factors, personnel experience levels, and the accuracy and comprehensiveness of written procedures.

For new facilities or in a design PSA, other difficulties may arise due to a lack of information. Visits to the facility and its simulator training centre, the evaluation of environmental factors and the experience level of its operational and maintenance staff, and the examination of plant-specific written procedures are not possible. It is therefore necessary to make certain assumptions, with respect to test and maintenance procedures, and other relevant normal

operating procedures, restoration procedures, accident management procedures, etc., in order to develop the HRA methodology.

Since it is either not practical or not possible to undertake a detailed assessment of every human action in a PSA, the accepted industry approach is to assign conservative HEPs to all tasks, following relatively simple guidelines. Typical examples of this are the Accident Sequence Evaluation Program (ASEP) Screening HRA and ASEP Nominal HRA models that are described in NUREG/CR-4772 (Reference 7-17), which are easier to implement, but which are still conservative with respect to the standard Technique for Human Error Rate Prediction (THERP)/Handbook methodology described in NUREG-CR-1278-F (Reference 7-18).

The means by which seismic post-accident (Category C) human errors shall be quantified is described below. The models are based on the ASEP procedures referenced above. Generally speaking, the human actions from the internal PSA are modified to arrive at a new HEP for seismic events. If the scope of a given project requires the performance of more detailed evaluation procedures for risk-significant human actions, they will be developed as an addendum to the generic methodology.

The HRA methodology described in the internal events PSA is followed (see Section 6).

7.7.4 Performance Shaping Factors

During a seismic event, the operator faces a complex situation, which is a result of the supplementary stress caused by the earthquake itself, the random damage of systems and components, possible induced fires and floods, aftershocks, and the likely impairment of communications and control room indications. The time that is available for diagnosis and for execution is also likely to be lower than for internal events. Therefore, it is expected that a seismic event has adverse effects on operator performance.

It is reasonable to assume that the impact on human actions will vary with the strength of the seismic event. Therefore, we assume that operators will be unable to perform required actions in the presence of seismic levels that are severe enough to fail the building structure, because the operators may be physically blocked by fallen debris. If some part of the building collapses, then the operators will be unable to perform actions, at least in that area. On the other hand, for very mild “g” earthquake levels, it is expected that there will be no degradation of the human action error probability, compared with the internal events PSA case. Regardless of the earthquake “g” level, however, most operators have not experienced a seismic event, and this can adversely affect their performance.

Also, a seismic event is assumed to have a greater impact on human actions in the short term, although some other factors are not time-dependent. These influences can be expressed in terms of time-dependent and time-independent performing shaping factors (see Section 6).

The time-dependent PSFs are:

- Operator Stress Level - in the first several minutes after the earthquake, the operators may have not recovered from the initial shock, but the effect slowly diminishes in time.

- Number of Concurrent Actions in Progress - in the early stages, a variety of activities can commence, producing some confusion in the control room. The plant begins to stabilize further into the event, thus reducing the amount of concurrent actions in progress.
- Communication - in the first several minutes, communication may be more difficult due to the shock of the seismic event, as compared to later into the event, when the plant starts to stabilize.
- Adequacy of Personnel - in the first minutes, some operators inside or outside control room may not be mentally or physically available to perform a desired task.

The time-independent PSFs are:

- Indications in the Control Room - a signal transmission line may be damaged by the earthquake, and the damage is assumed to be not recovered during the duty period. There is a potential for incomplete or misleading indications to the operator.
- Equipment Location and Accessibility—at high "g" levels, the earthquake may degrade the ability of the operator to get to certain locations, due to fallen structures blocking access to equipment or to the SCA.

As a result, the specific environment during a seismic event makes it difficult to directly use the actual operator performance data or simulator results, and there is no consensus on approach or methodology for quantifying the HEP. The approaches range from very simplistic, such as multiplying all HEPs obtained for internal events by a factor of 10, to the complex consideration of all the PSFs that are affected by a "g"-level-dependent influence factor, and by other weighting factors that take into account the particular PSF importance and its degradation during the seismic scenario (see Section 6).

The methodology for seismic PSA HRA modelling takes into account the influences of the intensity of the earthquake and of the elapsed time from the earthquake—separately for operator actions in the control room and for the actions on the field. The HEP for execution actions during seismic events are obtained by multiplying the HEPs calculated for the internal events PSA by the PSFs given in Table 7-4 and Table 7-5 for CANDU 6 and CANDU 9 systems, respectively. In these tables, the situations for which the operator is not credited are also represented. The following comments refer to the notations and assumptions that are employed:

a) The CANDU 9 MCR is designed to withstand and be functional for a DBE. However, fragility analysis may indicate that there is a margin "m" up to which the MCR maintains integrity and operator actions can be credited. The operator actions in the MCR are not credited for earthquakes that are more intense than m^1DBE (m^1 = margin factor form fragility analysis for SCA design earthquake), when the structural integrity of the MCR is not demonstrated.

b) The CANDU 6 MCR is not DBE-qualified, but the integrity of the MCR structure and the ability of the MCR to function are maintained up to a MCRDE (MCR Design Earthquake) value, which will be provided by fragility analysis. For earthquakes that are more intense than MCRDE, the plant operation is performed from the SCA, which is designed for DBE. A margin "m" provided by fragility analysis is considered for crediting operator actions in

the SCA. The operator actions in the SCA are not credited for earthquakes more intense than m^1DBE, when access to the SCA or the structural integrity of the SCA is not demonstrated.

c) The credit for operator actions in the field will be taken only when fragility analysis has indicated that there are sufficient margins for the unqualified structures. Operator actions in the field are not credited, if operator actions in the MCR or SCA are not credited.

7.8 Accident Sequence Quantification

7.8.1 Outline

ASQ is undertaken to estimate the frequency of the PDS following a seismic initiating event.

As mentioned in Section 7.6, event tree logic is developed to some final plant state within the containment boundary. The end-point or final state of an event tree sequence is a plant success state, where fuel cooling is maintained with no radiation release into containment, or a PDS, with a radiation release into containment and with the possible impairment of one or more containment systems. For each individual event tree sequence that ends in an undesirable plant condition or PDS (see Section 4.9), an assessment is required to determine the frequency.

The objective is to merge the various seismic steps (seismic hazard curve, component fragility curves and Boolean equations) for all the decision branch points that lead to the accident sequence under study (see Figure 7-1). ASQ yields an estimate of the frequency for the severe core damage by solving the seismic event tree, the fragilities of components, and the Boolean equations. Unlike the internal events PSA, individual cutsets are not obtained, except for random failures.

ASQ is performed on the master seismic event trees. The master seismic event trees consist of seismic failures of components and possibly random failure of components or systems. The random failure of systems are derived from the internal events PSA fault trees, as long as they have not failed from the seismic event. That is, the internal events PSA fault trees address only random failures not seismic failures. Therefore, equipment in these fault trees must be checked to ensure that they have not failed from the seismic event.

7.8.2 Methodology

The objective of ASQ is to provide an evaluation of the impact and contribution to the SCDF. The objective is met by solving the master seismic event tree in association with the seismic hazard curve, the fragilities of components and structures, and the Boolean equations.

ASQ will be performed using the EQESRA computer code developed by EQE International (Reference 7-19). Figure 7-6 shows the sequence of analysis and the EQE inputs and outputs that are used to perform the ASQ. The program EXPRESS of EQE (Reference 7-20) automatically converts Boolean algebra into the correct format for EQESRA. The three main inputs for EQESRA are

a) Seismic hazard curve—annual frequency of exceedance of specified peak ground accelerations.

b) Component or structure fragility—seismic fragilities of components or structures, in terms of A_m, the median peak ground acceleration, B_r, the logarithmic standard deviation due to randomness, and B_u, the logarithmic standard deviation due to uncertainty in the median. Non-seismic failures can be specified in terms of failure rate and error factor.

c) Boolean equation - Boolean equations for the seismic event tree, representing the combination of components.

The EQESRA Users' Manual provides further details on the application of the program (Reference 7-19). Tables 7-6, 7-7 and 7-8 show sample inputs for the seismic hazard curve, seismic fragilities of components, and Boolean equations, respectively.

Table 7-6 shows that one hazard curve is listed with 12 points on the curve. The first set of numerical numbers 0.05 to 1.0 corresponds to the accelerations for the hazard curve (g level). The second set of numbers, from 9.58×10^{-4} to 2.0×10^{-6}, corresponds to the probability values of the hazard curve.

Table 7-7 shows the fragilities for various components. Each component is followed by its A_m , B_u and B_r values. Inputs can also be entered in terms of probability, e.g., for operator actions or random component or system failures.

Table 7-8 shows the Boolean equations for the accident sequences in computer format, for input to the EQESRA code. The corresponding equations in standard Boolean equation format are shown below the echo printout.

Systems that have not failed from the seismic event can be credited. It is necessary to review these carefully to ensure that the equipment has not failed.

The Boolean equation is derived from the seismic event tree, using the ETA-II code (Reference 7-15). The components from the SSEL are assigned to their respective systems of the event tree. Fault tree analysis is performed, in order to evaluate random failures. Fault trees from the internal events PSA can be used and modified. The system fault tree logic is developed using the CAFTA fault tree editor (Reference 7-21).

There are three output files from EQESRA in ASCII:

a) Output. This file lists the input parameters and the results—the mean, median, 5%, 10%, 90%, 95% confidence bounds, the acceleration range versus the mean contribution, and the mean frequency. Filenames start with an "o" in the extension.

b) Plot - This file contains results in a Hewlett Packard Graphics Language (HPGL) format for plotting. Alternately, results can be obtained from the output file and can be plotted in a spreadsheet or a graphics program.

c) Log - This log file records any error messages.

When the entire seismic event tree is solved at one time, the result is the summed SCDF for the plant. To obtain individual accident sequence results, only the Boolean logic that corresponds to the selected accident sequence should be analysed. However, there may be a loss of accuracy, since not all combinations are being solved at the same time, i.e.: a summation of the individual sequences may not result in the same numerical number as that obtained by solving the entire seismic event tree at once.

Sensitivity analysis may be conducted, by selecting various parameters and by changing them. The selection depends on the initial result of the analysis.

7.8.3 Special Considerations for Reporting Results

The following information should be fully documented, as discussed in NUREG-1407 (Reference 7-2):

a) The hazard curve(s) used, and the associated spectral shape used in the analysis. As well, the upper bound cut-off to ground motion should be listed with any sensitivity analysis, in order to determine the effects on the overall results, and the ranking of seismic sequences.

b) A summary of seismic walk-down findings, procedures used, a list of team members and any subsequent actions taken.

c) All functional and systemic event trees. The manner by which non-seismic failures, human actions, dependencies, relay chatter, and seismic induced fire or flood are taken into account should be described.

d) A description of dominant functional and systemic sequences that lead to SCD, including any recovery actions.

e) Any seismically-induced containment failures, and other containment performance insights.

f) A table of component fragilities that are used for screening, and that are used in the final quantification.

g) A discussion of non-seismic failures and human actions that are significant contributors, or that have an impact on results.

7.9 References

7-1. USNRC (prepared by Brookhaven National Laboratory), 1985, Probabilistic Safety Analysis Procedures Guide, USNRC Report, NUREG/CR-2815, Revision 1.

7-2. J.T. Chen, N.C. Chokshi et al., 1991, Procedural and Submittal Guidance for Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, USNRC Report, NUREG-1407.

7-3. IAEA, 1993, Probabilistic Safety Assessment for Seismic Events, IAEA Report, IAEA-TECDOC-724, Vienna, Austria.

7-4. CNSC, 1980, Requirements for the Safety Analysis of CANDU Nuclear Power Plants. CNSC Consultative Document, C-6, Rev. 0.

7-5. Hickman J.W. et al., 1983, PRA Procedure Guide - A Guide to the Performance of Probabilistic Risk Assessment for Nuclear Power Plants, NUREG/CR-2300, prepared by American Nuclear Society and the Institute of Electrical and Electronics Engineers, US Nuclear Regulatory Commission.

7-6. CSA (Canadian Standards Association), 1992, General Requirements for Seismic Qualification of CANDU Nuclear Power Plants, CAN3-N289.1-M80, R92, Canadian Standards Association, Rexdale, ON.

7-7. CSA (Canadian Standards Association), 1992, Ground Motion Determination for Seismic Qualification of CANDU Nuclear Power Plants, CAN3-N289.2-M81, R92, Canadian Standards Association, Rexdale, ON.

7-8. CSA (Canadian Standards Association), 1992, Design Procedures for Seismic Qualification of CANDU Nuclear Power Plants, CAN3-N289.3-M81, R92, Canadian Standards Association, Rexdale, ON.

7-9. R.J. Budnitz, G. Apostolakis et al., 1997, Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts, USNRC Report, NUREG/CR-6372.

7-10. R.J. Budnitz, 1998, State of the Art Report on Current Status of Methodologies for Seismic PSA, Report publisher, NEA/CSNI/R(97)22, Paris, OECD.

7-11. B. Gutenberg and C.F. Richer, 1942, Earthquakes Magnitude, Intensity, Energy and Acceleration, Bulletin of the Seismological Society of America 32, 163-191.

7-12. D.L. Bernreuter et al., 1988, Seismic Hazard Characterization of 69 Nuclear Power Plant Sites East of the Rocky Mountains, USNRC Report, NUREG/CR-5250.

7-13. L.E. Cover et al., 1985. Handbook of Nuclear Power Plant Seismic Fragilities, USNRC Report, NUREG/CR 3558.

7-14. R.D. Campbell et al., 1988, Compilation of Fragility Information from Available Probabilistic Risk Assessments, LLNL Report, UCID-20571, Revision 1.

7-15. DS&S, 1993, *ETA-II Users' Manual for Version 2.1d*, Data Systems & Solutions, Los Altos, CA. Proprietary.

7-16. USNRC, 1986, Analysis of Core Damage Frequency: Surry, Unit 1 Internal Events, USNRC Report, NUREG/CR-4550.

7-17. A.D. Swain, 1987, Accident Sequence Evaluation Program: Human Reliability Analysis Procedure, USNRC Report, NUREG/CR-4772.

7-18. A.D. Swain and H.E. Guttmann, 1983, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, USNRC Report, NUREG/CR-1278.

7-19. EQE International, Inc., 1995, *EQESRA Users' Manual, Version 3.00*, EQE International, Inc., San Francisco, CA. Proprietary.

7-20. EQE International, Inc., 1995, *EXPRESS Users' Manual, Version 4.00*, EQE International, Inc., San Francisco, CA. Proprietary.

7-21. DS&S, 1993, *CAFTA Users' Manual for Version 2.3*, Data Systems & Solutions, Los Altos, CA. Proprietary.

Table 7-1
Sample of Information Required for Screening Evaluation

1. Equipment identification
2. Equipment/System description
3. Class of equipment
4. Building location
5. Room and/or row/column location
6. Capacity Spectrum
7. Demand Spectrum
8. Capacity/Demand Margin
9. Equipment General Characteristics
   included in earthquake experience class; attachment of external items; configuration similar to NEMA standards (electrical cabinets); natural frequency relative to predominant buildings frequencies; weight of equipment or cabinets (electrical); doors secured with latch or fastener (electrical cabinets); etc.
10. Anchorage
    appropriate equipment characteristics determined, size and location of anchors, adequacy of anchorage installation evaluated, anchorage capacity, etc.
11. Seismic interactions and proximity

Table 7-2
Sample of a Screening Verification Database

Equipment ID (1)	System/Equipment Description (2)	Equipment Class (3).	Bldg. (4)	Floor Elev. (5)	Room or Row/Col. (6)	Capacity Spectrum (7)	Demand Spectrum (8)	Capacity /Demand Margin (9)	Problems OK? (10)	Anchorage OK? (11)	Interactions and Proximity OK? (12)	Equipment OK? (13)	Notes (14)

Table 7-3
Equipment Information

Equipment ID	Equipment Description	Location	Normal Operating Position	Fail Safe Position	Class of Component	Power Supply and Control Power	PSA Basic Event
3461-PV41	EWS pneumatic valve for water from dousing tank to steam generators	SB	NC	FO	Pneumatic valve	48V DC to solenoid valve	3461PV41-$ VGCCFC

Table 7-4
Performance Shaping Factors and Credit of Operator Actions for Seismic Events at CANDU 6 Plants

Time Earthquake g	15 to 30 minutes	30 to 60 minutes	> 60 minutes
Operator Actions in the Control Room (MCR/SCA)			
0 to MCRDE	1.	1.	1.
MCRDE to DBE	No Credit	5.	1.
DBE to m^1DBE	No Credit	10.	5.
> m^1DBE	No Credit	No Credit	No Credit
Operator Actions in the Field			
0 to MCRDE	10.	5.	1.
MCRDE to DBE	No Credit	10.	5.
> DBE	No Credit	No Credit	No Credit

Notations:

MCRDE - Main Control Room Design Earthquake; to be provided by fragility analysis

DBE - Design Basis Earthquake

m^1 - Margin factor form fragility analysis for SCA design earthquake

Table 7-5
Performance Shaping Factors and Credit of Operator Actions for Seismic Events at CANDU 9 Plants

Time Earthquake g	15 to 30 minutes	30 to 60 minutes	> 60 minutes
Operator Actions in the Control Room (MCR)			
0 to SDE	1.	1.	1.
SDE to DBE	5.	1.	1.
DBE to mDBE	10.	5.	1.
> mDBE	No Credit	No Credit	No Credit
Operator Actions in the Field			
0 to SDE	10.	5.	1.
SDE to DBE	30.	10.	5.
> DBE	No Credit	No Credit	No Credit

Notations:

SDE - Site Design Earthquake

DBE - Design Basis Earthquake

m - Margin factor from fragility analysis for MCR design earthquake

Table 7-6
EQESRA Sample Hazard Curve Input

```
  1   12
       1
5.00E-02  1.40E-01  2.16E-01  2.90E-01  3.60E-01  4.30E-01  5.00E-01  5.80E-01
6.50E-01  7.20E-01  7.73E-01  1.00E-00
9.58E-04  3.58E-04  2.00E-04  1.29E-04  8.92E-05  6.49E-05  4.89E-05  3.77E-05
2.97E-05  2.37E-05  2.00E-05  2.00E-06
```

Table 7-7
EQESRA Sample Seismic Fragility Component Input

```
CL-IV
      0.30      0.25      0.31
D2O-PUR-INT
      0.55      0.24      0.31
DEAE-S-TK
      0.45      0.42      0.31
SDG-BATT
      0.65      0.30      0.30
FM-SLOCA
      0.75      0.30      0.30
FM-SCD
      1.00      0.30      0.30
SDS2
      0.70      0.30      0.30
SDS1
      1.00      0.21      0.35
EWS
      1.05      0.30      0.30
OP-INV-15M
   6.00E-2                              5
```

Values in the table represent A_m, β_r and β_u.

Table 7-8
EQESRA Sample Boolean Equation Input

```
   2    11   21   5    1
   1    11   81   7    2
   2    11   10  -1    3
   2    10  -31   3    1
   2    10  -10  -2    3
   2    10  -31   6    1



  E C H O   P R I N T O U T   O F   L O N G   E Q N

&CL-IV * (&D2O-PUR-INT * &FM-SLOCA) * &DEAE-S-TK *
(&SDS1 + &SDS2) * &FM-SCD
```

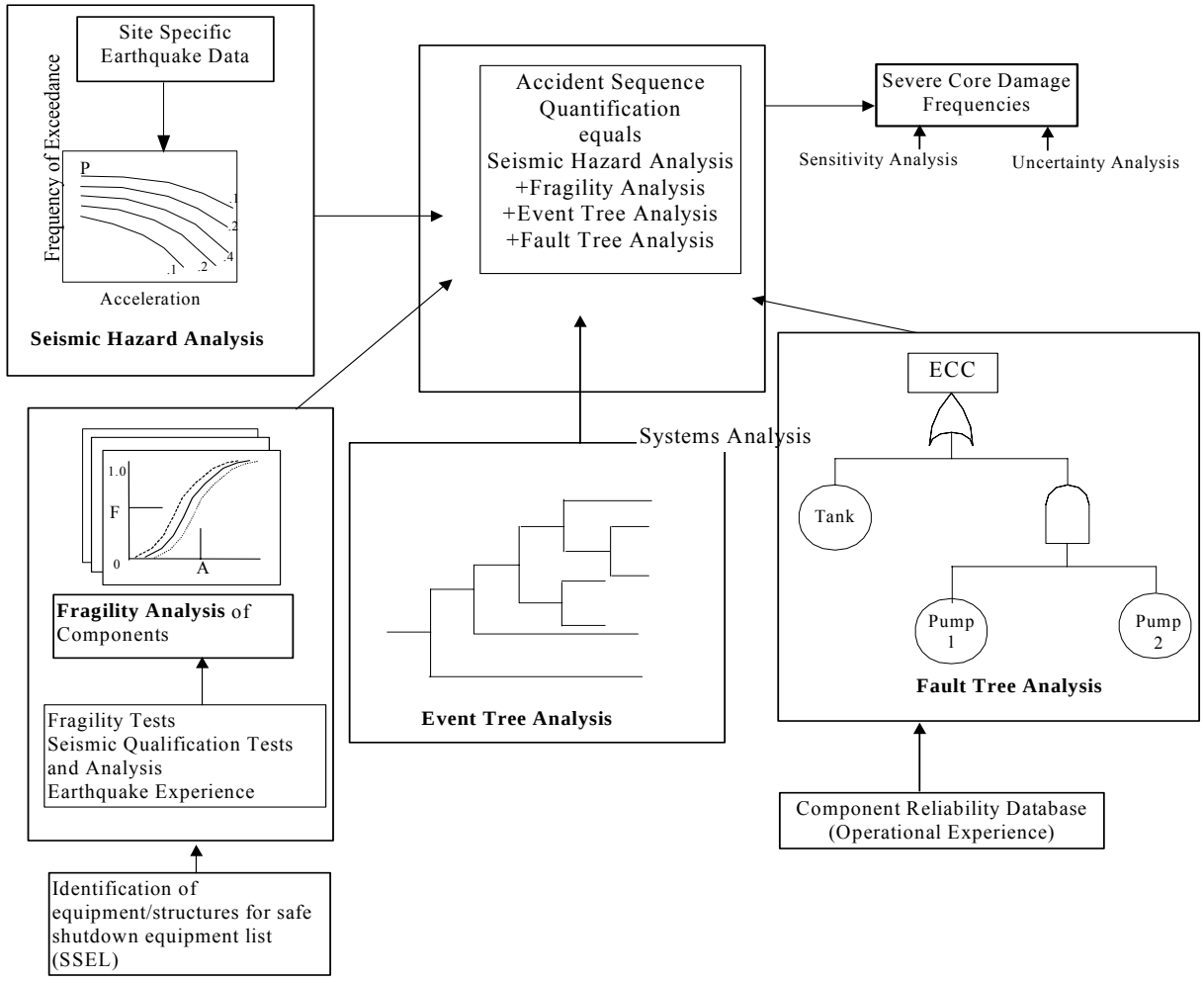


Figure 7-1 Steps of a Seismic PSA

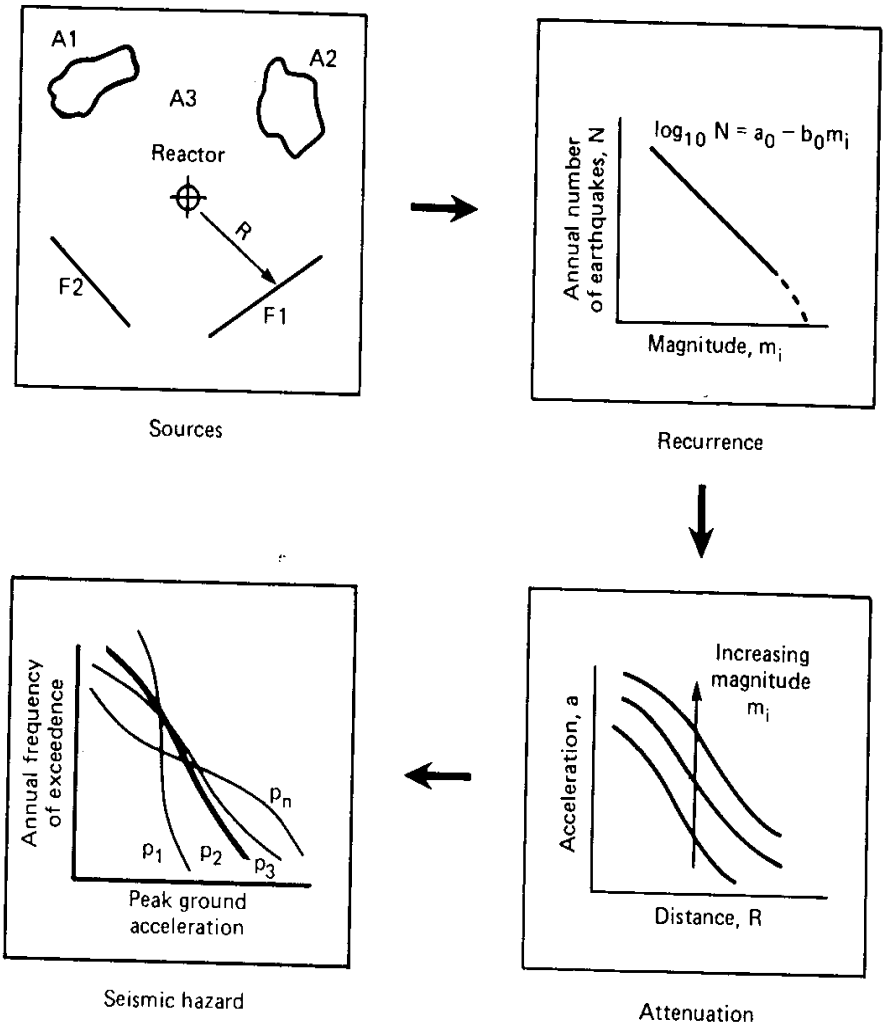


Figure 7-2 Main Steps Involved in Seismic Hazard Analysis (Reference 7-5)

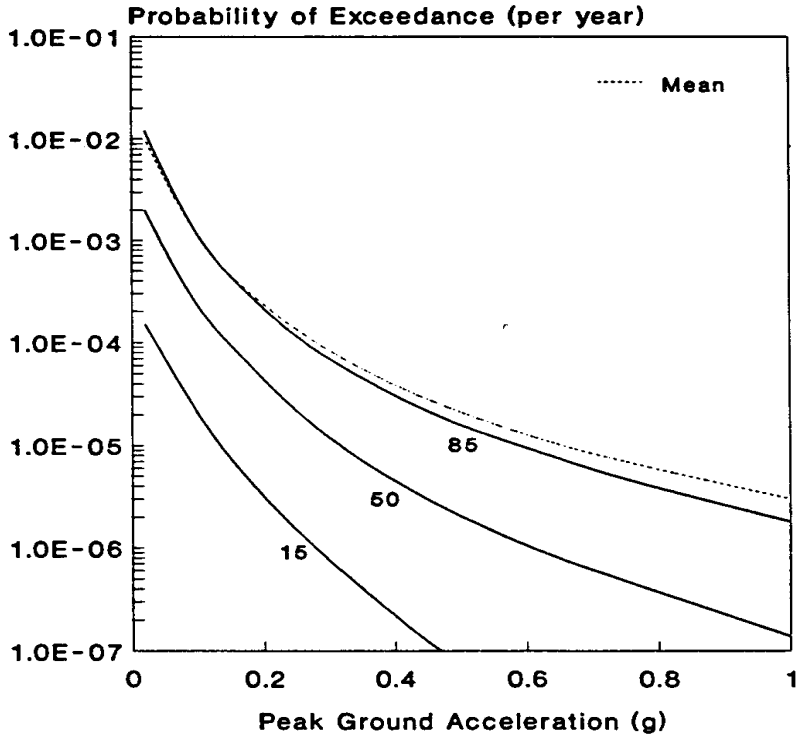
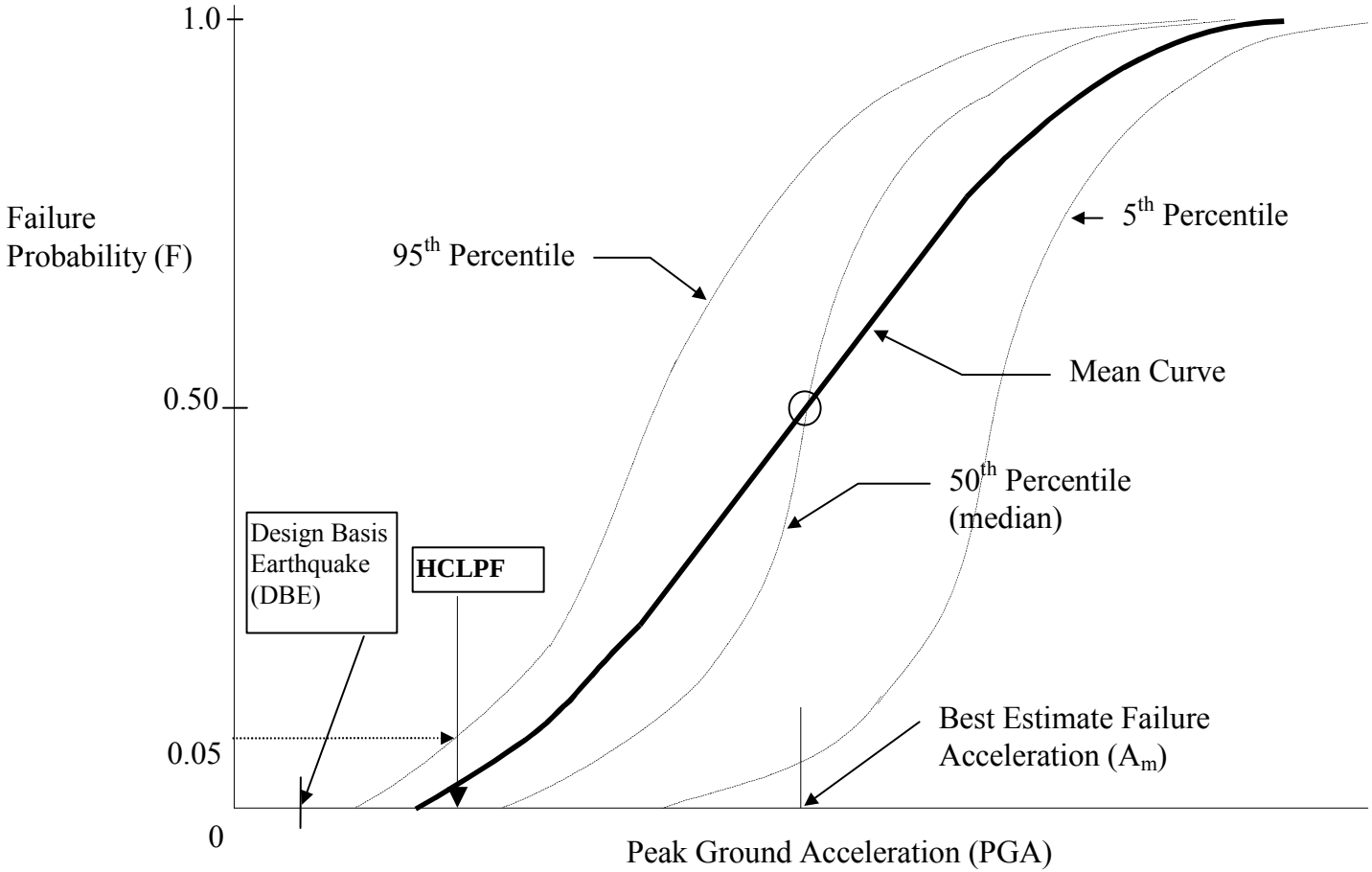
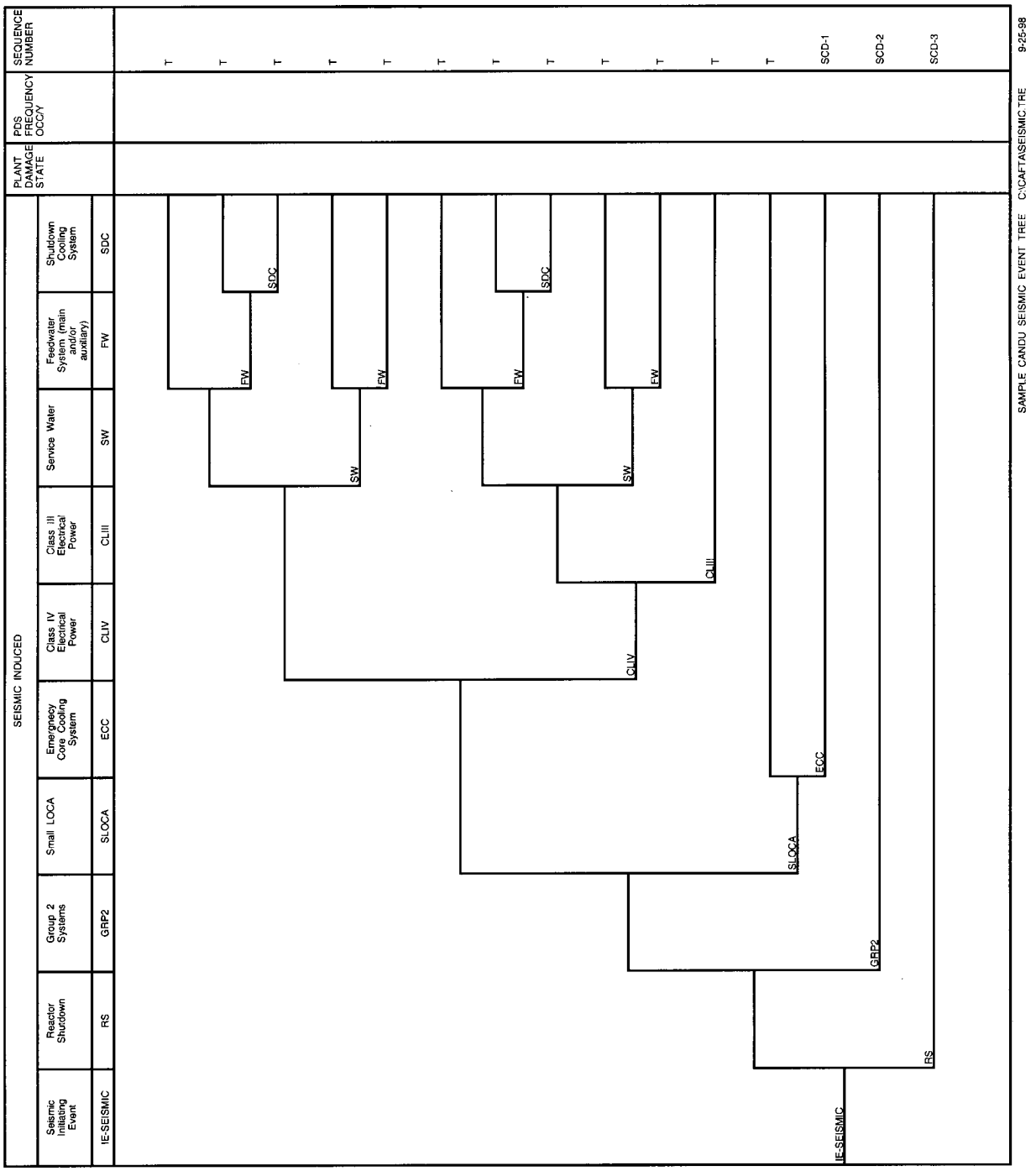


Figure 7-3 LLNL Hazard Curve for Surry NPP (Reference 7-12)



HCLPF is the abbreviation for a High Confidence (95%) of a Low Probability of Failure 5%)

Figure 7-4 Typical Fragility Curve



T - Transfer
SCD - Severe Core Damage

Figure 7-5 Sample Seismic Event Tree for CANDU 6 Plant

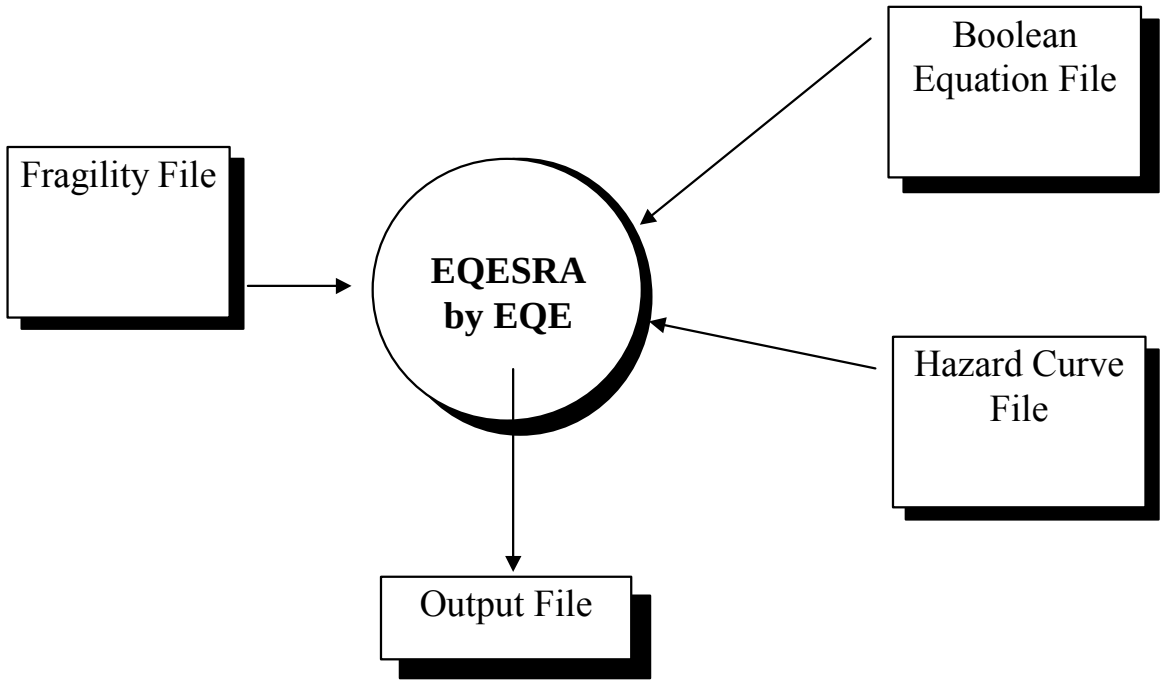


Figure 7-6 EQESRA Inputs/Outputs (Reference 7-19)

8. FIRE EVENTS PSA

8.1 Introduction

Fire events are generally common cause events, and may cause the failure of multiple systems or components that would otherwise be considered to be independent of each other. Therefore, their frequency of occurrence may be independent of the failure frequency of the systems that perform safety-related functions that maintain the plant in a safe state.

The progression of a fire event from its initiation to severe core damage is very complex, with a very high dependence on the types of components and their physical proximity to each other. The PSA of fire events starts with the identification of the basic cause of the fire event, and then examines historical or physical data to establish the sources and frequency of the fire event initiation. The physical layout and characteristics of the plant are studied to determine the impact of the IE on the systems that maintain the plant in a safe state. This identifies the systems that could be lost initially as a result of the event and as the event progresses, and the probability with which they may be lost. This information is used in conjunction with modified internal event PSA system models, in order to quantify the plant damage and SCDFs.

The methodology is applicable to reactor on-power operation, as well as during the shutdown state, by suitably modifying the event or fault trees for the internal events. Any relevant flooding that occurs as a result of fire suppression is addressed as part of the flood PSA. The failure of components that contain significant combustibles due to a seismic event is addressed as part of the fire PSA.

The methodology selected for the PSA of fire events follows internationally acceptable practices, as outlined by the International Atomic Energy Agency in Safety Series No. 50-P-4, (Reference 8-1).

8.1.1 Scope

The following is a list of the major aspects that are associated with an internal fire PSA:

a) The determination of generic fire IE frequencies, based on historical data.

b) The identification of plant characteristics that are related to the initiation and propagation of fires. Included in these characteristics are:

- fire zone data (fire geometry and area, fire barrier ratings, detection, suppression),
- fire hazards, and
- the location of safety related and PSA credited systems and equipment.

c) A plant walk-down, to confirm the information that is extracted from design documents, and to identify additional information that could affect the fire scenario models, fire propagation or fire impact on equipment.

d) A fire vulnerability analysis, which establishes potential fire scenarios and quantifies their impact on the plant, in terms of plant damage or SCDFs.

The following sections describe the methodology in general terms, and identify the basic assumptions that are incorporated in the methodology and its application to a plant assessment.

8.2 Fire Initiating Event Frequency Analysis

8.2.1 Fire Events

8.2.1.1 Definition of Fire Events

For CANDU plants, fire events are defined as events that are characterized by the presence of flame, burning, or smouldering, and that have the potential for growth and propagation to the point of causing a reactor trip and/or damaging safety related or PSA credited equipment. In the progression of fires, heating, arcing or sparks may result in potential fires, but in this methodology, the initiation of a fire is considered to be the point where a flame occurs.

In selecting events for the database, the potential impact of the event on plant safety during reactor operation, and the relevance of an event to a CANDU plant are considered. Generally, events with smoke and no fire are not included, as well as those that involve arcing, sparking, explosions and other short bursts of energy that fail to result in ignition. For the fire PSA, explosion events that involve mechanical effects but no fire are not considered.

The frequency of fire IEs is derived from operating experience in NPPs in North America. To establish fire IE frequencies for PSA purposes, the specific plant operating history (on-power, shutdown) needs to be known, and the fire events must have been consistently reported throughout that period. This information is available for US and Canadian plants, but not necessarily for off-shore plants. For off-shore plants, the International Atomic Energy Agency (IAEA) and Nuclear Energy Agency (NEA) events databases are not considered to contain all fire related events; for example, the events reported from Canada to IAEA/NEA would indicate that only major fire events are reported, not all fire IEs. Therefore, the IAEA and NEA events databases are not used as sources of fire event frequency information.

The CANDU Fire Events Database consists of fire events that have occurred at CANDU plants in Canada, as well as the fire events that have occurred in Light Water Reactors and that are relevant to CANDU plants. US LWR events are considered to be applicable to CANDU systems, if they involve similar types of equipment in systems that provide similar functions to those in CANDU plants. The data for the US LWRs are available from the Pickard, Lowe and Garrick (PLG)[1] database (Reference 8-9). The data for CANDU fire events were selected from the CANDU Owners Group (COG) database Reference 8-2.

[1] PLG is now part of ABSG Consulting Group

These two databases may include uncertainties and limitations that arise from differences in reporting criteria used by various plants, and from the completeness and accuracy of descriptions of the events. However, it is known that all the events reported to the Canadian regulator are included in the COG database, and that the information existing in the PLG database is currently used for US LWR plant Individual Plant Examination of External Events (IPEEE) studies that meet the requirements of USNRC. Also, the level of reporting appears to be similar in these two databases. Therefore, the use of the data from the COG and PLG databases is appropriate for this work.

It is also recognized that there is a large variability among the different plants in areas such as specific design, layout, maintenance procedures and practices, safety culture and fire protection features. However, the general level of technical standards for component manufacturing, safety regulations and requirements, personnel training, plant maintenance practice, etc., are not vastly different over the nuclear industry in North America. Moreover, fire events are evaluated individually at the component/equipment level, so that the differences of reactor types (CANDU vs. LWR) are not relevant when screening LWR fire events for applicability to the CANDU design. Therefore, it is considered appropriate to use LWR data for the CANDU fire events database.

8.2.1.2 Screening Criteria

Since LWR plants may contain systems that do not exist in CANDU plants, the events recorded in LWR plants are screened for applicability to CANDU plants. Thus, fire events that are associated with systems that are unique to LWR plants are not considered, as they are not applicable to CANDU plants. For example, fires in the following LWR systems are screened out:

- Turbine driven main feed water pumps in boiling and pressurized water reactors (BWRs and PWRs). However, “pump only” related fires are retained (e.g., those caused by lube oil or overheated bearings).
- Turbine driven auxiliary or emergency feed water pumps in PWRs. Although some CANDU NPP have these depending on design.
- Turbine driven high-pressure coolant injection (HPCI) systems and turbine driven reactor core isolation cooling (RCIC) systems in BWRs.
- Standby gas treatment systems in BWRs.

Events recorded in the US LWR and COG databases are also evaluated according to the definition of fire events. Events that involve components and systems that are not modelled in the PSA and are not located in the general areas that contain safety related or PSA credited equipment are screened out. As a result, the following categories of events are screened out:

- Fire code violations, false fire alarms and events relating to fire fighting systems (fire water protection systems) that do not involve a fire.

- Events with smoke and no fires (smoking bearings, belts), unless a detailed examination reveals that open flaming or a fire would likely occur if the event is allowed to progress.
- Arcing, sparking, shorts and explosions that are short bursts of heat energy, but that fail to result in ignition. Crankcase explosions in diesel generator sets are screened out, since they are contained and cannot propagate.
- Fires outside the fenced area, such as forest or grass fires, even if they result in the failure of transmission lines.
- Fires in the switchyard.
- Fires in administrative buildings, main entrance area, guardhouse, temporary buildings, or trailers.

An evaluation is also made about whether or not the fire can occur during reactor power operation and/or at shutdown. This is necessary, because there may be significant differences between the plant on power and the plant at shutdown, in areas such as: plant configuration, system operation, maintenance activities, and personnel access to various areas in the plant. As a result, the frequency of fire events for the plant with the reactor on power may differ from the case when the reactor is shutdown. Thus, the following three combinations are possible:

Category	Event Can Occur During		Applicability
	Shutdown	Power	
1	N	Y	Reactor on power only
2	Y	Y	Anytime
3	Y	N	Reactor shutdown only

The events in the first two categories are applicable to the fire PSA with the reactor on power. For this case, all the events in the first category, and only a fraction of the events in the second category, which represent the events that occur during power operation, are considered.

8.2.1.3 Categories of Fire Events Sources

The process to identify potential fire sources in the plant requires a systematic analysis of the recorded fire events. Thus, each fire event is characterized by the equipment, cause, and/or location of occurrence. The fire events are classified in a number of categories, which denote one or several of the following:

- component types (e.g., cables, motors, pumps, etc.),
- areas in the plant with common characteristics for several plants (e.g., MCR), and
- transient fires (e.g., fires caused by welding and cutting, transient combustible materials, human errors).

Table 8-1 contains the list of categories of fire event sources that contribute to fire risk for CANDU plants and also contains information on the components assigned to these categories.

The list of categories of fire event sources and the definition of these categories are tailored according to specific assumptions, as follows:

- Category 4 relates to all fires that occur in the MCR, regardless the cause and/or equipment involved (transient fires, fires in control panels, cabinets, etc.). This approach avoids the need to comprehensively list and sum the individual fire initiation frequencies for all fire sources for this area.
- Category 5 and Category 8 refer to Digital Control Computers (DCCs) and D_2O Recovery Dryers, respectively, both of which are specific to CANDU plants and are not present in US LWR plants. Therefore, the calculation of fire frequency considers only the CANDU data and CANDU plant operating history.
- Category 12 (pumps) refers to fire events that are related to the pumps only; fires that occur in pump motors are assigned to Category 14 (motors).
- Fires in junction boxes are included in Category 16 (power and control cables).
- Category 20 (turbine-generator) includes all the fire events that are related to the T/G group (i.e., T/G exciter, oil, hydrogen fires).
- Category 23 (transient fires) contains fires that are related to causes such as human error and transient fuel location.

In some cases, the classification of an event in one or another category may not be obvious, due to limited knowledge of the individual plant or a limited or incomplete description of the event. This requires that the events be analysed and judged on a case-by-case basis in a conservative manner.

8.2.1.4 CANDU Fire Events Database

The events that are retained following the screening process constitute the CANDU Fire Events Database for event frequency calculations. The CANDU Fire Events Database is developed in Microsoft (MS) Access format. The records in the MS Access database are easily retrieved and sorted, and are based on a given set of criteria, which allows the user to construct customized queries and to obtain customized reports.

The database contains the relevant remaining events that passed the screening process from the US LWR plants, as well as relevant remaining events from the COG database for the CANDU stations. For each event that is included in the database, the following information that is relevant for the assessment is presented:

- event ID in the original database (US LWR and COG, respectively),
- plant and unit where the event occurred,
- reactor type,
- date of event,
- operation mode of the reactor when the fire event occurred,

- event description,
- location of fire in the plant,
- fire event source category ID, and
- reactor state when a similar fire event can occur (on power, shutdown, anytime).

It is noted that the screened-out events are preserved in the original records from the COG and US LWR databases. Should one choose to screen these databases for other purposes, the screened-out events are still available.

8.2.2 Calculation of Fire Initiating Events Frequencies

The determination of the generic fire frequency that is due to existing potential fire sources in a CANDU plant involves the statistical processing of the information on fire events that is included in the CANDU Fire Events Database. The methodology for quantifying the frequency of fire events is based on the two-stage Bayesian method. This method combines the plant-specific data with the generic experience data to generate the plant-specific initiating events frequencies. Basically this method consists of establishing first a generic probability for each initiating event and then updating it with the plant-specific experience data. The calculations are performed using the first stage of the two stage bayesian update option.

The two stage bayesian update option is applied separately for each category of fire event source. The process involves the following steps:

- Create the Industry Data Set for each category of fire event sources.
- Create the prior distribution (first stage updating).
- Update the prior distribution with plant-specific data (second stage updating).

The calculation of fire events frequencies applies to a generic CANDU plant design; therefore, plant-specific data for the third step (second stage updating) is not available—this step is used for the analysis of a plant that has been operating for some years. The generic fire frequency for a category of fire event source is the prior distribution created in the first stage updating. This represents the frequency (in events per year) with which a fire (caused by sources included in the particular category) occurs in the plant during a period of one year of operation, with the reactor on power. These generic frequencies will be used during the fire vulnerability analysis, with weighting factors that are based on the number of sources that exist in each fire area, relative to the total number of sources that exist in the plant.

8.2.2.1 Industry Data Sets

An Industry Data Set constitutes a package of information used as input by RISKMAN Release 6.0 (Reference 8-3).

The frequency for each category of fire event source is calculated separately, such that a separate Industry Data Set is prepared for each of the categories of fire event source. The processing of

this data results in the prior distribution of the two-stage update. The mean of this distribution is retained as the point estimate frequency of occurrence of a fire caused by that category of fire event source.

The frequency of each fire event is calculated by on number of events (occurring during power and shutdown) during the time for plant operation (years) multiplied with the plant availability factor during this time.

8.3 Identification of Plant Characteristics

8.3.1 Plant Characteristics Database

The data related to plant systems (including safety related and PSA credited data), equipment, cables, and their locations are collected in the plant characteristics database, created in MS Access. The plant characteristics database is a relational database, and is made up of several data tables that encompass the fire zone data report, the location of mitigating systems for fire events report, and the fire hazard assessment report. Figure 8-1 shows the overall database relationship chart. The data tables are joined together or are related to each other. The result is that the data can be retrieved from all the fields of related data tables. Thus, customized reports, forms and queries can be easily created from these data tables.

The data tables are structured in such a way that they provide for the easy collection, organization, grouping, storage and retrieval of data. The tables are kept at reasonable sizes, so that the data can be easily managed and the required information can be efficiently used. The ability to utilize data table relationships is one of the elements of MS Access that makes it easy to record, update, and manage the data. These relationships greatly reduce the overall file size of the database. This is achieved by reducing the requirement of re-entering groups of data that would be repeated for several individual entries, and that would have similar characteristics. Each data table in this database is used to assemble data that are unique to the "key" or main focus of the table, which is described by its title. Any reference to data in one table will be passed along to other tables by way of a relationship link, allowing the pertinent information in the other table that matches the search criteria in that first table to be displayed.

Customized reports, which contain the required or relevant data, are created from various related and relevant data tables in the database.

8.3.2 Fire Zone Data

The fire characteristics of a CANDU plant are evaluated in terms of "fire zones", which are small sections of a plant that can be treated as a unit for evaluation purposes. A fire zone usually corresponds to a single room, but can consist of two or more rooms that are spatially linked. A fire zone is not necessarily bounded by physical barriers; spatial separation may be used between fire zones. A "fire area" is one or more fire zones that are contained within a defined set of fire barriers.

8.3.2.1 Data Tables

The data tables that are directly involved with the fire zone data are

- rooms
- zone exposure
- fire detection/suppression (D/S) layout
- fire D/S devices
- fire load
- zones

8.3.2.1.1 Rooms

This data table consists of the following fields (note that this description also applies to Sections 8.3.3 and 8.3.4, but is only described here):

a) Unit—this field is used primarily for database operator's reference, this field describes the unit from which the information was derived.

b) Room—this field is for the room number, written in an alpha-numerical form. It not only identifies the number of the room, but also the building and floor, as well. The first entry of the field is a letter, which identifies the building of the plant. The second is a digit, which identifies the floor. The remaining digits are sequential numbers, and are allocated to the rooms as they are encountered. For example, room 'S205' has the following meaning: 'S' stands for service building, '2' for the second floor and '05' for the fifth room.

   The designation for various buildings of the plant are as follows:

   R = Reactor Building,

   S = Service Building, and

   T = Turbine Building.

c) Description—this field is used to describe the room function and/or contents.

d) Elevation—this field records the elevation of the room, as it pertains to the original drawings.

e) Fire zone—the fire zone is an enclosure that conveniently defines a specific location in the plant for fire PSA. The zone may be defined by non-physical boundaries, such as "logical divisions" or "equipment grouping"; thus, it may not necessarily restrict fire and smoke from spreading.

   A number is designated to each individual fire zone. The numbering system is similar to that of the room. The first letter is the building designation, and the following three digits are sequential numbers that are allocated to the fire zones as they are encountered.

f) Fire area—the fire area is an area or a portion of a building or plant that is separated from other areas, and is bounded by fire barriers that have at least a 2-hour rating or equivalent.

Openings in the barriers are equipped with doors, enclosures, seals, etc, that have fire ratings that are at least equivalent to the rating of the barrier.

The numbering system is again similar to that of the fire zone. The first letter designates the building, and the subsequent digit or digits designate the area number.

8.3.2.1.2 Zone Exposure

This data table contains the following fields:

a) ID - this field is a unique record identifier (for MS Access record management purposes only).

b) Zone - the number that is designated to the fire zones is recorded in this field. The numbering system is the same as that of the fire zone in the above "Rooms" data table.

c) Zones exposed - this field is an outside fire zone or zones to which the fire zone in question is exposed.

d) Pathway - this field describes the path of least resistance to fire propagation towards the adjacent fire zone.

e) Barrier rating - the rating for the physical barrier of the fire zone is given here, in hours.

8.3.2.1.3 Fire D/S Layout

a) Fire DS ID - this ID is a link to the unique record identifier that represents the fire detector/suppresser.

b) Zone - the number that is designated to the fire zone is recorded here. The numbering system is the same as that of the fire zone in the above "Rooms" data table.

c) Room - the room number is placed here as an optional field. It not only identifies the number of the room, but also the building and floor as well. The numbering system is the same as the one used for the room in the above "Rooms" data table.

d) Quantity - This field shows how many fire D/S devices of the described type are in this fire zone.

8.3.2.1.4 Fire D/S Devices

a) ID - this field is a unique record identifier (for MS Access record management purposes only).

b) Device - the description of the fire detector or suppresser is recorded here.

c) Hazard category - a category is given to represent the device's potential for initiating a hazard, as well as its susceptibility to a given hazard.

d) Detector? - is this device a fire detector? A check box is provided—a check mark in the box means "yes".

e) Suppresser? - is this device a fire suppresser? A check box is provided—a check mark in the box means "yes".

f) Auto? - does this device work automatically? A check mark in the box means "yes". In the case of a detector, this is obviously yes, but it is not obvious in the case of a suppresser.

8.3.2.1.5 Fire Load

The fire load data table consists of the following fields:

a) ID - this field is a unique record identifier (for MS Access record management purposes only).

b) Zone - the number designated to the fire zone is recorded here. The numbering system is the same as that of the fire zone in the above "Rooms" data table.

c) Heat load - this field represents the amount of heat (in Joules) that is generated by the total amount of combustibles in the fire zone.

d) Area - the area of the fire zone (in square metres) is given here.

e) Fire load - this field is calculated by dividing the total heat load by the zone area, and is given in J/m^2.

8.3.2.1.6 Zones

a) Zone - the number that is designated to the fire zone is recorded here. The numbering system is the same as that of the fire zone in the above "Rooms" data table.

b) Description - this field provides an overall description of the rooms that make up the fire zone, and typically describes the type(s) of equipment and/or facilities that are available in the rooms.

8.3.3 Fire Hazards

There are different types of components in a NPP that can initiate a fire. These are identified for each location, and are related to other relevant data used in the detailed fire hazard analysis or in the PSA for the plant.

8.3.3.1 Data Tables

For the purposes defined in the scope of this document, the data tables that are directly involved with the fire hazards are

- rooms
- zones
- combustibles
- ignition sources

- fire load

8.3.3.1.1 Rooms

This data table is described in Section 8.3.2.1.1.

8.3.3.1.2 Zones

This data table is described in Section 8.3.2.1.6.

8.3.3.1.3 Combustibles

The combustibles data table contains the following fields:

a) ID - this field is a unique record identifier (for MS Access record management purposes only).

b) Zone - the number designated to the fire zone is recorded here. The numbering system is the same as that of the fire zone in the above "Rooms" data table.

c) Combustible - this field contains a description of the combustible item that is present in the fire zone.

d) Quantity - this field contains the amount of the combustible in the fire zone.

8.3.3.1.4 Ignition Sources

The ignition sources data table contains the following fields:

a) ID - this field is a unique record identifier (for MS Access record management purposes only).

b) Zone - the number designated to the fire zone is recorded here. The numbering system is the same as that of the fire zone in the above "Rooms" data table.

c) Ignition source - this field contains a description of the ignition source that is present in the fire zone.

d) Quantity - this field contains the amount of the specific ignition sources in the fire zone.

8.3.3.1.5 Fire Load

This data table is described in Section 8.3.2.1.5.

8.3.4 Location of Mitigating Systems

This section describes the data compilation for the location of mitigating systems for fire events. These data are part of the Plant characteristics database used to record information about the plant characteristics that are related to the initiation and propagation of fires. The data are

collected from information obtained from the plant arrangement drawings, equipment layout drawings, fire protection zones drawings, related reports listed in the reference section, and from data collected from the plant walk-down.

8.3.4.1 Data Tables

For the purposes defined in the scope of this document, only the data tables that are directly involved with the location of mitigating systems for fire events are discussed below. These data tables are

- rooms
- zones
- system
- equipment categories
- equipment
- cables
- cable layout
- cable/system

8.3.4.1.1 Rooms

This data table is described in Section 8.3.2.1.1.

8.3.4.1.2 Fire Zones

This data table is described in Section 8.3.2.1.6.

8.3.4.1.3 System

The system data table contains the following fields:

a) SI - this field is the subject index number that is assigned to the plant system.

b) System name - this field gives the name of the plant system.

c) Function - a description of the primary function/purpose of the plant system is given here.

d) Safety related system? Is this system a safety related system? A check box is provided - a check mark at the box means “yes”.

e) PSA credited? Is this system a PSA credited system? A check box is provided - a check mark at the box means “yes”.

8.3.4.1.4 Equipment Categories

The equipment categories data table contains the following fields:

a) ID - this field is a unique record identifier (for MS Access record management purposes only).

b) Category - a category name is given here to identify different pieces of equipment that are part of a category (that is the source of the same fire hazards) and that are susceptible to the same fire hazards.

8.3.4.1.5 Equipment

The equipment data table contains the following fields:

a) SI - the subject index identifier for the piece of equipment is given here.

b) Tag - the tag number of the piece of equipment is given here. The alphabetical prefix identifies the equipment type, and the numeric suffix is a unique identification number that is assigned in series.

c) System - this field is the plant system's SI to which the piece of equipment is assigned.

d) Description - a brief description of the piece of equipment is given here.

e) Hazard category - a category name is given here to identify different pieces of equipment that are part of a category (that is the source of the same fire hazards) and that are susceptible to the same fire hazards.

f) Room - the room number is placed here as an optional field. It not only identifies the number of the room, but also the building and floor, as well. The numbering system is the same as the one used for the room in the above "Rooms" data table.

g) Structure or device - this field identifies whether or not the piece of equipment can be identified as a structure (e.g., does the item terminate a cable? In other words, is an entire cable dedicated to this piece of equipment?) or a device (e.g., an item that has a wire attached to it).

h) Elevation - this field identifies the elevation of the piece of equipment.

i) Notes - any special notes about the item can be entered here.

8.3.4.1.6 Cables

The cables data table contains the following fields:

a) Cable ID - a unique alphanumeric identifier that is given to a cable is entered here.

b) Hazard category - a category name is given here to identify different types of cable that are part of a category (that is the source of the same fire hazards) and that are susceptible to the same fire hazards.

c) Notes - any special notes about the cable can be entered here.

8.3.4.1.7 Cable Layout

The cable layout data table contains the following fields:

a) Cable ID - a unique alphanumeric identifier that is given to a cable is entered here.

b) Room - the room number is placed here as an optional field. It not only identifies the number of the room, but also the building and floor, as well. The numbering system is the same as the one used for the room in the above "Rooms" data table.

c) Length - the length of the cable, from where it enters the room to where it leaves the room or terminates, is entered here.

d) Raceway ID - this number identifies one section of the path that the cable makes.

e) Tray or conduit - This field specifies if the raceway ID identifies a cable tray ora conduit.

f) Notes - any special notes about the layout can be entered here

8.3.4.1.8 Cable/System

The cable/system data table provides a quick entry method of linking a specific cable to the plant system(s) that it supports. The data table contains the following fields.

a) Cable ID - a unique alphanumeric identifier that is given to a cable is entered here.

b) System - this field is the plant system's SI to which the piece of equipment is assigned.

8.4 Plant Walk-Down for Fire Events

The progression of a fire, from a fire IE to a fully developed fire, is very dependent on the specific physical location of the source of the fire, and on any combustible materials within the fire area. It is generally not possible to include all relevant details in design documentation, and changes may have occurred during the construction of the plant that are not fully reflected in the design documentation. Therefore, it is necessary to confirm the information included in design documents, and to obtain additional relevant information regarding an existing plant through one or more plant visits, normally termed "plant walk-downs".

8.4.1 Objectives of Plant Walk-Down

The objectives for the plant walk-down are

a) To confirm the accuracy of the plant information assembled from design documentation.

b) To obtain additional information that is not available from design documentation, such as details about field installed equipment, maintenance practices, operating procedures, transient combustibles, storage areas, etc.

c) To identify potential interactions between systems and equipment that would affect the progression of a fire.

8.4.2 Collection of Plant Walk-Down Information

The walk-down information will be collected by a multi-disciplinary team that has the following personnel, as a minimum:

a) a fire PSA team leader,

b) a fire PSA analyst, and

c) a seismic PSA analyst (to identify potential seismically induced fires).

The following information will be collected, using a system of notes and checklists:

a) Confirmation of the fire sources and combustibles that are present in the area.

b) Confirmation of the type and location of fire detection and suppression equipment in the area.

c) Confirmation that the fire barriers and any other passive fire protection features are present, and are as described in design documentation. Their specific construction and geometry are also noted.

d) Confirmation that the identified safety related equipment is present in the area. Any other items of a safety related or PSA credited nature are also noted.

e) Observation of the relative amounts of the fire initiation sources in all areas, for the purposes of apportioning the fire initiation frequencies for the different categories.

f) Observation of the relative locations of fire sources, safety related equipment, and PSA credited equipment.

g) Observation of floor gratings and openings in the fire zone or fire area boundaries that could affect fire propagation.

h) Observation of pathways of transient combustibles in the plant, types, and amounts (e.g., lube oil).

The information collected during the walk-down will be entered into the fire hazards database for use during the fire hazards analysis and the probabilistic safety assessments.

8.5 Fire Vulnerability Analysis

The fire vulnerability analysis provides an understanding of the impact on plant safety of internal fire IEs, and quantifies the risk in terms of SCDF. To calculate the severe core damage frequencies, the fire vulnerability analysis uses information regarding generic frequencies for categories of fire event sources, plant layout (fire areas, fire zones, fire barriers), location and interaction of components and equipment in the plant, as well as the modified internal event PSA plant models.

The fire vulnerability analysis consists of the following steps:

a) Determination of fire IE frequencies in each fire area.

b) Definition of fire scenarios in each fire area.

c) Qualitative screening of fire areas that require no further consideration.

d) Quantitative screening of fire areas, and calculation of plant damage and severe core damage frequency using PSA system models.

e) Refinement of the fire scenarios for areas that have a significant impact on the SCDF, in order to obtain a more realistic evaluation of the fire scenario, along with the recalculation of plant damage and SCDF using PSA system models.

The qualitative and quantitative screening of the fire scenarios is performed to reduce the number of fire scenarios for which a detailed fire hazard analysis is performed. The screening analyses assume a worst case impact of fire in the areas to which it is applied. Scenarios that are not screened out are retained for detailed fire hazard analysis, which provides a more accurate determination of the impact of the fire on plant safety and SCDF. The PSA plant modelling for both screening analysis and detailed analysis is based on the internal events PSA model, and is suitably modified to reflect systems and components that are damaged by the fire.

8.5.1 Calculation of Fire Initiating Events Frequencies in Fire Zones

The overall fire hazard in a fire zone is given by contributions from the individual fire sources that exist in the particular location. At the plant level, fire events are classified in categories of fire hazard sources (see Section 8.2.1.3), for which fire frequencies that are expressed in events/plant/year are available from historical records of nuclear plant operation (Reference 8-4). These plant frequencies are then adjusted with weighting (apportioning) factors, to account for the number of items of each category of fire source in the room.

The composite fire frequency for the fire zone i, λ_i, is given by the following expression (Reference 8-4):

$$\lambda_i = \Sigma\, w_{i,j}\, \lambda_j + \lambda_h\, w_h$$

where $w_{i,j}$ = weighting (apportionment) factor for source-based categories of fire event source j (Categories 1-3, 5-22 and 26) in fire zone i.

λ_j = source-based fire occurrence frequency for the source-based category of fire event source j. The product $w_{i,j}\, \lambda_j$ represents the contribution of the source category j to the fire frequency in the zone i.

w_h = weighting factor for transient fires (categories 23, 24 and 25).

λ_h = source-based fire occurrence frequency for transient fires (categories 23, 24 and 25).

For the source-based categories of fire event sources (Categories 1-3, 5-22 and 26), the weighting factors $w_{i,j}$ are calculated as

$$w_{i,j} = N_{i,j} / NT_j$$

where $N_{i,j}$ = number of component items of Category j in the room i.

NT_j = total number of component items of Category j in the fire areas in the plant.

Similarly, the weighting factors for power and control cables (Category 16) are calculated by dividing the weight of cable insulation in the area by the total weight of cable insulation in the fire areas in the plant (References 8-5, 8-6, 8-7). The values for $N_{i,j}$, NT_j and the amount of cable insulation are determined from the information on the components and equipment existing in the fire areas (see Section 5).

The weighting factor for transient fires (Categories 23, 24 and 25) w_h depends on the number and nature of maintenance operations and the amount of human activity in a room. In a simplified approach (Reference 8-4) it is assumed that the contributions of various fire zones is uniform throughout the installation, such that

$$w_h = 1 / NL$$

where NL is the total number of fire zones in the installation where maintenance is performed. It is recommended to calculate w_h as the ratio between the activity level in the fire zone i and the total amount of activities in the plant. The estimation of these activities, however, requires intimate knowledge of the maintenance procedures and working practices in the plant. Therefore, in this report, the first method for calculating w_h is recommended.

The fire frequency in the MCR is the frequency of the category of fire event source 4. This is calculated based on the recorded fire events that occur in the MCR in the plants considered (see Section 8.2), regardless of their cause (equipment failure, human error, etc.).

8.5.2 Fire Scenarios

A fire initiated in a location can develop and jeopardize the availability of fire susceptible components and equipment in that area, and potentially in adjacent areas. The way that a fire is initiated in an area and progresses to its final conclusion is called the fire scenario. The identification of the safety related (PSA credited) components that could be damaged by the fire is essential in the evaluation of the fire scenario. Qualitatively, the fire evolution and consequence depends on a number of parameters, such as

- the number and location of fire event sources,
- the geometry of the enclosure and the amount of fuel (combustibles) available,
- the availability of manual and/or automatic fire suppression systems,
- the propagation pathways,
- the fire barrier rating and location, and
- the number and location of safety related systems and components.

Quantitatively, the frequency of a fire scenario is given by the frequency of fire initiation, the suppression failure probability, and, for propagation scenarios, the fire barrier failure probability

of the particular fire scenario. The fire scenario frequency is the frequency used in the quantification of the accident sequence in the fire PSA.

Since not all fire scenarios are expected to have a significant impact on plant safety, a screening analysis is first performed. This analysis is based on conservative assumptions that are designed to reduce the number of fire scenarios retained for a detailed fire progression analysis.

8.5.3 Fire Scenarios for Screening Analysis

Fires in a number of areas of the plant may have little or no impact on the plant damage or SCDFs; therefore, they can be eliminated from further consideration by a simple screening analysis. Fire scenarios that are developed for screening analysis are characterized by the following assumptions:

a) The frequency of fire initiation is the composite frequency for all categories of fire event sources that are present in the room. All the combustible material that exists in the room where the fire was initiated is assumed to burn. For scenarios where propagation to other rooms is possible, all the combustible material in the rooms to where the fire propagates is also assumed to burn.

b) When fire propagation is considered, the fire barriers are assumed to be degraded to 75% of the nominal rating, and this value is compared with the fire load. When the load is lower than the barrier rating, a generic barrier failure probability based on Reference 8-8 is used.

c) The automatic fire suppression system is assumed to operate, with the appropriate failure probability, only to prevent fire propagation (i.e.: not for limiting fire damage within the area). For automatic fire suppression, a generic failure probability based on Reference 8-8 is used.

d) Manual fire suppression is not credited.

e) All equipment that is susceptible to fire damage and that exists in the room where the fire was initiated, is damaged. All components in the rooms to which the fire propagates are also considered to be damaged. Damaged components are assumed to fail to perform their safety function, unless the function is demonstrated to be fail-safe.

8.5.3.1 Qualitative Screening

Qualitative screening is used to eliminate areas that have an obviously low impact on plant safety from further analysis, without the use of PSA plant models. The main criteria for qualitative screening of fire areas and/or scenarios are as follows:

- A fire in the area does not cause a demand for a plant trip or shutdown.
- The fire area does not have safety related equipment.
- The fire does not propagate to other areas that have safety related equipment.
- The fire area does not have a credible fire source or a significant amount of combustibles.

Additional considerations for qualitative screening analysis are

- that the plant trip frequency due to fire is relatively lower than that due to other causes, and
- that the PSA equipment unavailability due to fire is relatively lower than that due to other causes.

8.5.3.2 Quantitative Screening

The quantitative screening of fire areas and/or scenarios is primarily based on the fire initiation frequency and an analysis of the impact on plant safety, using information from the PSA plant models. A fire location and/or scenario is screened out for the following situations:

- The unavailability of the equipment/system in a location due to fire is substantially lower than the unavailability of the same equipment/system due to all other causes.
- The frequency of the reactor trip due to fire-induced equipment failures is substantially lower than the reactor trip frequency from all other causes.
- The SCDF of an accident sequence from a fire in the location under consideration is substantially lower than the individual accident sequences for the corresponding internal events (e.g., three orders of magnitude, or less than 10^{-8} events/yr).

The quantitative screening analysis using the Level I internal events plant model is performed as follows:

- Calculate the IE frequency for all areas that are not screened out in qualitative screening.
- Assume that all equipment and cables are damaged by fire in fire area/scenario.
- Determine the fire impact on mitigating system models, and determine which models cannot be credited.
- Determine the internal event PSA event trees that can be used, and modify them accordingly.
- Quantify the accident sequence for event tree.
- Keep track of the aggregate severe core damage frequencies of the screened scenarios, and add them later to the total SCDF.

8.5.4 Fire Scenarios for Detailed Analysis

The following constitute the steps in a detailed analysis (see the calculation example in Appendix C):

- Identify and define the fire scenarios to be analysed.
- Perform PSA analysis for the selected fire scenarios, taking into account various refinements, such as
  - more realistic modelling of fire growth and propagation,
  - credit for fire detection and suppression, and

- credit for operator recovery action, if applicable.

- Calculate SCDFs for fire scenarios that require detailed analysis.
- Calculate the summed SCDF for fire, by adding the fire risk contribution for all scenarios.

Fire scenarios that are developed for detailed analysis are characterized by the following assumptions:

a) The frequency of fire initiation is given by the frequency of the particular fire event source that exists in the location analyzed. Only the fuel in the original fire source burns. However, if it is demonstrated that other combustibles and/or fire sources (components, equipment, etc.) consequently catch fire, then the fuel that characterises these sources is also considered.

b) When fire propagation is considered (propagation scenarios), the nominal rating of the fire barriers is considered, and this value is compared with the fire load. When the load is lower than the barrier rating, a generic barrier failure probability based on Reference 8-8 is used.

c) Automatic and manual fire suppression is credited, with the appropriate failure probability, for both suppressing the fire and for preventing fire propagation. For automatic fire suppression, a generic failure probability based on Reference 8-8 is used. Manual fire suppression is credited with a failure probability that is dependent on the elapsed time, and on whether or not fire detectors are present in the location.

d) In establishing the damage that is caused to a target from a particular fire source, the cable insulation and damage thresholds are currently not well known. For the fire PSA, a cable ignition temperature of 773 K (932°F) is assumed, along with a damage temperature of 623 K (662°F).

8.5.4.1 Fire Progression Modelling and Fire Consequences Evaluation

The fire modelling analysis provides information on the spatial transient evolution of temperature in the fire zone. This is important for calculating the heat loads on fire barriers, for evaluating the component degradation with respect to distance from the fire, temperature and duration of exposure, and for determining fire propagation times.

The COMPBRN IIIe computer code (Reference 8-10) will be used to calculate fire propagation and to determine the time interval between fire initiation and damage to critical equipment. COMPBRN IIIe was developed at UCLA. Alternative North American fire modelling codes that can be used are FAST, CFAST and FPETOOL. These codes are not as widely accepted, validated or used for nuclear plant applications as COMPBRN, even though they may model a fire just as well. European fire analysis codes (Reference 8-11) that have been developed for nuclear plant applications include the French codes FLAMME-S (IPSN) and MAGIC (EdF).

The code calculates the time to damage critical equipment, once a fire has started. This failure time is used in conjunction with information on fire suppression, in order to estimate the probability that a given fire will cause equipment failure, leading to SCD if the fire is not suppressed.

COMPBRN IIIe follows a quasi-static approach to simulating the process of fire during the pre-flashover period in an enclosure. COMPBRN uses a zone model, essentially dividing the fire environment into three zones: flame/plume, cold gas layer and hot gas layer. Fire and heat transfer correlations are employed to predict the thermal environment as a function of time. The thermal response of various targets in the fire scenario are modelled to predict the amount of time that is required for a fire to damage or ignite critical equipment. The critical equipment is generally taken to be a cable tray carrying cables that are necessary for the safe shutdown of the plant, although other critical components, such as pumps can be modelled.

It should be pointed out that there are limitations to the COMPBRN IIIe code. The most significant limitations are listed below:

- The code does not perform well when the fire source is too close to the ceiling, within the hot gas layer, or when a target is directly on top of a flame.
- Doorways in COMPBRN are defined as openings that extend from the floor to a certain height, and that allow natural movement for the hot gases and air that are flowing in and out.
- Ventilation ports can only be located at the ceiling or on the floor. The user specifies the fraction of flow entering or leaving each port.
- All rooms are modelled as being rectangular in shape. Round or shaped rooms must be approximated as rectangles having equivalent wall surface areas. All objects must be oriented parallel to one axis.
- Vertical or inclined burning objects cannot be modelled with accuracy in the current version of the code. The interference effect of several layers of objects (e.g., cable trays separated by small vertical distances) can be modelled.
- The code does not accurately model oxygen depletion, thus leading to a conservative result compared with other fire analysis codes (Reference 8-12).

8.5.4.2 PSA Modelling of Plant Response During Fire Events

For each fire scenario addressed in the detailed fire hazard analysis, the response of the plant is analyzed using PSA methodology. This involves

- the identification of the PSA IE,
- the development of event trees and the description of accident sequences, and
- the development of fault trees for the analysis of system availability.

For fire PSA analysis, plant modelling for fire events is based on the internal events PSA model. However, the application of this model requires the following supplementary activities:

a) Identification of the PSA IE and of the corresponding internal events event tree (e.g., general transient, loss of feed water, consequential LOCA, etc.). This step forms the transition from the fire analysis to PSA analysis for each fire scenario, using the PSA model. Based on judgements for the components and equipment that are damaged by fire, the cause of the reactor trip is established, thus defining the IE and the particular event tree to be used. For

example, if the reactor is tripped automatically, then the trip signal will define the type of event tree that is applicable; if the reactor continues to operate but the operator decides to actuate manual shutdown, then the general transient event tree would be used. Quantitatively, the frequency of the PSA IE is given by the frequency of the fire scenario.

b) Development of the internal events event trees. For the PSA IE that are determined in the previous step, the event trees that are built for internal events PSA are reviewed for applicability to the particular fire scenario. This review will consider the following aspects:

   1) Safety and mitigation systems

      Fire events may affect the availability of safety related and mitigating systems, such that systems that are normally considered as being available in internal events event/fault trees cannot be credited during fire events. In these situations, the event/fault trees must be modified accordingly, by setting the failure probabilities (unavailabilities) to 1. Although some components may be damaged by fire, their fail-safe characteristic may still be credited.

   2) Post-accident operator execution actions

      During fire events, access for the operating staff to certain locations for the purpose of mitigating actions may be impaired. If the location in the field is not accessible, then that operator action is not credited. If the operator needs more time to access the location (e.g., via alternate routes), then this supplementary time needs to be considered in establishing the time available for the action. Post-accident operator actions will be quantified according to the methodology established in the human reliability and recovery analysis methodology, (see Section 6). In particular, an additional factor will be applied to the HEP that is due to the increased stress experienced during actions that are required in areas affected by heat or smoke.

c) Development of the fault trees for the systems that are involved in the event trees. This review may be required, since individual components and equipment in the safety related systems, as well as services (e.g., electrical power supply) to these systems, may not be available due to the fire. Although the fault tree structure will not be changed, for quantification purposes, the unavailability of these components will be set to 1.

8.6 Human Reliability Analysis for Fire Events

It is assumed that fire events in various areas in the plant do not influence operator performance in the MCR. Therefore, HEPs for such fire events are considered to be the same as for the internal events PSA. For the case of fire in the MCR, a factor of 5 is applied to the HEP for post-accident execution actions, compared to the HEP for the internal events PSA, in order to account for the increased stress (References 8-13 and 8-14). The Fire Risk Scoping Study (Reference 8-15) can also be used as another source for fire PSA.

8.7 References

8-1. IAEA, 1992, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants, Level 1, IAEA Report, Safety Series No. 50-P-4.

8-2. COG, 1998, COG OPEX Database. Proprietary.

8-3. ABSG Consulting Inc., 1998, RISKMAN® PRA Workstation Software User Manual I: Data Analysis, Release 6.0, 1999 PLG Inc., 300 Commerce Drive, Suite 200 Irvine, CA 92602, Proprietary.

8-4. R. Bertrand, F. Bonneval, G. Barrachin and F. Bonino, 1997, Estimation of Fire Frequency from PWR Operating Experience, Presented at the IAEA Symposium on Upgrading the Fire Safety of Operating Nuclear Power Plants, Vienna, Austria, 1997 November 17–21.

8-5. Baltimore Gas and Electric, 1997, Calvert Cliffs Nuclear Power Plant - Individual Plant Examination for External Events (IPEEE) Summary Report.

8-6. Braidwood Nuclear Power Plant - Individual Plant Examination for External Events (IPEEE) Submittal Report", June 1997.

8-7. Byron Nuclear Power Plant - Individual Plant Examination for External Events (IPEEE) Submittal Report, December 1996.

8-8. USNRC, 1990, Procedure for the External Event Core Damage Frequency Analyses for NUREG-1150, USNRC Report, NUREG/CR-4840.

8-9. ABSG Consulting Inc., Fire Database 1998, PLG Proprietary Database.

8-10. V. Ho, S. Chien and G. Apostolakis, 1990, COMPBRN IIIe, An Interactive Computer Code for Fire Risk Analysis, UCLA Report (prepared for EPRI), UCLA-ENG-9016.

8-11. M. Dey, M. Z. Azarm, R. Travis, G. Martinez-Guridi and R. Levine, 1998, Technical Review of Risk-Informed, Performance-Based Methods for Nuclear Power Plant Fire Protection Analyses, USNRC Draft Report for Comment, NUREG-1521.

8-12. M. K. Dey, 1997, Technical Methods for a Risk-Informed, Performance-Based Fire Protection Program at Nuclear Power Plants. Presented at the IAEA Symposium on Upgrading the Fire Safety of Operating Nuclear Power Plants, Vienna, Austria, 1997 November 17-21.

8-13. Commonwealth Edison Company, 1996, Zion NGS Units 1 and 2, IPEEE for Severe Accident Vulnerabilities Submittal Report.

8-14. Commonwealth Edison Company, 1996, Byron NGS Units 1 and 2, IPEEE for Severe Accident Vulnerabilities Submittal Report.

8-15. J.A Lambright et al., 1988, Fire Risk Scoping Study: Current Perception of Un-addressed Fire Risk Issues, NUREG/CR-5088.

Table 8-1
Categories of Fire Event Sources

Category ID	Category Name	Components
1	Battery	
2	Battery charger	
3	Inverters	
4	MCR	Panels and cabinets in the control room
5	DCC computer	
6	Diesel generator sets	
7	HVAC equipment	Heaters, fans, chillers, filters, air compressors
8	Dryers	D_2O recovery dryers
9	Hydrogen fires	Hydrogen vessels (excluding turbine-generator hydrogen fires)
10	Logic and protection cabinets	Relays, fuses, panels, switches
11	HTS pumps	
12	Pumps	Motor pumps and diesel driven pumps
13	Motor control center	
14	Motors	MOV, strainer motor, starter motors
15	Motor generator sets	
16	Power and control cables	Cables, junction boxes
17	Low voltage switchgear	Low voltage equipment (480 V or less)
18	High voltage switchgear	High voltage equipment (above 480 V)
19	Buses	
20	Turbine-generator	T/G exciter, oil, hydrogen
21	Main unit transformer	
22	Transformers	Transformers of all voltages
23	Transient fires	Human error, transient fuel location
24	Cable fires caused by welding and cutting	
25	Transient fires caused by welding and cutting	
26	Standby generators	Gas turbines

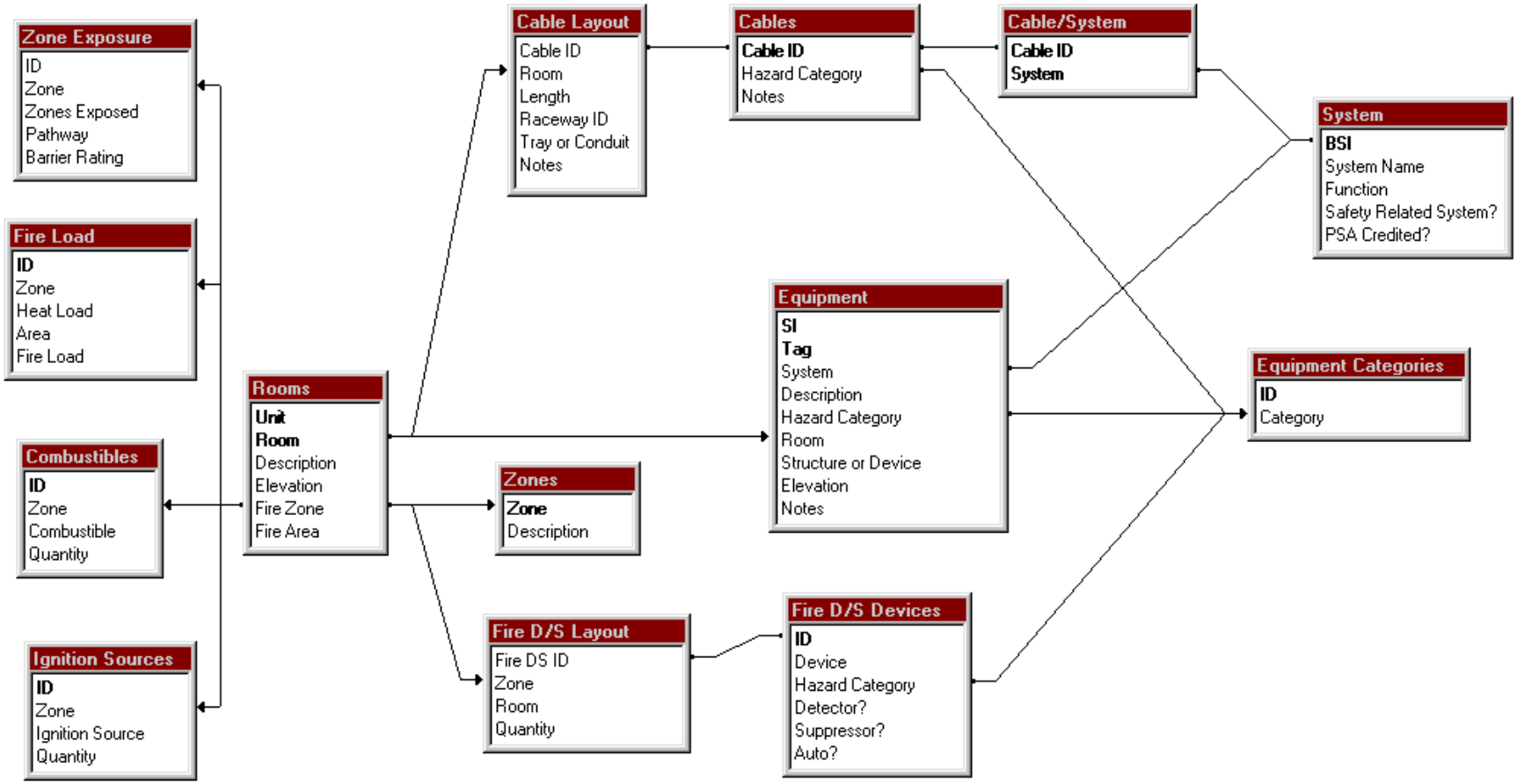


Figure 8-1 Overall Database Relationship Chart

9. FLOOD EVENTS PSA

9.1 Introduction

This analysis describes the methodology for the PSA for flood events for a CANDU NPP. The analysis describes the method for assessing the consequences of reactor accidents involving internal floods only.

The methodology was defined as part of the GPSA program, and will be applied to current and future CANDU plant designs. This section provides the specific methodology for flood events, and is used in conjunction with the generic methodology for the Level I PSA described in Section 3. The results of the Level I PSA, including internal fire, flood and seismic events, are provided as input to the Level II PSA.

9.1.1 Scope

Only internal flooding events are analysed to estimate their potential to cause SCD, and to identify any plant design or operational vulnerabilities that can cause internal flooding.

Internal floods may result from component failures, or from the incorrect operation of equipment or systems within the plants. Internal floods may occur, for example, as a result of a rupture of a pipe or a vessel, or be caused by leakage from a component that is incorrectly assembled or is left in a disassembled state following maintenance.

An internal flood may potentially lead to SCD by first causing the failure of the systems that maintain the heat sinks, and then by contributing to failures of engineered systems that are designed to mitigate such events. In evaluating the frequency of flood-induced accident sequences, the probability of coincident random equipment failures is considered, in addition to the initial damage caused by the flood itself.

This methodology will not consider external flood causes, such as bad weather, river flooding, upstream dam failure, wind waves, precipitation, snow melt, etc. These events are plant–specific; therefore, they have to be assessed on a case-by-case basis.

The basic components of the internal flood PSA methodology are

a) the determination of flood areas based on the design flood calculation, general arrangement drawings, information about flood barriers or steam barriers, or other available design information.
b) the identification of flood area characteristics, in terms of flooding sources and the location of safety related and PSA credited systems and equipment.
c) qualitative screening analysis, which involves the screening out of flood areas from further analysis, based on qualitative evaluation. The qualitative evaluation focuses mainly on the location of safety-related systems and equipment.

d) quantitative screening analysis, which involves the screening out of flood areas from further evaluation, based on the conservative evaluation of SCDF.

e) the refining of results for some scenarios, by performing analysis to eliminate conservatisms.

f) detailed analysis of the potentially significant flooding sources and scenarios that are identified in the screening analysis. The flooding frequency is calculated based on plant-specific data. Local operator recovery actions are also credited.

A plant walk-down for the flooding analysis is necessary to ensure that the analysts have made correct assumptions and calculations.

9.2 General Approach for Flooding Event Analysis

Internal flooding requires consideration as a significant risk contributor, because of its potential for causing CCFs and/or human actions, which may result in an initiation of an accident and the loss of one or more accident mitigating systems.

The major concern in the flood PSA is equipment failure due to submergence or sprayed water. Flood events are of particular concern, because they are "common cause" initiators. In other words, the event itself can cause failures of redundant components and systems, and thereby reduce the number of mitigating systems that are available to bring the plant to a safe and stable state.

The detailed analysis of the flooding events is plant-specific, since their likelihood of occurrence, progression and subsequent impact on plant systems is highly dependent upon factors such as plant layout, pipe work arrangements and drainage, as well as prevailing flood protection features and programs.

The basic approach is a screening analysis that first establishes key safety equipment locations and potential flood sources. Flood scenarios are identified based on the source of flooding, the extent of propagations to adjacent locations, and the equipment impact.

The following considerations will provide practical limits to the analysis:

a) Only one flood event is assumed to occur at a time (e.g., only pipe break or tank rupture).

b) The internal events analysis treatments of LOCAs inside containment adequately address flood sources and their effects.

c) Temporary hose/piping connections can be excluded from the analysis as flood sources, since they are used relatively infrequently.

d) Seismic induced floods are analysed in the seismic PSA.

e) Floods are treated as IEs and not as events that are subsequent to another initiator.

f) Spurious activation of sprinkler systems is considered.

g) Areas surrounded by walls are assumed to be properly sealed, so that flood propagation via walls will not be considered, although the effect of drains must be taken into account.

h) The critical height of the electrical cabinets is generally assumed to be 15.2 cm (6 inches). The critical height of the pumps is generally assumed to be 1.0 m, if specific information is not available. The critical height of motor operated valves (MOVs) is assumed to be the same as that of the pumps.

i) The vacancy factor of the area occupied by the mechanical equipment and by the electrical cabinets is generally assumed to be 0.6 and 0.8 respectively, based on US LWR experience. For the CANDU 6 turbine building the vacancy factor is in the order of 0.9 based on a general system layout. These values should be assessed on a case-by-case basis.

j) A closed loop system is not generally considered to be a flooding source. A closed system contains a limited amount of inventory, and the pumps circulate the flow. Usually, breaks in a closed loop would trip the pumps, which would stop the flood.

k) Only random failures will be considered in the flooding analysis. Flooding due to human errors (caused by leakage from a component that is incorrectly assembled or is left in a disassembled state following maintenance) is not analysed. It is assumed that the operator can take immediate corrective action to mitigate the accident.

The major tasks of the flood analysis are as follows:

1. Qualitative screening analysis
2. Quantitative screening analysis
3. Detailed analysis
4. Sensitivity analysis

The above steps are presented below in more detail.

9.2.1 Qualitative Screening Analysis

9.2.1.1 Assembly of Plant Information

The plant information that is required for the analysis includes the location of major flood sources, major piping, major equipment for safe shutdown, any potential flood barriers for preventing propagation, and the location of electrical and instrumental equipment that may be affected by water.

The analyst can become familiar with the plant, by reviewing key plant design information such as arrangement drawings, equipment locations, PSA models and system drawings.

This task also involves extensive plant visits, which are normally termed plant walk-downs.

The objectives of the plant walk-down are:

- to collect general information about the configuration of the plant, flooding sources, spray sources, equipment that would be affected by these sources, protection devices for flood propagation, etc.; and
- to confirm with plant personnel that the documentation being used is in fact the best available information, and to receive clarification concerning any questions that might have arisen in the review of the documentation.

A multi-disciplinary team will collect the walk-down information.

As a result of a plant walk-down, the analyst can gather actual information to determine if flood doors that are indicated in the design documents are installed. As well, the analyst can determine whether or not the doors are kept closed as intended, the drains are installed and are not plugged, and there are additional potential flooding sources that are not identifiable from plant drawings alone.

Information including flooding and spray sources, pipe sizes drainage features, equipment heights above floor level and general room/area information can be recorded on the walk-down checklist.

A sample data recording sheet is shown in Table 9-1.

9.2.1.2 Identification of Flood Areas

This step involves the definition of various areas of the plant as being independent, with respect to internal flooding. An area is termed independent if flooding outside the area cannot intrude into the area, without the failure of an enclosing flood barrier (walls, doors, etc.).

The physical layout of the plant buildings, together with the location and size of potential flood sources are considered in determining the independence of an area.

It is useful to initially consider the plant as consisting of a few large independent areas, such as the service building, the turbine building, the reactor building, the emergency water supply pump station, the high pressure – emergency core cooling accumulator building, etc.

These areas are easily identified as being independent with respect to internal flooding, because they are distinct structures that have only a few interconnecting pathways (personnel or equipment access ways, shared drainage systems, etc.).

One other factor that may contribute to the independence of an area is physical separation, i.e.: walls. It is not recommended to consider the collapse of walls or leakage through construction joints. The leakage rates are minor, and they can be easily accommodated by installed drainage systems.

In CANDU plants, expansive plant structures such as a turbine building can be divided into smaller areas within a larger independent area. These smaller areas are separated by walls from the other areas, and contain components that pertain to a particular mitigating system.

9.2.1.3 Identification of Flooding Sources

In this step, the major flooding sources, together with their water capacity are identified. The major water sources at the plant include the major tanks and the systems that supply, circulate and process water.

For CANDU plants, the major water sources are

- the raw service water system,
- the condenser circulating water system,
- the emergency water supply system,
- the dousing water system,
- the emergency core cooling system, and
- the fire water system.

9.2.1.4 Identification of Equipment in Each Flooding Area

To determine the impact of flooding originating in a certain area of the plant, it is necessary to know what flood-susceptible equipment is located in the area.

To know the impact of flooding in each flooding area, two steps are necessary:

- identification of the systems used for accident mitigation, and
- identification of the safety system components, based on active components that are likely to change state during an accident (pumps, valves), components that induce initiating events upon failures, and sensors or transmitters that are essential for plant monitoring.

9.2.1.5 Qualitative Screening of the Flood Areas

The intention of the qualitative screening is to focus analysis efforts on the critical areas of the plant, by examining worst-case scenarios only.

In this step, flood areas are screened out if they do not contain any susceptible equipment for safe shutdown, or if they do not contain any equipment that, if damaged, would lead to an IE.

Also, flooding sources that do not have enough capacity to damage the equipment that is required for safe shutdown or to lead to an IE are screened out in this stage of the analysis.

9.2.2 Quantitative Screening Analysis

9.2.2.1 Evaluation of Flood Frequencies

For the purpose of the screening analysis only, the flood initiation frequencies for each flood area are determined on the basis of CANDU operating experience data.

The data will be derived from the COG SER flood data and other documents that list CANDU plants operating experience. Raw data should be first collected based on word search criteria (including "flood") and then reviewed for relevance.

The plant-specific flood frequencies from piping data will be used in the detailed analysis.

9.2.2.2 Identification of Flood-Induced Initiating Events

For each flood area in which a flood can occur or propagate to, it is necessary to examine the flood susceptible equipment, in order to determine which of the IEs defined in the internal events assessment may occur as a result of flood damage. The major concern in the flood PSA is equipment failure due to submergence or sprayed water.

If the flooding causes more than one type of IE, then the most severe IE will be considered.

9.2.2.3 Identification of Flood Propagation Paths

In this step, the propagation modes that are considered include operational errors (i.e.: watertight doors or hatchways left open) and mechanical failures (i.e.: failure of valves in the drain lines).

The probability of propagation to adjacent areas is evaluated based on judgement. The following values are used in the screening analysis (P_{bf} represents the flood protection barrier failure probability):

- Failure of water-tight doorway $P_{bf} = 0.1$ or 10^{-3}
- Failure of non-water-tight doorway $P_{bf} = 1.0$ or 0.1
- Drain line check valve failure to seat $P_{bf} = 1.3 \times 10^{-4}$
- Failure of sealed cable penetration $P_{bf} = 10^{-2}$

It is not recommended to consider the collapse of walls or leakage through construction joints (the leakage rates are minor, and can be accommodated by installed drainage systems).

9.2.2.4 Initial Quantification of Flooding-Induced Accident Sequences Frequencies

The initial quantification of flooding sequences can be performed using an event tree based code package (i.e.: ETA). To evaluate the flooding-induced accident sequence frequencies, the

initiating flood frequencies for each flood area, flood sequence scenarios, flood event trees and mitigating system fault trees are required.

By modifying the relevant fault tree/event tree models, a CCDP for each scenario (or group of scenarios that have similar impacts) is calculated, such that both flood-induced and random failures are taken into consideration.

One example is the transmitter rooms, which may be damaged by a rupture in the fire water line in the reactor building. When the transmitter rooms are flooded, Group 1 control is lost due to a lack of control information. Therefore, one of the event trees for the reactor building flooding accident will be developed to express "loss of Group 1 control".

The CCDP is calculated by summing all the severe core damage frequencies in a particular flooding accident event tree (a value of 1.00 is assigned to the IE frequency).

9.2.2.5 Preliminary List of Potentially Significant Flooding Areas and Scenarios

The severe core damage frequency is calculated by multiplying the flood frequency by the CCDP. If the result is less than 10^{-6} events/year (the SCDF is negligible, compared with the internal IE caused by the flood), then the flood scenario may be screened from further analysis.

Because of the use of a conservative flooding frequency and no operator action to cease the flooding, this screening criterion is judged to be appropriate.

It is expected that in the detailed analysis, the order of magnitude of these specific sequences will be further reduced, due to more realistic assumptions and due to the fact that they will not be dominant contributors to the SCDF that is due to a flooding event.

9.2.2.6 Refining the Initial Screening Model

When the initial model is set up, various conservative assumptions are made, in order to minimize the plant data collection effort and to simplify the screening evaluation process.

The initial screening results are then reviewed to determine the particular assumptions that are dominant. Then, if practicable, additional data collection and analysis are performed, in order to refine the screening model and assumptions and thereby reduce the number of flooding sources that have to be subjected to detailed analysis.

By performing further analysis to eliminate conservatisms, the results may be refined for some scenarios. Each scenario can be divided into sub-scenarios that are based on the individual sources that are present in the flood location, if their impact is expected to be greatly different. Then, the flood scenario frequency is reduced by empirical factors (<1) that lower the frequency used in the screening analysis. Credit can be taken for the following factors:

- Location factor—the likelihood of the leakage location being sufficiently close to impact "target" safety-related equipment.
- Direction factor—the likelihood of spray being directed at target equipment.

- Propagation factor—if applicable, this is the likelihood of a propagation path (e.g., door) being open (see Section 9.2.2.3).
- Severity factor—the probability that the leakage rate is great enough to cause the submergence that is assumed in the screening analysis.
- Operator factor—the likelihood of successful operator recovery action to isolate or otherwise mitigate the leakage, before the target equipment is affected. This factor will be based on the time that is available to the operator, which can be calculated from the leak rate, room dimensions and equipment occupancy. For post-accident operator actions, both diagnosis errors and execution errors are modelled as per Section 6.

The detailed scenarios/sub-scenario frequencies are then combined with the appropriate CCDPs to obtain better estimates of the flood-induced SCDF for each flood area. These are summed with the SCDFs that are retained from the screening analysis to obtain a total SCDF.

9.2.2.7 Final List of Potentially Significant Flooding Areas and Scenarios

The results of the screening analysis are compared with the screening criterion (severe core damage frequency less than 10^{-6}) to identify a final list of flood areas that require further detailed analysis.

9.2.3 Detailed Analysis

This part of the analysis deals specifically with the potentially significant flooding sources and scenarios that are identified in the screening analysis. The flooding frequency is calculated based on plant-specific data, and the impact of intermediate flooding growth stages within each area are assessed together with a more realistic evaluation of the capability of flooding damage to spread to adjacent areas. Local operator recovery actions, which are performed in areas that are not affected by flood, are also credited. Once the flood SCDF sequences have been calculated, the summed SCDF can then be calculated.

9.2.3.1 Definition of Flooding Areas

The flooding area is defined to be the area that is bounded by the walls or barriers that are able to reasonably contain the floodwater in the area. The barriers do not need to be watertight doors or barriers. A fire door is considered to be able to reasonably contain floodwater for a sufficient amount of time.

CANDU 6 design mainly consists of open areas and thus, there are only a few areas that can be considered as flooding areas. The flooding area is considered to be the area covered by the flood. The floodwater is assumed to flow into lower levels if there are any openings. Thus, this methodology is based on the flooding sources in a given area (buildings and flow elevations).

9.2.3.2 Flood Frequency Estimation

Flooding can be caused by piping breaks, valve ruptures, expansion joints rupture, tank ruptures, etc.

If there is more than one flooding source in one area, then the flood frequency is calculated by summing the flood frequencies from all sources.

9.2.3.2.1 Piping Failure Frequency

There are several approaches for estimating piping break frequency. Two approaches are presented here - the Thomas correlation, and the WASH-1400 approach.

There are also other available data sources.

The Thomas correlation (Reference 9-1) estimates the pipe failure frequency as a function of pipe diameter, length, thickness, the number of welds, and other empirical correction factors such as aging, design, quality, etc. The equation is as follows:

$$P_c = P_L' \times (Q_p + A \times Q_w) \times B \times F$$

where

P_c = Probability of pipe catastrophic rupture

$P_L' = P_C \backslash P_L$, empirical correlation based on membrane stress and wall thickness

Qp = pipe geometric factor, equal to $D_p L_p / T_p^2$

Q_w = welding geometric factor, equal to $n \times D_w L_w / T_w^2$

D_w, D_p = diameter of welding and pipe, respectively

L_w, L_p = length of welding and pipe, respectively

T_w, T_p = thickness of welding and pipe, respectively

A = welding material factor

B = design learning curve factor

F = plant age factor

This equation also has the provision to determine the frequency for different break sizes. However, the application of this equation requires detailed piping information, which is not practical to acquire. Therefore, this correlation is also not recommended to be used in the flooding PSA.

The WASH-1400 approach (Reference 9-2) estimates the pipe break frequency as a function of pipe diameter (i.e.: > 3 in. and < 3 in.) and "segments", as follows:

For piping > 3" diameter, median: 8.76×10^{-7} events/yr, 95% confidence: 2.62×10^{-5} events/yr

For piping ≤ 3" diameter, median: 8.76×10^{-6} events/yr, 95% confidence: 2.62×10^{-4} events/yr

Segments are defined as the section between major components, such as valves and pumps. A pipe "Tee" fitting is considered to be a segment. The WASH-1400 frequency is a composite frequency that accounts for large, medium and small break sizes. This approach does not require detailed information and is relatively simple to apply. Thus, this approach is most suitable for the generic purpose of this flooding assessment.

The flooding PSA for Calvert Cliffs plants in the US (Reference 9-3) compared the approach of the Thomas correlation, (Reference 9-1), and the flood failure data experience for LWRs, and concluded that

- since the Thomas correlation utilizes the length of pipe segments as well as the number of segments, it tends to calculate a higher frequency;
- if frequencies are calculated for a building or a system, the results from the Thomas correlation and flood experience data are relatively close; and
- for piping with few welds, the Reference 9-2 frequency is more realistic, whereas the Thomas correlation may predict a high frequency.

Based on the above observations and the simplicity of its application, the WASH-1400 approach (Reference 9-2) is recommended for use in the flooding PSA.

9.2.3.2.2 Valve Rupture Frequency

External ruptures of valves can cause flooding. The CANDU operating experience shows the failure rate of external leaks, but the definition of external leaks is not stated. For example, the failure rate of external leaks for MOVs that are larger than 2" is 1.65E-2/y, which is judged to include all types of leaks. Therefore, it is not recommended to use the failure mode of external leaks in the flooding PSA.

Reference 9-5 presents following failure rates of leaks and ruptures for valves:

Manual Valve	1.3E-8/hr
Air-Operated Valve	2.0E-8/hr
Motor-Operated Valve	1.7E-7/hr
Check Valve	5.2E-8/hr

Of the 18 failures reported, only one was a valve body crack. Therefore, the flooding frequency due to the valve rupture can be estimated by dividing the failure rate by 18.

Reference 9-2 presented the median rupture frequency of all types of valves as 1.0E-8/hr with an error factor of 10. Thus, the mean rupture frequency of valves would be approximately 3.0E-8/hr.

The frequency is consistent with that of Reference 9-2 and the factor of 18 presented in Reference 9-5 is reasonable.

Therefore, it is recommended that the flooding frequency due to the rupture of valves be estimated using the frequency presented in Reference 9-5.

9.2.3.2.3 Expansion Joints Failure Frequency

One of the major causes of flooding is the rupture of expansion joints in high flow-rate piping.

The CANDU database presents the frequency of external leaks for expansion joints. This failure frequency is equivalent to the failure frequency for all modes of expansion joints. The failure rate includes external leaks; therefore, it is too conservative to be applied in the flooding PSA and therefore not selected.

The Calvert Cliffs PSA (Reference 9-3) used the failure frequency presented in the Oconee PRA for the expansion joints of the Condenser Cooling System. The failure frequency is 2.5×10^{-4} events/yr, and has been widely used in flooding PSAs for LWR plants in the USA.

It is recommended to use the Calvert Cliffs PRA failure frequency for the flooding PSA.

9.2.3.2.4 Tank Failure Frequency

The rupture of tanks can cause flooding.

CANDU experience data show the frequency of external leaks for tanks which includes tank's ruptures as being 2.3×10^{-3} events/year. The failure frequency is for all types of failure modes. Thus, the failure frequency is considered too conservative for use in this flooding PSA methodology.

Reference 9-4 shows the rupture frequency for the feed water storage tank and refuelling water storage tank for PWRs as being 2.8×10^{-4} events/year and 2.3×10^{-4} events/year, respectively. The data are based on 1.36×10^{5} hours of operating experience with no failures. These data are more applicable, considering that there are no catastrophic failures of tanks.

Therefore, in the flooding PSA, it is recommended to use the failure frequency of 2.3×10^{-4} events/year for the rupture frequency of tanks.

9.2.3.3 Flood Flow Rate

In the case of a flooding event, the operators can isolate the flooding before it can affect the safety functions.

The estimation of available time for operators to isolate the flooding is one of the essential tasks in the flooding PSA.

The time available would be dependent on the flooding flow rate and the floodable space.

The flooding flow rate would be limited by the maximum pumping rate, maximum flow rate of orifices, and maximum flow rate of pipes. Since all three factors can limit the flow, the lowest

flow rate among them would be the flooding flow rate. The maximum pumping rate would be the pump run-out flow rate, multiplied by the number of operating pumps.

The orifice flow rate can be estimated by using the following equation:

$$Q_{F.R.} = 0.525 \times C \times D^2 \times (Dp/\rho)^{1/2}$$

where

C = 1 for a double-ended break

D = inside pipe diameter (inches)

Dp = pressure differential (psi)

ρ = water density = 62.3 lb/ft^3

In order to apply this equation, information regarding the operating pressure at the orifice point and the diameter of the pipes are required.

The maximum flow rate of piping can be estimated by using the following equation:

$$Q = 96.3 \; A \times (\Delta P/\rho \; K \; Le)^{1/2} \times 7.48 \times 60$$

where

A = inner surface area of piping

ΔP = differential pressure

ρ = density of flood flow

K = resistance factor

Le = equivalent length of the piping

This equation is known to have high uncertainty, due to the inherent nature of K and Le. Also, the use of this equation requires detailed information about the layout of the piping, in order to estimate Le.

If all the required information for estimating the flood rate is not available (e.g., the operating pressure of piping flooding sources is not available), then the orifice flow rate is estimated using the pump discharge pressure.

If both the operating pressure at the orifice point and the pump discharge pressure are not available, then the normal pumping flow rate, multiplied by the number of operating pumps is used for the flood flow rate.

9.2.3.4 Operator Recovery Actions

In the detailed analysis, local operator actions, such as the opening or closing of valves or pumps to terminate water spill or to re-divert the water, the closing of the door in the flooded area and the preventing of flood propagation to adjacent areas, are considered to be creditable.

The time available for the operator action to isolate the flood can be estimated, by dividing the amount of flooding water by the flow rate.

For post-accident operator actions, both diagnosis errors and execution errors are modelled as per Section 6 of this document.

In assessing the diagnosis time, the time starts from the receipt of the first alarm and indications to the operator of the off-normal conditions, but excludes the time taken to execute the action.

The HEP for the execution tasks is calculated in dependence on the task and the stress level. The recovery actions are classified as dynamic tasks. Credit for the second and/or third operator can be given, depending on the time available and the location of the task to be performed.

9.2.3.5 Categorization of Flood

The flood frequency and flood flow rate are estimated using the above equations. Failure frequencies are used for guillotine-type breaks of the piping and catastrophic failures of tanks or valves. Experience shows that flooding due to catastrophic failures is quite rare.

The Calvert Cliffs PRA (Reference 9-3) categorizes the flood frequency and flood flow rate as large, medium and small floods, using the following factors:

Flood frequency (large flood)	= Flood frequency × 0.1
Flood flow rate (large flood)	= Flood flow rate
Flood frequency (medium flood)	= Flood frequency × 0.3
Flood flow rate (medium flood)	= Flood flow rate/3
Flood frequency (small flood)	= Flood frequency × 0.6
Flood flow Rate (small flood)	= Flood flow rate/6

This categorization method is widely accepted, and is used in most flooding PSAs for LWRs.

It is recommended to use this categorization method in the flooding PSA.

9.2.3.6 Other Calculations for Flooding PSA

Floodwaters that accumulate in an area can propagate to other areas via doors, or they can be transferred to sumps via floor drains. For the case of small flooding, the flood propagation or outward flow under doors or drains can impact the flooding scenario.

The flow rate under a door can be estimated using the following equation:

$$Q^{F.R.}(\text{Door}) = 448.8(0.7021 + 0.0074\ W)\ a\ W\ \{2g(H-a)\}^{0.5}\ \text{gpm}.$$

where a = floor undercut (ft)

W = door width (ft)

g = 32.2 ft/sec^2

H = flood depth (ft)

In estimating the flow rate from the above equation, it is assumed that the floor undercut is typically 1.5 inches, and the width of the door is 4 ft.

The transferred flow rate via drains can be roughly estimated using the following equation:

$$FR\ (\text{Drain}) \sim 7.6\ d\ H^{3/2}\ (\text{ft}^3/\text{sec})$$

where d = diameter of drain in ft.

H = water depth in ft.

9.2.3.7 Probabilistic Evaluation of Flood Growth

The growth of the flood level is determined by taking into account the flooding flow rate, the free cross-sectional area available for flooding, and the capability of the drainage pathways (floor drains and leakage pathways to adjacent areas under doorways). In addition, drain obstruction due to the failure of any check valves or due to drain blockage must be addressed.

Flood growth may be terminated at any time by operator action that is taken to isolate the flood source, or by the exhaustion of the flood source itself.

9.2.3.8 Classification of Flood Scenarios

After the flood areas and the flooding sources in each specific flood area are identified, the flood scenarios are developed.

The flood scenarios are dependent on the flooding source, the area's layout, the flood propagation, and the time that is available for the operator to isolate the flood.

There may be several flood scenarios for a flood event in one flood area. The scenarios differ from each other by the rate and magnitude of the flood in a given area, the damage to any critical equipment, and the manner in which they are mitigated.

Flood scenario diagrams will be developed for a particular flooding event. The entry point of the flood scenario diagram is the frequency of the flooding event, and the end points of the flood scenario are the flood damage states—the failure of mitigating systems after the flooding event.

9.2.3.9 Evaluation of Flood-Induced Accident Sequence Probabilities

The end points of the flood scenario diagrams are the flood damage states, which will be assessed further by developing event trees (for the failure of mitigating systems after the flooding event).

The heading of the event tree represents the failure of the mitigating system(s), i.e.: the loss of the service water system due to flooding, the loss of RCW and the feed water system due to flooding, etc. The flood frequency is assumed to be 1.0 in this step.

After quantification, the end points of the event tree for each specific flood damage state are summed together, and they represent the CCDP.

9.2.3.10 Evaluation of the Severe Core Damage Frequencies due to Flooding Event

This step evaluates the severe core damage frequency for different flooding sequences. An example of flood calculation is given in Appendix D.

For each flood scenario, the flood frequency, the probabilities of operator error in terminating the flood, the flood propagation probability (flood barrier failure probability) and the CCDP of flood-induced accidents are required, in order to evaluate the severe core damage frequency as follows:

$$F_{CDF} = F_{IE} \times P_{BF} \times P_{OP} \times P_{CD}$$

where

F_{CDF} = severe core damage frequency of flood-induced accident (events/year)

F_{IE} = Flood frequency (events/year)

P_{BF} = Failure probability of flood barrier

P_{OP} = Failure probability of operator action

$P_{CD,}$ = CCDP

The results are the final severe core damage frequencies for each flooding sequence.

9.3 References

9-1. H.M. Thomas, 1981, Pipe and Vessel Failure Probability, Reliability Engineering Volume.

9-2. USNRC, 1975, WASH-1400, Reactor Safety Study – An Assessment of Accident Risks in US Commercial Nuclear Power Plants, USNRC Report, NUREG – 75/014.

9-3. Baltimore Gas and Electric, 1993, Calvert Cliffs Nuclear Power Plants Probabilistic Risk Assessment Individual Plant Examination, Summary Report, Publisher.

9-4. IAEA, 1988, Component Reliability Data for Use in Probabilistic Safety Assessment, IAEA Report, IAEA-TECDOC-478.

9-5. W.H. Hubble and C.F. Miller. 1980. Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants. NUREG/CR-1363, Volume 1-3.

Table 9-1
Data Recording Sheet

Walk-down Analyst:	**Date:**		
A. GENERAL INFORMATION:			
Plant/Unit:	**Building:**		
Room/Area/Zone:			
Room Title:			
B. EQUIPMENT LOCATED WITHIN AREA (provide list):			
System/Components:	**Height Off Floor**	**Spray Source Nearby (Y/N)**	**Spray Protected (Y/N)**

10. LEVEL II PSA

10.1 Overview

The level II PSA consists of probabilistic and deterministic analysis elements. The probabilistic element consists of the development and quantification of containment logic models. The tasks for the development of the logic models include

- the grouping and categorisation of accident sequences into PDSs— see Section 4.9, where the PDSs are described;
- the development of a CET, which defines a spectrum of containment damage or release states;
- the development of CET top event definitions and the quantification of failure probabilities by fault tree analysis; and
- the collapsing of the CET release modes into a few release/consequence categories. The release categories are containment failure bins, for which fission product releases (source terms) are calculated.

The containment model development and quantification procedures are supported by deterministic models of accident progression (a Level II PSA code). These include

- physical process analysis of accident progression, i.e.: containment response, and
- source-term analysis of radionuclide releases to the environment.

Containment performance analysis refers to the study of the progression of the various accident sequences that result in releases of radionuclides into containment.

Strictly speaking, all of the analysis tasks that deal deterministically with the accident progression from each PDS and with the calculation of the frequency and magnitude of releases from containment can be classified as Level II PSA activities. However, a distinction is drawn between the analyses of the design basis and severe accidents that are required to demonstrate compliance with Reference 10-1, and the analyses that go beyond the design basis—SCD accident sequences. For the purposes of this document, only the SCD accident progression will be referred to as Level II PSA.

10.2 Implementation

The following tasks are required for the containment performance analysis:

a) Identify containment performance features
   1) Collect and review plant data, and
   2) Select and review reference plant analyses that are contained in documents such as
      - safety report, and
      - other safety reports (e.g., containment ultimate pressure capacity reports).

b) Develop accident sequences
   1) Define the PDSs, and
   2) Evaluate containment performance and determine credible containment failure modes.

c) Develop the CET
   1) Develop the CET and define top events,
   2) Create logic models for the CET top events, in terms of containment systems performance, and
   3) Quantify branch point probabilities by means of fault tree analysis.

d) Develop containment release model
   1) Categorize the release modes,
   2) Estimate source terms, and
   3) Define release categories.

10.3 Containment Performance Features

The first task of the CET analysis is to identify the containment features that are likely to affect the progression of a design basis or severe accident event. This task involves the collection of plant data, the identification of unique features of the specific plant being analyzed, and the selection of deterministic analyses from relevant CANDU safety reports.

Certain features of the plant, such as the moderator system, containment design, pressure and temperature limits, and the containment systems may significantly affect the progression of design basis or severe accidents. Plant-specific features that can be important to accident progression include:

- Containment performance characteristics and minimum allowable performance limits, e.g., design pressure, structural integrity (ultimate pressure capability), penetration thermal limits, and isolation failure and bypass pathways.
- Unique containment features. For example, some containment structures tend to relieve overpressure through cracking rather than through a structural failure.
- Containment systems capabilities and limits, e.g., local air coolers, isolation system, ventilation system, hydrogen igniters, post-LOCA instrument air system and gross containment leakage monitoring.
- Primary heat transport and main steam system features.
- Operator actions that impact accident progression.

10.4 Collection/Review of Plant Data

The information gathered under this task is generally qualitative in nature; however, sufficient quantitative information to support the scoping calculations for key phenomena is also compiled.

For example, qualitative information includes the containment type (i.e., single-unit containment for the CANDU 6 and CANDU 9 type reactors), structural design (e.g., reinforced vs. pre-stressed concrete containment) and the containment layout.

Quantitative information includes the core thermal power rating, containment design parameters (e.g., design pressure, failure pressure, containment volume), containment systems capacities, HTS system conditions (coolant inventory, LRV setpoints) and the ECCS capacities.

The collected CANDU 6/CANDU 9 containment systems and related reactor data are organized and related to parameters that impact accident progressions. Generally, the containment parameters that are important in risk determination include

- containment ultimate capacity (pressure/temperature limits),
- containment systems mitigating capability, and
- containment systems-induced failure modes (i.e.: isolation failure or bypass mechanisms).

Plant information can be collected from the following sources:

- containment layout drawings,
- containment structural design information (in the containment design manual),
- the containment system model,
- primary (HTS) and secondary (main steam/water) systems descriptions (in system design manuals),
- containment systems descriptions (in containment design manual),
- technical specifications (in the specific CANDU 6 or CANDU 9 PSAR), and
- abnormal operating manuals (AOMs)—the basis of these procedures, i.e.: the Operator Response Guidelines (ORGs), are developed (as part of the PSA work) as an input to the AOMs.

10.5 Development of Accident Sequences

Accident sequences that do not lead to SCD but that do cause releases into containment are grouped into the PDSs described in Section 4.9. The sequence groupings are based on similarities in accident progressions and systems that impact the containment response to accident loads. This serves as the interface with the Level I PSA, and provides the starting point for investigating the various containment response scenarios with the aid of the CET.

The PDSs become the inputs to the CET, and the CET end states (outputs) are grouped into a relatively small number of release categories (RCs) that give the frequency and magnitude of radionuclide releases from containment for each of the PDSs.

The analysis steps for this task, i.e.: the development of accident sequences, require that the following be accomplished:

a) definition of PDSs (see Section 4.9),

b) construction of the CET and supporting fault trees, and

c) assessment of containment failure modes (containment impairment states).

10.6 Containment Event Tree Model Development

10.6.1 General

CET analysis begins with the set of PDSs that define the boundary conditions of the accident sequences identified in the analysis. Releases to the environment depend on the interactions between the characteristics of the PDS and the conditions of the containment structure and its systems. The development of the CET requires the identification of the important containment failure modes, e.g., isolation failures, containment bypass, and the overpressure failure of containment envelope, from which the CET top events are derived. Fault tree analysis is then carried out, in order to estimate the failure probabilities of the top events.

The development of the CET involves the following steps:

a) Identification of containment failure modes (containment impairment states).

b) Identification of CET top events, which are generally containment performance- or failure-oriented.

c) Development of fault trees in support of the CET top events. The fault trees model the important systems, phenomena and operator actions that affect containment integrity and radionuclide releases.

d) Grouping of the CET end-states (release modes or containment failure bins) into release or consequence categories, according to the frequency and magnitude of the radionuclide release from containment.

Containment bypass is considered in establishing PDSs and it is considered as a sub-category of a PDS.

10.6.2 CET Top Events

In the process of developing the CET, it is necessary to identify those systems and functions whose success or failure can influence the release of radionuclides to the environment. The CET top events are generally containment performance- (success/failure) oriented, reflecting

performance issues that affect source term magnitudes. The CET will include the analysis of the important containment systems for CANDU 6:

a) Local air coolers
b) Airlocks
c) Containment isolation system
d) Dousing system
e) Hydrogen igniters and/or hydrogen recombiners (for new CANDU 6 designs)

The systems that require modelling for the CANDU 9 design are

a) Local air coolers
b) Airlocks
c) Containment isolation system
d) Hydrogen igniters / hydrogen recombiners.

10.6.3 CET Top Event Logic/Fault Trees

The CET top events are supported by logic trees, which model the logical relationship of the relevant issues that determine the likelihood of the CET nodes (branch points). The logic trees are fault tree representations of the various phenomena, systems-related issues and boundary conditions that are modelled as basic events. The basic events determine the likelihood of the top event.

Some of the supporting fault trees contain events that are phenomenological in nature, such as a containment failure due to a hydrogen (H_2) burn or steam overpressure. Since such failure modes are expected to occur only in sequences of very low frequency, simple conservative criteria will be developed to determine whether or not the event is considered to be possible for a given PDS. If the criteria are met, then the probability is set to unity; if not, then the probability is set to zero.

10.7 Containment Bypass Events

A special class of events exists, where the release of radionuclides from the HTS is directly outside containment. The potential for such events exists, wherever the HTS piping itself is outside containment, e.g., instrument lines, or where the failure of an interface could lead to the same result. Some of these events include:

- steam generator tube rupture,
- rupture of degasser-condenser heat exchanger into the RCW system,
- rupture of the HTS purification heat exchanger into the RCW system, and
- interfacing LOCA (“V” scenario).

In the absence of any automatic or operator action to stop the leak, HTS coolant will be discharged outside containment until, ultimately, cooling to the core is lost.

10.7.1 Assessment of Containment Failure Modes

During the CET analysis, an assessment is made of the likely containment failure modes, such as isolation failures, containment bypass, loss of local air coolers, etc. A complete list of containment failure modes (containment impairment states) is identified during the process of CET development.

For CANDU 6 and CANDU 9 systems, pressure and temperature transients within containment that are due to mass and energy discharged from breaks in the primary or secondary HTSs are simulated using containment computer codes such as PRESCON2 (Reference 10-4). The behaviour of airborne gaseous radionuclides inside containment is modelled using a computer code such as SMART. An evaluation of the ultimate capacity of the containment structure is required, in order to assess its ability to withstand the pressure loads.

10.8 Environmental Transport and Consequence Analysis

For CET analysis described above, containment failure 'bins' or release modes (RMs) are developed. The RMs are CET end states with similar source-term characteristics, and are combined into a few RCs for off-site consequence analysis, in order to enable the comparison of doses to C-6 criteria as in References 10-1 and 10- 2 (note that reference 10-2 is under review by the industry and is a draft). Off-site consequence analysis is known as Level III PSA.

RCs define the sequence of radioactive releases outside the containment boundary, and are quantified in terms of dose. These values are checked against the limits given in the appropriate C-6 document.

For events that are not covered in the safety report for a given project, dose calculations are performed as part of the PSA support analysis described in Section 4.3.2.1 of this document. The PSA support analysis dose calculations will use best estimates as their input.

10.9 Severe Core Damage Accident Progression

10.9.1 MAAP CANDU

10.9.1.1 Introduction

The Modular Accident Analysis Program (MAAP) is an integral systems analysis code for assessing severe accidents, and was initially developed during the industry-sponsored IDCOR program. Ownership of MAAP was transferred to EPRI at the completion of IDCOR. Subsequently, the code evolved into a major analytical tool for supporting the plant-specific Individual Plant Examination (IPEs) requested by USNRC Generic Letter 88-20 (Reference 10-3). Furthermore, the scope of MAAP (its design basis) was executed to include

accident management, using the new models included in MAAP4. In addition, MAAP3B was expanded to include the OPG CANDU designs, and this has been further updated to the MAAP4-CANDU model. MAAP4 has been also modified to represent the VVER designs used in Finland and central Europe, and to represent the vertical pressure tube design used in the Fugen plant in Japan.

The MAAP for CANDU NGS MAAP4-CANDU (M4C) is a computer code that can simulate the response of the OPG or AECL CANDU 6 and CANDU 9 NGSs during severe accident conditions, including actions that are undertaken as part of accident management. The MAAP4-CANDU code was developed on the base of the MAAP4 code (used for PWRs and BWRs). The architecture of the MAAP4 CANDU software system is discussed below and a schematic is shown in Figure 10-1.

10.9.1.2 Scope

Use of M4C allows us to predict quantitatively the progression of severe accidents starting from normal operating full power conditions and applying a set of NPP system faults and initiating events leading to HTS inventory blowdown, core heatup and melting, HTS failure, calandria vessel failure, reactor vault failure and containment failure. Furthermore, some models are included in the code to analyze accident mitigation measures, such as debris cooling in the calandria vessel or containment.

M4C has models of the following principal CANDU systems in addition to other important systems:

- Two-loop HTS including piping, pumps, inlet and outlet headers and feeders,
- Pressurizer;
- CANDU reactor core;
- Steam generators - primary and secondary sides;
- Containment building including a number of compartments;
- Calandria vessel and moderator cooling system;
- Reactor vault;
- Shield Tank;
- End shield cooling system;
- Emergency core cooling system (high, medium and low Pressure components);
- Reserve Water System;
- Containment dousing spray system;
- Local air coolers;
- Power operated and passive (spring loaded) relief valves

M4C treats the spectrum of physical processes that might occur during an accident such as steam formation in the HTS, core heatup, hydrogen generation, calandria and reactor vault failure, core debris-concrete interaction, ignition of combustible gases, steam explosions, fluid entrainment by high velocity gas, fission product release, -transport and -deposition. The most important distinguishing feature of M4C compared with MAAP4 is the model of the CANDU horizontal reactor core with fuel bundles situated inside pressure and calandria tubes. The important processes and phenomena which control the core behaviour are modelled in the CANDU Channels Routine, including:

- Temperature excursion and deformation of fuel and fuel channels and interactions with the moderator system;
- Zircaloy-steam reaction;
- Thermal mechanical failures of fuel channels;
- Disassembly of fuel channels;
- Formation of suspended solid debris beds;
- Motion of solid and molten debris bed;
- Interaction of the core debris with steam;
- Fission product release.

MAAP4-CANDU features also include:

- Operator interventions in a flexible manner, allowing user to model operator behaviour.
- Capability of different events modeling (such as crash cooldown system operation- i.e.: simultaneous opening of steam generator safety valves).
- Input flexibility - code has two files containing input parameters: A “parameter” file containing specific NGS data such as main NGS operating parameters: pressures, temperatures, equipment volumes, water inventory, etc. The second one is an “input” file containing characteristics of the sequence to be analyzed, namely whether it is a Station Blackout, large LOCA, small LOCA or Steam Generator Tube Rupture so that the user can easily make any changes in plant data or specific regime data.
- M4C is organized such that the effects of uncertainties in individual physical processes (models) can be conveniently analyzed through changes in selected input parameters, which define the phenomenological model.

The typical accident sequences which could be analyzed by M4C are:

- Large Break Loss-of-Coolant Accidents;
- Small Break Loss of Coolant Accidents;
- Transient initiated events such as Loss of AC and DC power;
- Steam Generator Tube Rupture; and

- Main Steam Line Break.

10.9.1.3 Modular Structure of MAAP

MAAP has a modular structure, in which separate subprograms are dedicated to specific region models and physical phenomena. This structure facilitates code enhancements, because improvements to phenomenological or region models can be made to relatively small subprograms. MAAP4-CANDU consists of a main program, which directs program execution through several high-level subroutines. These subroutines call a sequence of system and region subroutines at each time step, which, in turn, call phenomenological subprograms as required. At the lowest level, a set of property-library subprograms for physical properties and utility subprograms are available for I/O.

There are four levels of subprograms within MAAP4-CANDU:

- high level (executive) subroutines,
- system and region subroutines,
- phenomenology subroutines, and
- property and utility subroutines.

The **high level subroutines** include the main program, the input-output subroutines, the data storage and retrieval subroutines and the numerical integration subroutines. The time integration subroutines INTRT and DIFFUN control the time step, and call the system and region subroutines at each time step during an accident transient.

The **system and region subroutines** include the EVENTS subroutine, which sets the event flags (Boolean variables), thus providing the status of the system and the status of operator interventions. The event flags control code execution. The region subroutine defines the differential equations for the conservation of internal energy and mass. The system subroutine examines inter-region flows. The system and region subroutines pass global variables by common blocks, and operate on them by calling the phenomenology subroutines.

The **phenomenology subroutines** describe the rate of the physical processes that are taking place in each region of the NGS model. The phenomenology subroutines are generic in nature, and can be called by any of the system, or region subroutines, or by other phenomenology subroutines. This modularisation allows the fundamental physical models to be changed by altering or rewriting a subroutine, independent of the rest of the MAAP4-CANDU subroutines.

The **property and utility subroutines** provide the physical properties (e.g., specific heat, saturation pressure, viscosity, etc.) of the important materials (e.g., steam, water, air, etc.). Property and utility subroutines are generally called by the phenomenology subroutines.

The code is written in the FORTRAN77 language, and contains 514 subroutines.

10.9.1.4 Solution Technique

The MAAP code uses a two-stage computational procedure, in which the present values of the dynamic variables that describe the state of the system (often masses and internal energies) are used to calculate their rates of change. These rates are integrated in a separate subroutine, in order to provide updated values for the dynamic variables.

The integration technique generally used in MAAP is an explicit, first order, Euler method. An alternative approach, a second order Runge-Kutta integration, can be selected through the parameter file. A typical M4C run has time steps as small as 0.001 seconds and as large as 20 seconds.

10.9.1.5 Program Features

A number of features are incorporated in MAAP4-CANDU to enhance its usefulness. Some of these features are discussed below.

10.9.1.5.1 Auxiliary Building Model

MAAP4 can model the auxiliary/reactor building response for mass and energy flows, from either the containment (e.g., failure of the containment boundary due to overpressure) or the primary system. The auxiliary/reactor building model can be run simultaneously with the primary system and containment models. In M4C, there is no real distinction between the containment compartments and the auxiliary building compartments; in effect, the phenomena have been expanded and treated generically for all compartments, due to the nature of the generalized containment model.

10.9.1.5.2 Input Flexibility

The parameter file, which is required by MAAP4 to define the reactor system, consists mainly of plant-specific data that will not change from one run to another. These data are relegated to a disk file, which is read by M4C at the start of execution. Accident-specific inputs, such as accident initiators and operator actions, are contained in a separate input deck, which is read by M4C during execution. The user may change parameter file entries for individual runs, by specifying those changes in the input deck. Thus, the parameter file for a specific plant needs to be prepared only once, and temporary changes to any parameter file entries can be made at execution time, without manipulating the parameter file itself.

10.9.1.5.3 Operator Interventions

M4C enables the user to model the plant operator in a general way. The user may establish one or more intervention conditions, by specifying limits for any variable within a set of key variables, or by declaring any of more than one hundred event flags as key events. When a key variable reaches its specified limit or a key event flag changes status, program execution pauses, and operator actions (also specified by the user) are taken. The operator actions consist of

changes to the event flags and/or the re-definition of some plant parameters. In this way, M4C is directed by a pseudo-operator, who uses present plant conditions to make operational decisions.

10.9.1.5.4 Accident Summary

An accident summary is printed at the end of a run, and provides a chronology of significant events such as engineered system response and operator actions.

10.9.1.6 MAAP Benching Marking

Numerous comparisons between MAAP4 and separate effects tests, integral experiments, actual plant transients and accidents have been performed to illustrate the performance of individual models, and to provide confidence in the MAAP integral results. Activities that have been used to benchmark the MAAP4 program are listed in the MAAP4 manual.

10.9.1.7 Output

During the run, MAAP-CANDU produces several types of output files.

Log file

This file contains computer-specific file location information and computer diagnostic messages. It also contains operator intervention and user-defined event codes.

Event summary file

This file contains a more complete list of changes in event codes than the log file, and shows the sequence run, e.g., SG is dry, shutdown system is on or off, ECCS pumps are on or off, etc.

Tabular output file

This file contains calculated physical quantities, such as pressures, temperatures, water levels, fuel/debris masses, gas composition, fission product masses, erosion depths, etc.

Information is written to this file at user-input print intervals.

Plot files

Values of specific variables are written at more frequent intervals to the plot files, for subsequent plotting. The number and content of the plot files is specified by user in the parameter file, and is normally about 30 plot files, with each plot file containing about 30 parameters. Post-processor programs, MULTY-PLOT or LOOK, are used for plotting X-Y graphs (e.g., pressure in the specified compartment versus time). These plots can be printed on paper.

Restart file

During the run, the code creates the restart file, which could be used for repeating the same accident sequence from some intermediate time point, using different CANDU systems or

equipment. Restart data files are written at time intervals that are chosen by the user. M4C can resume execution from any time point at which a restart file entry was written. The restart may have new program intervention conditions, new operator actions, or even changes to the parameter file.

10.9.1.8 MAAP4 Events

There are three types of MAAP4 events:

- Automatic events, which have predefined meanings and which are set by the MAAP4 code during a run. Changes in the status of automatic events (TRUE to FALSE or FALSE to TRUE) may be used as intervention conditions.
- External events, which have predefined meanings and which are set by the input file as accident initiators or operator actions.
- User-defined events, which have meanings and status change logic that are defined by the user

10.10 References

10-1. CNSC, 1980, Requirements for the Safety Analysis of CANDU Nuclear Power Plants, CNSC Consultative Document, C-6, Revision 0.

10-2. CNSC, In preparation, Requirements for the Safety Analysis of CANDU Nuclear Power Plants, CNSC Consultative Document, C-6, Revision 1 (this document is under Review by the industry and is a Draft).

10-3. D. Crutchfield (NRC) to all Licensees. 1988, Generic Letter 88-20, Individual Plant Examination for Severe Accident Vulnerability.

10-4. W.M. Collins and R.K. Black, 1984, PRESCON2 Subsonic Compressible Fluid Flow Modelling, In Proceedings of the International Conference on Containment Design, pp. 191-194, Canadian Nuclear Association.

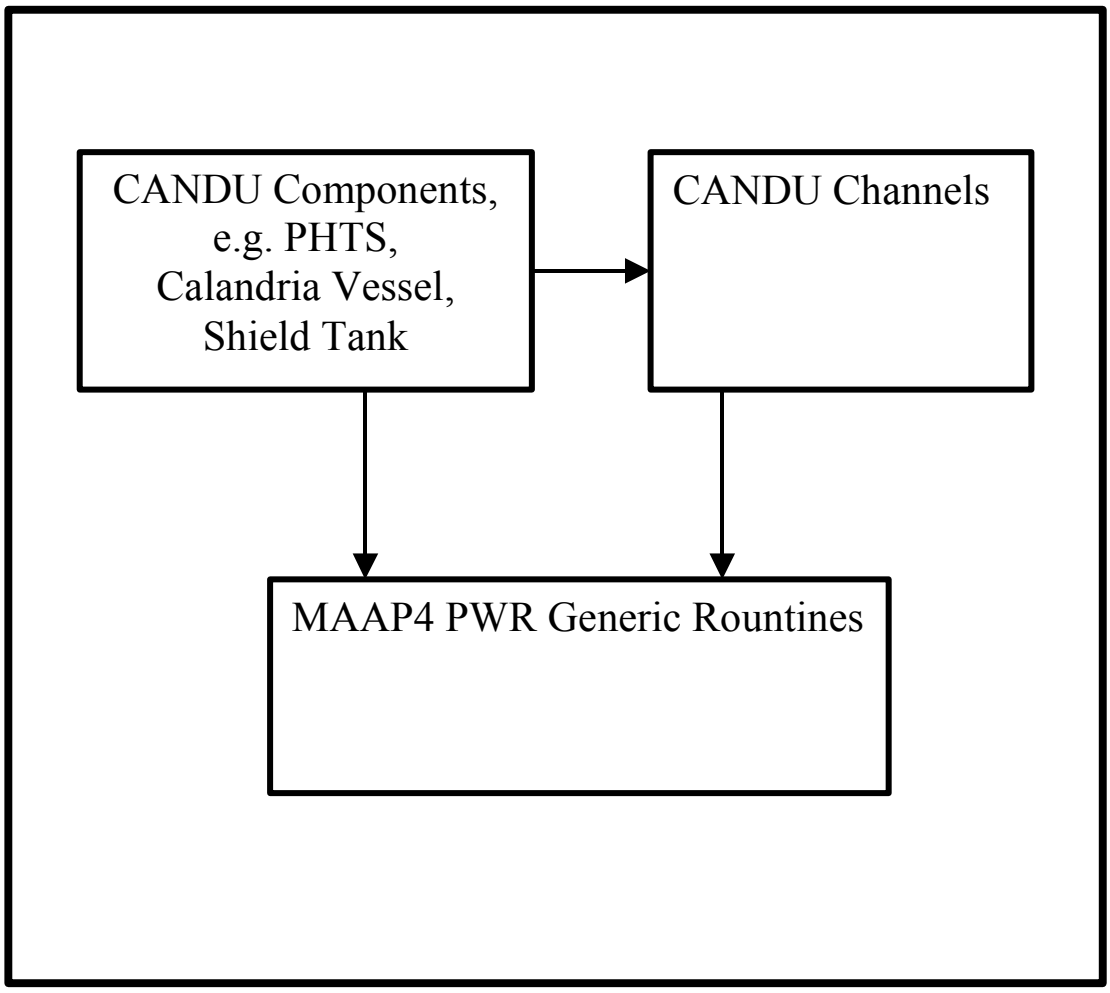


Figure 10-1 Schematic of the Architecture of the MAAP4 CANDU Software System

11. CONCLUSIONS

This document describes the methodologies used in the Generic CANDU PSA program at AECL. Special emphasis was placed on developing expertise in human reliability analysis, common cause failure and seismic, fire and flood events.

As well, a code was selected and developed to conduct Level II accident analysis to determine the timing of various events during severe accident progression and the release of fission products from containment for CANDU 6 and CANDU 9 designs.

The CCF method that was selected and described was the Unified Partial Method. The basic features of the UPM and its application were described. The method allows flexibility (qualitative and quantitative assessment), provides results that are tailored to the system being analyzed and permit sensitivity analysis to examine the effects of design changes.

The HRA methodology follows ASEP and THERP, which are internationally accepted methods.

Seismic PSA requires expertise in a number of disciplines, from the development of the seismic hazard to the calculation of HCLPFs for building structures and components. These calculations are then used as inputs by event tree analysis and seismic codes to determine SCDF frequencies. Mitigating system fault tree analysis for internal events is also required as inputs to the seismic PSA. Training was provided to AECL staff in seismic PSA and seismic PSA software was acquired.

Fire PSA involves a number of steps, including the calculation of relevant initiating event frequencies for CANDU components, knowledge of equipment location, the use of fire hazard assessment, and the development of event tree scenarios for specific fire zones in the plant. Training was provided to AECL staff in fire PSA and fire PSA software was acquired.

Flood PSA also involves steps that are similar to the fire PSA; however, flood PSA is not as complex. The methodology adopted is similar to international practice.

The steps involved in a Level II PSA have been described. MAAP4 CANDU was selected as the Level II code, and was modified for CANDU 6 and CANDU 9 designs. It is now possible to run the code for various scenarios, such as LOCAs and station blackout events. The validation and verification of the code is in progress.

These methodologies, tools and training allow AECL to conduct internal, fire, flood and seismic PSAs, and to conduct consequence analyses on all CANDU reactor products.

12. GLOSSARY

Abnormal Event (or Condition or Situation) - an event that disrupts the normal conditions in a plant. In the context of this document, it corresponds to the occurrence of an IE, a LOCA, or a system failure subsequent to an IE or LOCA.

Accident - an event or series of events in a plant that results in an abnormal situation, and that requires an appropriate system response (including human response), in order to restore the plant to a safe condition. This definition is a subset of the "Abnormal Event" event described above.

Accident Repair Time - the time required to gain access to the failed process system, and to return it to a functioning state, together with any other required equipment that was subsequently affected.

Accident Sequence Quantification (ASQ) - the process for quantifying accident sequences, in order to determine the dominant accident sequences, cutsets and frequencies.

Accident Sequences, Dominant - those combinations of IEs and hardware and human failures that lead to undesirable consequences with significant frequency.

Availability - the probability that the device (system) is operating satisfactorily at any given point in time, when used under stated conditions, and where the total time includes the operating time, active repair time, and administrative time.

Basic Human Error Probability (BHEP) - the probability of a human error for a task that is considered as an isolated entity, i.e., it is not influenced by previous tasks.

Basic Event (BE) – one of the primary events – see "primary event".

Basic Event (BE) Data base – one of three reliability databases in CAFA. The BE database has a .BE file name extension, and is referred to as the .BE file or database. It contains the BE label (or name) description, based on the fault tree event labelling scheme, probability data, and other support information

Basic Event Label/Name – A sixteen character label that contains the Subject Index (SI), Component Number (CN), Component Type (CT), Component Class (CC) and Failure Mode (FM) for the unique identification of a basic event.

Checker - a person who is assigned to verify the accuracy of another person's work, either while that person is doing the work, or after its completion. The use of a checker is an example of human redundancy. A checker is not the same as the person who performs an inspection. The checker is "person-oriented", whereas the inspector is "equipment-oriented" - see "Human Redundancy."

Checklist - a written procedure, in which each item is to be checked off using a pencil or other writing instrument as its status is verified.

Common-Cause Failure (CCF) - a failure that has the potential to fail more than one function or other abnormal event simultaneously, e.g., a human error that results in the mis-calibration of several setpoints.

Complete Dependence (CD) - a dependence between two activities that are performed by the same person, or between activities that are performed by different people. CD describes a situation in which, if the relationship between activities or people is positive (positive dependence), then failure to perform one activity correctly will result in certain failure to perform the other. Similarly, if success occurs in performing the first activity, then success will occur with the other. The opposite results will occur, if the relationship between the activities or people is negative (negative dependence).

Containment Envelope - comprises the reactor building, sealed penetrations, closed and open penetrations. All open penetrations are part of the containment isolation system.

An intact containment assumes that the reactor building perimeter wall is intact, and that the main and auxiliary airlocks and irradiated fuel transfer room are closed and intact.

Cutset - a set of elements whose failure will cause the system to fail.

Cutset, Minimal - a set of elements that has no proper subset, and whose failure alone will cause the system to fail.

Dependence (between two activities) - the situation in which the probability of failure (or success) for one activity is different, depending on whether a success or failure occurred on another activity. The activities may be performed by the same person (within-person dependence) or by different persons (between-person dependence). For the same pair of activities, the level of dependence may differ for errors of commission and errors of omission.

Diagnosis - the attribution of the most likely cause(s) of an abnormal event to the level that is required to identify those systems or components whose status can be changed, in order to reduce or eliminate the problem. Diagnosis includes interpretation, and (when necessary) decision-making.

This definition of diagnosis does not mean that it is necessary to assign the proper name of the abnormal event, in order to figure out what to do to cope with the event. The requirement for diagnosis in a post-accident situation can be minimized to the extent that the displays and emergency operating procedures clearly and unambiguously define the sequence of actions that is required, after the initiation of some abnormal event.

Dormant Failure – a failure that occurs when a piece of equipment is not in operation. The equipment may be out of service or on standby. This failure is not immediately detectable, unless detected and annunciated by a specific system. Without detection and annunciation, the failure will only be detected when there is a demand for the system, or during testing to ensure operability.

Event Tree Analysis - a method of modelling plant-level sequences that may lead to a PDS and that represents the response of the plant to the IE.

Failure Probability (unavailability) – the probability that, at any given point in time, a system or component will be unavailable on demand, i.e., not functional or operationally ready when required.

Fault Tree Analysis - a deductive type of failure analysis that focuses on one particular undesired event at a time, and then provides a method for determining the possible causes of that event. The fault tree itself is a graphical model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event.

Fault Tree Event Labelling Scheme – a method for uniquely identifying the primary events in a fault tree.

Front-Line System - those systems that directly performs a function to maintain normal reactor operation (e.g., feedwater) or during emergency operation (e.g., ECCS).

Fuel Channel Failure - the failure of the pressure tube (PT) and the calandria tube (CT).

Human Error Probability (HEP) - the probability that an error will occur when a given task or activity is performed. The nominal HEPs in the tables in this document are judged to represent medians of the lognormal distributions of HEPs.

Human Redundancy - the use of a person to check another person's work, or to duplicate the work. (synonym: "Checker") This term is the analog of equipment redundancy in a parallel system, i.e., at least two humans must err, in order that human error contributes to the probability of some unwanted system condition.

Initiating Event - an event that creates a disturbance in the plant and that has the potential to cause the release of fission products, depending on the successful operation of various mitigating systems in the plant.

Inspection - the recovery factor that describes someone looking at items of equipment to ascertain their status. If the task is to check someone else's work (by checking component status), then the job is designated as that of a checker. The inspector is "equipment-oriented", whereas the checker is "person-oriented".

Level I PSA - the identification and quantification of accident sequences, component data and human reliability, in order to determine a frequency of PDSs inside the containment.

Level II PSA - an analysis of the physical processes of an accident and the response of the containment, in addition to the analysis performed in a Level I PSA.

Level III PSA - environmental transport and consequence analysis. The Level III PSA assesses the public health risk and economic consequences of the accident, in addition to performing the tasks of a Level II PSA.

Loss of Core Structural Integrity - a loss of heat sinks leading to core damage that involves multiple fuel channel failures and core disassembly.

Mean Time to Repair (MTTR) – the average active repair time between the initiation and completion of a repair of a component. The MTTR of a component is given by the ration of the cumulative repair time (based on observation of actual repairs) in a given elapsed time, to the cumulative number of repairs (or failures) of the component in the same elapsed time. The MTTR does not include the time that is associated with repair-related activities, such as administration time.

Mission Reliability - the probability that, under stated conditions, the system will operate in the mode for which it was designed (i.e., with no malfunctions) for the duration of a mission.

Mission Time - the period of time in which a device (or system) must perform a specified mission under the required operating conditions.

Mitigating System - those systems whose primary function is to protect the reactor and ultimately the public against any abnormal event or initiating event, e.g., SDS, SDS2, FW, SDC, ECC or EWS etc. The system assists in returning the unit to a safe state.

Parallel System - a system which contains more than set of equipment that can perform the same function. For failure of the system, all "parallel" paths must fail. In fault tree analysis, the parallel trains in the system are modelled with an "ANDed" gate.

Performance Shaping Factor (PSF) - any factor that influences human behaviour. PSFs may be external to the operator, or they may be part of his or her internal characteristics.

Plant Damage State (PDS) - a group of fission product releases into containment that includes severe accident/severe core damage sequences, which have similar characteristics with respect to the severe accident progression and containment performance. In CANDU PSA, PDS also includes economic damage to the plant.

Post-Accident Task - all tasks required to cope with an abnormal event.

Post-Calibration Test - a test to determine if a particular component has been properly calibrated.

Post-Maintenance Test - a test to determine if a particular component works properly after maintenance.

Pre-Accident Task - a term denoting activities that are performed under normal operating conditions, including special conditions such as start-up operations or other activities, and that can affect the availability of equipment that are needed to cope with an abnormal event. (synonym: "test and maintenance task")

Primary Event – an event that, for one reason or another, has not been developed further, and hence represents the limit of resolution for a particular fault tree. Primary events include basic events, undeveloped events, developed (interfacing) events, conditioning events, and normally expected or external events.

Recovery Analysis - the process of identifying, quantifying and applying recovery actions to dominant minimal cutsets following ASQ. Normally, there are two types: those accomplished from the control room, and those performed in the field (if possible).

Recovery Factor (RF) - a factor that prevents or limits the undesirable consequences of a human error. One of the most common RFs is human redundancy. Other RFs are the effect on human performance of displays of component status in the control room (especially those which are annunciated), the effects of post-maintenance tests or post-calibration tests, and the effects of daily or shiftly inspections, especially those involving the use of written checklists.

Reliability - the probability that a device will perform a required function under stated conditions for a stated period of time.

Restore or Restoration Task - the returning of valves, circuit breakers, and other components to their normal states after the completion of maintenance, calibration, or testing. Restoration is not usually considered to be part of maintenance, because operations personnel, rather than maintenance personnel, usually perform the restoration tasks.

Restoration (Down) Time – the time interval during which a component is in the "down" state. The restoration time includes the following: detection time, administration time, MTTR, and the time between the completion of the repair and the return of the component to service.

Screening Analysis - the use of conservative estimates of human behaviour (i.e., higher human error probabilities and longer response times than expected) for each system event or human task, as an initial type of sensitivity analysis. If a screening failure probability does not have a material effect in the systems analysis, then it may be dropped from further consideration.

Sequence Designator - the abbreviation for a particular sequence resulting from an event tree which includes an initiating event and success and failure of mitigating systems.

Series System - a system which contains equipment one after another. Failure of any equipment in the train will fail the system. In fault tree analysis, the equipment in the system is modelled with an "ORed" gate.

Severe Accident - in a CANDU reactor, this is an accident in which the fuel heat is not removed by the coolant flow in the HTS. Severe accidents are characterized by plant damage states PDS3 and PDS4.

For example, a LOCA + LOECC is classed as a severe accident in a CANDU reactor, but it does not lead to SCD, due to the presence of the moderator as a heat sink. In LWRs, this would normally result in a core melt. In CANDU reactors, the moderator provides a heat sink for the core, and no fuel melting or fuel channel failures occur. Fuel damage (sheath failure) and structural distortion of the fuel bundles may occur within the fuel channels.

A LOCA + LOECC accident is defined by plant damage state PDS3 for the early need for the moderator as a heat sink, and by PDS4 for the delayed need for the moderator as a heat sink.

Severe Core Damage (SCD) Accident - an accident in which the rapid or late loss of core structural integrity occurs. SCD accidents are characterized by plant damage states PDS0, PDS1, PDS2.

PDS0 involves accidents with rapid loss of core structural integrity.

PDS1 involves accidents with late loss of core structural integrity with the PHTS at a high pressure (for example, a LOCA + LOECC combined with the loss of the moderator as a heat sink at high PHT pressure).

This event is beyond design basis accident.

PDS2 involves accidents with late loss of core structural integrity with the PHTS at a low pressure (for example, a LOCA + LOECC combined with the loss of the moderator as a heat sink at low PHT pressure).

Support System - a system that provides a function to a front-line system (e.g., electrical power, control power, instrument air, service water).

Surveillance - see "Inspection".

System, Dormant or Standby - a system (or part thereof) that is not in use during normal plant operation.

System, Mitigating – a system that is required to function following an IE to assist in returning the plant to a safe state.

Unreliability - the probability that a device will fail within a given period of time. Unreliability can be calculated as 1 minus the reliability of the device.

Zero Dependence (ZD) (between two activities) - the kind of dependence in which the probability of failure or success for one activity is the same, regardless of whether failure or success occurred for the other activity. The same or different person(s) may perform the activities (synonym: "Independence").

Appendix A

Internal Events PSA Supporting Information

A.1 Data Reduction and Confidence Limits

Once a mass of raw data has been collected regarding a component or a generic class of components, it is necessary to reduce the mass to a manageable amount using accepted statistical methods. Having derived a failure rate or a "mean time between failure" (MTBF) from a set of raw data, confidence limits for that calculated value need to be determined. There is a statistical technique for estimating confidence limits on failure rates and MTBFs.

An engineering interpretation for the statistical concept of confidence limits is that the calculated mean from the raw data will not exceed or fall below a certain value with a specified probability (or confidence). For example the 95% upper confidence limit for a MTBF is the value for which we are 95% confident that the MTBF will not exceed. Similarly we can say that the 5% lower confidence limit is the value that we are 5% confident that the MTBF will not fall below. The difference between the 5% lower confidence limit and the 95% upper confidence limit is called the symmetrical 90% confidence interval.

For data that conform to an exponential distribution, which will usually be the case for failure times, the confidence limits on the MTBF (or $1/\lambda$), are calculated using the χ^2 (Chi-square) distribution. The formulae that are used are as follows:

For an upper confidence limit on a MTBF:

$$\theta \leq \frac{2T}{\chi^2 \alpha, (2n)}$$

For a 50% confidence limit on a MTBF:

$$\theta \leq \frac{2T}{\chi^2 \alpha, (2n+1)}$$

For a lower confidence limit on a MTBF:

$$\theta \leq \frac{2T}{\chi^2 \alpha, (2n+2)}$$

where:
- θ = the value of the confidence limit
- T = the total observed time
- χ^2 = the χ^2 value taken from tables (e.g., Table A-1), at probability α and either (2n) or (2n+2) degrees of freedom
- α = the specified confidence value
- n = the number of observed failures.

These expressions have another useful application. Where highly reliable components are used, and the population of such components is small, the chances of observing failures over a relatively short time span is also small. Thus the expression for a lower confidence limit is often used to obtain a median estimate of a MTBF or a failure rate by using the χ^2 value for 50% probability and 2 degrees of freedom.

Consider this example. There are 123 two inch isolating valves in a plant. Over 7 years of observations, 17 failures of these valves have been observed.

The total time observed is 123 * 7 = 861 component years.

MTBF = 861/17 = 50.64 years

λ = 1/MTBF = 1/50.64 = 1.97E-02 failures/year

For the 90% upper confidence limit χ^2 at 90% and 34 d.f.

= 23.95226

Therefore UCL = $\frac{861 * 2}{23.95226}$ = 71.89 years.

For the 10% lower confidence limit χ^2 at 10% and 36 d.f.

= 47.21216

Therefore LCL = $\frac{861 * 2}{47.21216}$ = 36.47 years.

Since λ = 1/MTBF the UCL for the MTBF becomes the LCL for the failure rate, and vice versa.

Therefore UCL = $\frac{1}{36.47}$ = 2.74E-2 f/yr

and LCL = $\frac{1}{71.89}$ = 1.39E-2 f/yr

If zero failures have been observed then χ^2 for 50% and 2 d.f.

= 1.38629 (Table A-1)

Median estimate MTBF = $\frac{861*2}{1.38629}$ = 1242.16 years

Failure rate = 8.05E-4 f/yr.

Table A-1
χ^2 versus n, Q; n = 1 - 30, Q = 0.95, 0.50, 0.05

	95%	90%	50%	10%	5%
Q	9.500E-01	9.000E-01	5.000E-01	1.000E-1	5.000E-02
n					
1	.00393	.0158	.45493	2.706	3.841
2	.10259	.211	1.38629	4.605	5.991
3	.35163	.584	2.36597	6.251	7.815
4	.71072	1.064	3.35669	7.779	9.488
5	1.14548	1.610	4.35145	9.236	11.070
6	1.63539	2.204	5.34812	10.645	12.592
7	2.16735	2.833	6.34580	12.017	14.067
8	2.73261	3.490	7.34412	13.362	15.507
9	3.32512	4.168	8.34283	14.684	16.919
10	3.94030	4.865	9.34182	15.987	18.307
11	4.57481	5.578	10.34009	17.275	19.675
12	5.22604	6.304	11.34032	18.549	21.026
13	5.89186	7.042	12.33975	19.812	22.362
14	6.57064	7.790	13.33927	21.064	23.685
15	7.26094	8.547	14.339	22.307	24.996
16	7.96185	9.312	15.33850	23.542	26.296
17	8.67176	10.085	16.33817	24.769	27.587
18	9.39046	10.865	17.33790	25.989	28.869
19	10.11702	11.651	18.33764	27.204	30.144
20	10.85003	12.443	19.33743	28.412	31.410
21	11.501	13.240	20.337	29.615	32.671
22	12.33802	14.041	21.33704	30.813	33.924
23	13.091	14.848	22.337	32.007	35.172
24	13.84843	15.659	23.33673	33.196	36.415
25	14.611	16.473	24.337	34.382	37.652
26	15.37918	17.292	25.33646	35.563	38.885
27	16.151	18.114	26.336	36.741	40.113
28	16.92789	18.939	27.33623	37.916	41.337
29	17.708	19.768	28.336	39.087	42.557
30	18.49253	20.599	29.33603	40.256	43.773

A.2 Plant Success States

A.2.1 Description of Success States

Stable plant success states are achieved when the plant is shown to be in a safe shutdown condition (fuel cooling is maintained) with no radionuclide releases for the entire duration of the accident repair time (see Section A.2.2).

Event sequences which end in a success state are labelled ”S”. The following cases involving various stages of heat transport system cooldown via the heat transport pumps, thermosyphoning or the shutdown cooling system (SDC), have been identified. These success states and their conditions are described below.

A.2.1.1 Forced Flow with Full HTS Inventory

The conditions for this success state are summarized below:

a) Heat transport system pumps are available.

b) Heat transport system coolant is circulated by heat transport pumps.

c) Decay heat is transferred to at least two steam generators from the HTS loop (CANDU 9) or to at least one steam generator per HTS loop (CANDU 6).

d) Steam generator water is supplied by either the main feedwater (MFW) or auxiliary feedwater (AFW) pumps or the emergency water supply (EWS) system for CANDU 6. For CANDU 9, water may be supplied from MFW, AFW or by the group 2 feedwater or reserve water systems.

A.2.1.1.1 Thermosyphoning Flow with Full HTS Inventory

The conditions for this success state are summarized below:

a) Heat transport pumps are not available.

b) Heat transport system coolant is circulated by thermosyphoning (natural circulation).

c) Decay heat is transferred to at least two steam generators from the HTS loop (CANDU 9) or to at least one steam generator per HTS loop (CANDU 6).

d) Steam generator water is supplied by either the main feedwater (MFW) or auxiliary feedwater (AFW) pumps or the emergency water supply (EWS) system for CANDU 6. For CANDU 9, water may be supplied from MFW, AFW or by the group 2 feedwater or reserve water systems.

A.2.1.2 Thermosyphoning with Partial Inventory

In some cases the liquid relief valves (LRVs) may open spuriously or may open due to high heat transport system pressure, and fail stuck open. The HTS inventory is discharged into the degasser or bleed condenser, causing the temperature of the outflow from the condenser to increase. When the temperature exceeds a certain setpoint, a signal is sent to isolate the condenser by closing certain level control valves. Once the condenser is filled up, no further inventory is discharged to the condenser and no more HTS inventory is lost.

As a result of the event, a part of the HTS inventory is located in the degasser condenser. When the inventory transfer is not made up, the heat transport pumps are not guaranteed to run in the long term due to a possibility of cavitation. The operator then trips the heat transport pumps. In this case the HT flow is maintained by thermosyphoning with partial inventory.

The conditions for the success state are:

a) Heat transport pumps cannot run due to partial loss of inventory.

b) Heat transport system coolant is circulated by thermosyphoning (natural circulation).

c) Decay heat is transferred to all steam generators from the HTS loop (CANDU 9) or to both steam generators in each HTS loop (CANDU 6).

d) Steam generator water is supplied by either the main feedwater (MFW) or auxiliary feedwater (AFW) pumps or the emergency water supply (EWS) system for CANDU 6. For CANDU 9, water may be supplied from MFW, AFW or by the group 2 feedwater or reserve water systems.

A.2.1.3 Shutdown Cooling Operation

When shutdown cooling is the heat sink, there are two modes of operation. One is “shutdown cooling operation with heat transport pumps” and the other is “shutdown cooling operation with shutdown cooling pumps.” The latter is further sub-divided into the following two states:

a) Heat transport system is cold, depressurized and full, and

b) Heat transport system is cold, depressurized and drained to the headers.

These modes and states are discussed below.

A.2.1.3.1 Shutdown Cooling Operation with Heat Transport Pumps

The conditions for this success state are summarized below:

a) The heat transport system is full and pressurized (4 to 9 MPa)

b) Heat transport system and shutdown cooling system are inter-connected.

c) Flow is maintained by means of the heat transport pumps.

d) Decay heat is transferred to shutdown cooling heat exchangers.

A.2.1.3.2 Shutdown Cooling Operation with HTS Cold, Depressurized and Full

In this success state the HTS is cold, depressurized and full. The conditions for this state are summarized below:

a) The heat transport system (HTS) is cold, depressurized and full.

b) Heat transport system and shutdown cooling system are inter-connected.

c) Flow is maintained by means of the shutdown cooling (SDC) pumps.

d) Decay heat is transferred via the shutdown cooling heat exchangers.

A.2.1.3.3 Shutdown Cooling Operation with HTS Cold, Depressurized and Drained

In this success state the HTS is cold, depressurized and drained to the headers. The conditions for this state are summarized below:

a) The heat transport system (HTS) is cold, depressurized and drained to at least the header level.

b) The heat transport and shutdown cooling systems are inter-connected.

c) Flow is maintained by the shutdown cooling (SDC) pumps.

d) Decay heat is transferred to the shutdown cooling heat exchangers.

A.2.2 Accident Repair Time And Success State Mission Time

The event tree success end-states are attained when the plant is in a safe shutdown state with no releases for the entire duration of the accident repair time.

The accident repair time is defined as the time required to gain access to the failed process system, and return it to a functioning state together with any other required equipment that was subsequently affected.

In the normal cooldown operation, phase 1 cooldown (260^{o}C to 1149^{o}C) usually takes about 40 minutes, phase 2 cooldown (149^{o}C to 82^{o}C) about 80 minutes, and phase 3 cooldown (82^{o}C to 38^{o}C) about 4 to 5 hours. The HTS is then kept cool by the shutdown cooling (SDC) system until the plant can be returned to power operation.

The cooldown time is not the accident repair time. The accident repair time is the time required to recover from the initiating event, i.e., the time to repair the failed process system / equipment and any associated equipment which may have been affected during the event, until the plant is returned to full-power operation. In this case, the accident repair time can be quite long. In principle, the event tree should be terminated when the plant is in the safe shutdown condition for the duration of the accident repair time, however, the success state mission time is used for convenience to terminate the event tree.

In general, the success state mission time is selected using the following criteria:

a) If the accident repair time is quite long (several days, weeks, or months), and if a redundant system exists, then the mission time for the success state need not be taken as the full accident repair time. In such cases, the mission time for the success state may be taken as the repair time of the other system.

b) Even if the initiating event is successfully terminated in a relatively short period of time, the failure of any system which may have been affected is considered.

c) If a particular mitigating system is required to function, and no other redundant system exists to perform the same function, then the mission time for the system may be equal to the accident repair time. In most PSAs a 24 hour mission time may be used.

A.2.3 Success State and Mission Time

During the normal cooldown operation, once the phase 1 cooldown is completed (decay heat is removed by the steam generators, and feedwater is supplied to the steam generators), the operation is transferred to the shutdown cooling mode of operation. However, there are two cases where the fuel cooling mode is not transferred to the SDC operation:

a) The initiating event, e.g., failure of a process system, is successfully terminated during the phase 1 cooldown and the plant can return to the power operation, or

b) Shutdown cooling operation is unavailable, so the operator does not transfer to SDC mode and keeps the plant in the phase 1 operation mode.

In case (a), the accident repair time is very short. In case (b), the plant should remain in phase 1 cooldown mode by the time the initiating event is fixed and SDC (shutdown cooling) system is repaired. If the SDC system is not operable, the plant cannot return to power operation even if the initiating event is successfully terminated. The system (phase 1 cooldown) should continue to operate until the time the failed process system returns to a functioning condition, as well as the SDC system. The time is referred as the accident repair time.

Suppose the case that the accident repair time is quite long and the SDC system is not operable, and the feedwater continues to be supplied to the SGs but fails after the repair time of the SDC system. (The repair time might be the mission time of feedwater system). Even if the feedwater fails during the accident repair time (by definition, the accident repair time includes also the time required to return feedwater system to a functioning condition), group 2 feedwater would be available as a feedwater back-up, or the SDC system could be repaired. Then, the sequence could be terminated successfully.

In some cases, the phase 1 cooldown mode is completed normally and the cooldown operation proceeds to the next phase involving shutdown cooling (SDC) system operation. However, if the SDC system fails during the operation, then the operator returns to the phase 1 cooldown mode of operation. Cooldown of the heat transport system continues in the phase 1 cooldown mode at least until the time that the SDC system is repaired.

In the PSA, not every case is considered. It is assumed that if a success state is maintained for a mission, the event sequence is successfully terminated based on the assumption that there are many means available to terminate the event. The mission time should be sufficiently long to cover every case.

In our example, once the phase 1 cooldown operates during the mission time, the event sequence is terminated successfully without any releases. The following cases are covered:

a) Phase 1 cooldown mode is completed normally (within 40 minutes) and the cooldown operation proceeds to the next phase;

b) Phase 1 cooldown is completed normally but the SDC system is not available. The plant stays in the phase 1 cooldown mode. Once the phase 1 cooldown continues for the duration of the mission time, the SDC system can be repaired or other means could be available.

c) Phase 1 cooldown is completed normally and the operation is transferred to SDC system mode of operation, but SDC system fails and the operation is returned to the phase 1 cooldown mode. The SDC system could be repaired within the mission time of the phase 1 cooldown operation, or other means could be available.

A.3 Component Type and Boundary Description

In the Table A-2 below, the component type and boundary descriptions are shown.

Table A-2
Component Type and Boundary Description

Component	CT Code	Boundary Description
Absorber Rod	-	-
Accumulator	AC	The vessel including inlet and outlet up to the first flange or weld.
Actuator	AT	
Adjuster Rod	-	-
Air Conditioning Unit	ACU	Package unit includes compressor, evaporator, condenser, fan, filter, motor and associated control circuit as applicable for a self-contained unit.
Air Cooler	-	-
Air Dryer	-	-
Airlocks	AL	Airlock as a package unit includes the vessel proper, doors, seals, windows, self-contained air supplies and control circuits both electrical and pneumatic.
Airlock Doors	AD	
Airlock Door Hinge	ADH	

Component	CT Code	Boundary Description
Airlock Door Latch	ADL	
Airlock Mechanisms	AM	
Airlock Rupture Disc	ARD	
Airlock Seals	AS	Seal, including hose and fittings.
Airlock Window	ALW	
Alarm Units (Current, Trip Test, Etc.)	AU	Component, including all subcomponents but excluding electrical terminations. NB: The SDS2 Trip Test Alarm Unit includes the following components: 1. In-Core Amplifier and Trip Test Circuit 2. Dynamic Signal Compensator Circuit 3. Difference Signal Circuit 4. Alarm Unit
Amplifiers 1. Ion-Chamber - Includes Log N Rate / Output for SDS1/2 and RRS 2. In-Core Neutron Flux Detector for SDS1/2 and RRS 3. Isolation	AF	Component including all subcomponents and 24 Vdc supply. Includes relay output contacts. Excludes external cable terminations.
Analyser Analyser Indicator Switch	A	Component including all subcomponents
Annunciators	AN	Component including all subcomponents such as internal wiring, boards, switches and bulbs.
Battery	BY	Battery cells, interconnecting links and supporting structures. Does not include outgoing cables with their connections.
Board - Printed Circuit (DCC Computer)	B	Component itself, including all subcomponents on PCB. Failures due to loss of power supply are not included.

Component	CT Code	Boundary Description
Bus - Electrical	BU	Conductors complete with insulators, mounting hardware, supporting structures, bus transfer and spurious bus protection relays which can cause bus outages. Isolated phase buses include cooling equipment, associated controls and wiring.
Cable - Electrical	CAB	Complete cable with conduit where used but without terminations
Cable Electrical (High Voltage)	-	-
Cable Connector / Termination	CT	Component including all subcomponents
Card	-	-
Chassis	-	-
Chiller Unit	CHU	Package unit includes compressor, evaporator, condenser, motor and associated control circuit as applicable for a self-contained unit.
Circuit Breaker (Electrical)	CB	The circuit breaker proper complete with insulators, mounting hardware and supporting structure. Only breaker protection relay failures that cause the breaker to change state or that prevent the breaker from changing state are included. Does not include other relays, Class I DC control power, breaker disconnects or remote compressed air supplies.
Compensator	KQ	Component, including all subcomponents. Excludes cable terminations.
Compressor	CP	Includes contribution from motor failures. It does not include contribution from loss of power supply to the motor.
Computer (Station Control)	-	
Computer (Shutdown Systems)	-	
Computer Card (Printed Circuit Board - PCB)	-	
Computer PCB Chassis (DCC Computer)	CC	Printed Circuit Boards (Cards) are not included.

Component	CT Code	Boundary Description
Computer I/O (DCC Computer)	CD	Includes only individual AIs, AOs, DIs and DOs in the computer. Does not include remainder of components on the I/O boards, generic board faults or any other hardware faults in the computer.
Computer Memory Module (DCC Computer)	CM	
Computer Watchdog Timer (DCC / PDC)	CW	
Computer I/O (PDC Computer)	CX	Includes only individual AIs, AOs, DIs and DOs in the computer. Does not include remainder of components on the I/O boards, generic board faults or any other hardware faults in the computer.
Contactor	CN	
Control Absorber Rod / Unit	-	-
Controller	C	Component, including all subcomponents. Pneumatic controllers include fittings or flanges. Electronic controllers do not include external cable connections.
Cooler	-	
Damper	D	Damper includes all subcomponents of the damper and its actuator where applicable.
Demister (Moderator Cover Gas System)	DEM	
Digital Computer Controller	DCC	
Diode	DI	Includes component and electrical wiring from last termination point to the component. Does not include electrical terminations.
Direct Contact Cooler (Moderator Cover Gas System)	-	
Door	-	-
Dryer - Air (Heatless and Heat Regenerated)	DR	Includes receiver, heaters, and associated solenoid valves for alternating air flows between operating and regenerating modes.

Component	CT Code	Boundary Description
Duct	DU	
Expansion Joint	EJ	Component including all subcomponents and supports.
Fan	FA	Includes all fan components up to first inlet and outlet connections including bellows. It includes belts where applicable but does not include fan motor.
Fan / Motor Set	FMS	Includes all fan components up to first inlet and outlet connections, bellows, belts where applicable and the fan motor
Filters	F	Filter up to inlet and outlet connections including filter vessel itself as a pressure boundary component or any moveable filter media and its drive.
Flame Arrester	FL	
Fuse	FU	The complete fuse but does not include the fuseholder.
Gas Chromatograph (Moderator Cover Gas System)	-	
Gauge	-	
Generator - Diesel (Class III Standby / Emergency Power Supply)	GD	
Generator - Main Turbine / Generator	GT	Generator includes stator, rotor, hydrogen cooling and stator cooling as contained within the generator housing boundary.
Grid	GR	
Heater - Electric	HT	Includes heater assembly, element and control wiring.
Heat Exchanger Air Cooler	H	Vessel up to inlet and outlet nozzles including all subcomponents such as tube bundle, divider plates and baffles.
Hose - Flexible (Catenary Hoses for FH System)	HO	
Ignitor (Hydrogen)	IG	Component including all sub-components.
Indicator	I	Component including all subcomponents.

Component	CT Code	Boundary Description
Indicator - Electronic	-	
Ion Chamber Test Assembly	IY	The ion chamber including test shutter and shutter control wiring.
Instrument Tubing	IT	
Inverter	IN	Component, including all subcomponents as a self-contained unit.
Ladder Logic - Relay	LLR	
Local Air Coolers (LACs)	-	
Mechanism - Reactivity Control Rod	MX	Includes drive motor, clutch assembly, pulley, lost motion “dog” plates, gear box, etc. and any other portion of the drive mechanism. Excludes electrical cable terminations to mechanism, the control rod itself and the rod assembly.
Meters (Indicator - Electronic)	ME	Component including all subcomponents.
Module - Computer Memory	-	
Module - Reactivity Control Rod	M	Component, including all subcomponents. Excludes electrical cable terminations.
Motor	M	Component including all subcomponents.
Motor Control Centre	MCC	MCC includes all sub-components in the MCC starter control unit such as the contactor proper, the 600-120Vac control transformer, the ground fault detector, etc. It does not include the 600 V power circuit breaker and MCC bus and power and control fuses.
Motor Starter	MS	Includes all subcomponents inside the self-contained unit such as the contactor, control transformer, overload relay ground fault detector. It does not include the 600 V power circuit breaker or the power and control fuses.
Orifice	OR	Pressure boundary component.
Panel	PL	
Penetration - Mechanical (Piping)	PM	Component, including all subcomponents.

Component	CT Code	Boundary Description
Penetration - Electrical Cable	PE	Includes all subcomponents in this self-contained unit, except for the pigtail cables
Pipe	PI	Piping includes all pressure boundary components i.e. nozzles, fittings, valve bodies and bonnets and pump casing and bolting which form or join the pressure boundary.
Potentiometer Switching Module	PSM	Component, including all subcomponents. Excludes electrical terminations.
Power Supply	PS	Component, including all subcomponents. Excludes electrical terminations.
Primary Element / Sensor	E	Component, including all subcomponents up to the first fitting, flange where applicable. Does not include electrical connectors. Excludes the test shutter facility of the ion chambers.
Programmable Digital Comparator	PDC	Computer is considered to be a package unit consisting of keyboard, central processor, dynamis and static storage devices (e.g., tape, disk) and output devices (e.g., monitor and printer) and I/O boards. Individual AIs, AOs, DIs and DOs are not included.
Pump	P	Includes all intake and discharge piping associated with the pump and internals up to but excluding the flange or weld. It includes shaft / impeller driven lube oil pumps, but excludes auxiliary lube oil pumps. It does not include pump motor failures or electrical cable terminations to the motor.
Pushbuttons (See Switches - All Types)	SMP	Component including all subcomponents.
Reactor (Nuclear)	REN	
Recombination Unit	RC	Component including all subcomponents
Recorders	RR	Component including all subcomponents. Excludes electrical cable terminations.
Rectifiers	RF	Component including all subcomponents. Excludes electrical cable terminations.
Relay	R	Component including all subcomponents.
Resistors (Fixed and Variable)	RSF RSP	Component including all subcomponents.

Component	CT Code	Boundary Description
Rods - Reactivity Control	Rd	Includes control rod, push rod, cable, thimble and guide tube. Excludes drive / drop mechanism and rod control mechanism.
Rupture Disks	RU	Component including all subcomponents.
Screen (Travelling)	SC	Includes motor and all drive components, control circuits for auto operation and cleaning. Does *not* include the solenoid or pneumatic valves associated with back washing.
Seals	-	-
Sequencer - Class III Loads	SEQ	-
Signal Modifier	Y	Component, including all subcomponents. Excludes electrical cable terminations.
Strainer (All Types and Sizes Including Auto-Backwash Types)	ST	Includes motor, basket and associated C&I for solenoids which initiate and perform bach-washing. Does *not* include the solenoid or pneumatic valves associated with back-washing.
Switches - Pressure Indicating Switches Only	S	Component, including all subcomponents up to the first fitting, flange where applicable. Does not include electrical connectors.
Switches - All Types, Including Pressure Indicating	S	
Switches - Limit	S	
Tank	TK	Vessel including inlet and outlet up to the first flange or weld.
Timer - Watchdog	-	
Timer - Relay	-	
Transmitters - Process	T	Component including all subcomponents. Excludes electrical cable terminations.
Transformer	TX	Transformer includes coolers, cooling fans, bushings, current transformers, oil circulating pumps, water circulating pumps, and controls. It also includes protective devices supplied with the transformer such as gas detector and pressure relief devices. The tap changer is not included.
Transmission Lines	TL	-

Component	CT Code	Boundary Description
Valves	V	Motor Operated Valve: Includes contribution from motor, but not power supply to the motor operator. Includes contribution from failure of associated limit and torque switches. Pneumatic Valve: Includes contribution from actuator, but not air supply to the actuator. Includes contribution from failure of associated limit and torque switches.
Voltage Regulators	VR	

Table A-3
Component Failure Modes and Mechanisms

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Absorber Rod	See "Rod - Reactivity Control"	-	-	-
Accumulator	Fails (Any Failure Type) Rupture External Leak Internal Leak Low Pressure Unavailable Due to Maintenance Unavailable Due to Test	FF RU XL IL LP UM UT	Overpressure Wall Thinning Weld Diaphragm	The vessel including inlet and outlet up to the first flange or weld.
Actuator	Fails (Any Failure Type) Fails to Operate Spurious Operation External Leak Unavailable due to Maintenance Unavailable Due to Test	FF OP SP XL UM UT		
Adjuster Rod	See "Rod - Reactivity Control"	-	-	-
Air Conditioning Unit	Fails (Any Failure Type) Internal Leak External Leak Inadequate Heat Transfer Excessive Heat Transfer Fails to Start	FF IL XL HI HE FS	Tube Leak Control Circuit Compressor Fan Blocked Filter Valve Belt Refrigerant Fitting Motor Expansion Joint	Package unit includes compressor, evaporator, condenser, fan, filter, motor and associated control circuit as applicable for a self-contained unit.
Air Cooler	See "Heat Exchanger - Cooler"	-	-	-
Air Dryer	See "Dryer"	-	-	-

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Airlocks	Fails (Any Failure Type) Fails Closed (Fail to Open) Fails Open (Fail to Close) Fail to Equalize Slow to Operate Fail to Seal External Leak Fast Operation Unavailable Due to Maintenance Unavailable Due to Test	FF FC FO SO SF XL - UM UT	Seal Inadequate Air Supply Door Mechanism Equalizing Mechanism Control Circuit Window Relief Valve Door Actuator	Airlock as a package unit includes the vessel proper, doors, seals, windows, self-contained air supplies and control circuits both electrical and pneumatic.
Airlock Doors	See Individual Airlock Components	-		
Airlock Door Hinge	Fails (Any Failure Type)	FF		
Airlock Door Latch	Fails (Any Failure Type) Fails Closed (Fails to Open) Fails Open (Fails to Close)	FF FC FO		
Airlock Mechanisms	Fails (Any Failure Type) Fails to Operate Slow Operation Spurious Operation Unavailable Due to Maintenance Unavailable Due to Test	FF OP SO SP UM UT		
Airlock Rupture Disc	Fails (Any Failure Type) Opens Spuriously	FF OS		
Airlock Seals	Fails (Any Failure Type) Fails to Deflate (Remains Inflated) Fails to Inflate (Remains Deflated) External Leak Fails to Seal Unavailable Due to Maintenance Unavailable Due to Test	FF RI RD XL SF UM UT	Bad Hose Connector Crack Deformed	Seal, including hose and fittings.
Airlock Window	Fails (Any Failure Type) External Leak Internal leak	FF XL IL		

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Alarm Units (Current, Trip Test, Etc.)	Fails (Any Failure Type) High Output Low Output No Output Erratic Output No Change in Output with Changing Input Spurious Trip Fails to Trip High Setpoint Setpoint Low Slow Operation Contacts Fail Closed Contacts Fail Open Open Circuit Unavailable Due to Maintenance Unavailable Due to Test	FF HO LO NO EO NC SP FT HS SL SO FC FO OC UM UT	Contacts Dirty Contacts Sticking Faulty Board Out of Calibration	Component, including all subcomponents but excluding electrical terminations. NB: The SDS2 Trip Test Alarm Unit includes the following components: 1. In-Core Amplifier and Trip Test Circuit 2. Dynamic Signal Compensator Circuit 3. Difference Signal Circuit 4. Alarm Unit
Amplifiers 1. Ion-Chamber - Includes Log N Rate/Output for SDS1/2 and RRS 2. In-Core Neutron Flux Detector for SDS1/2 and RRS 3. Isolation	Fails (Any Failure Type) High Output Low Output Erratic Output No Output No Change in output with changing input Open Circuit (Isolation Amp.) Unavailable due to Maintenance Power Supply (Hi Voltage) Loss Fails to Trip High Setpoint Spurious Trip	FF HO LO EO NO NC OC UM PS FT HS SP	Short Circuit Open Circuit Faulty Board Out of Calibration Power Supply	Component including all subcomponents and 24 Vdc supply. **Includes relay output contacts.** Excludes external cable terminations.

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Analyser Analyser Indicator Switch	Fails (Any Failure Type) High Output Low Output No Output Erratic Output Contacts Fail Closed (Fail to Open Contacts Fail Open (Fail to Close) Contacts Fail to Reopen Contacts Fail to Reclose Fails to Operate Contacts Open Spuriously Contacts Close Spuriously	FF HO LO NO EO FC FO OO CC OP OS CS	Contacts Burned Contacts Dirty Mechanical Failure Out of Calibration Wiring Fitting	Component including all subcomponents
Annunciators	Fails (Any Failure Type) Fail to Alarm Spurious Alarm	FF SP	Short Circuit Open Circuit Bulb Control Circuit	Component including all subcomponents such as internal wiring, boards, switches and bulbs.
Battery	Fails (Any Failure Type) No Output Low Output Unavailable due to Maintenance	FF NO LO UM	Short Circuit Open Circuit Bad Cell Corrosion	Battery cells, interconnecting links and supporting structures. Does not include outgoing cables with their connections.
Board - Printed Circuit (DCC Computer)	Fails (Any Failure Type)	FF	Circuit Failure Relay Coil	Component itself, including all subcomponents on PCB. Failures due to loss of power supply are not included.
Bus - Electrical	Fails (Any Failure Type) Open Circuit Short Circuit Short to Ground De-Energized Unavailable Due to Maintenance Unavailable Due to Test	FF OC SC SG DE UM UT	Insulation Breakdown Broken Conductor Fan Cooler Filter Protective Circuit Protective Relay	Conductors complete with insulators, mounting hardware, supporting structures, bus transfer and spurious bus protection relays which can cause bus outages. Isolated phase buses include cooling equipment, associated controls and wiring.

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Cable - Electrical	Fails (Any Failure Type) Open Circuit Short Circuit Unavailable due to Maintenance	FF OC SC UM	Insulation Breakdown Broken Conductor Conduit	Complete cable with conduit where used but without terminations
Cable Electrical (High Voltage)	See "Transmission Line"	-	-	-
Cable Connector/Termination	Fails (Any Failure Type) Open Circuit Short Circuit Short to Ground Unavailable due to Maintenance	FF OC SC SG UM	Loose contact Dirty Contact Shielding	Component including all subcomponents
Card	See - Board, Printed Circuit	-	-	-
Chassis	See - Computer, PCB Chassis	-	-	-
Chiller Unit	Fails (Any Failure Type) Forced Outage Internal Leak External Leak Inadequate Heat Transfer Excessive Heat Transfer Fails to Start Spurious Trip	FF FP IL XL HI HE FS SP	Tube Leak Control Circuit Compressor Refrigerant Fitting Motor Flange/Gasket	Package unit includes compressor, evaporator, condenser, motor and associated control circuit as applicable for a self-contained unit.

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Circuit Breaker (Electrical)	Fails (Any Failure Type) Fails Closed (Fails to Open) Fails Open (Fails to Close) Fails to Reopen Fails to Reclose Fails to Operate Opens Spuriously Closes Spuriously Slow Operation Noisy Unavailable Due to Maintenance Unavailable Due to Test Common Mode (For Two SF6 CBs with Common Protection Circuit)	FF FC FO OO CC OP OS CS SO NY UM UT CM	Contacts Stuck Open Contacts Stuck Closed Operating Mechanism Protective Circuit Control Circuit Short Circuit Open Circuit Spring Indicator	The circuit breaker proper complete with insulators, mounting hardware and supporting structure. Only breaker protection relay failures that cause the breaker to change state or that prevent the breaker from changing state are included. **Does not include other relays, Class I DC control power, breaker disconnects or remote compressed air supplies.**
Compensator	Fails (Any Failure Type) High Output Low Output No Output Erratic Output No Change in Output with Changing Input Unavailable due to Maintenance	FF HO LO NO EO NC UM	Faulty Board Open Circuit Out of Calibration Short Circuit	Component, including all subcomponents. Excludes cable terminations.
Compressor	Fails (Any Failure Type) Internal Leak External Leak Fails to Start Fails while Running Fails to Restart Low Output Contaminated Delivery Unavailable Due to Maintenance Unavailable Due to Test	FF IL XL FS FR RF LO CD UM UT	Control Circuit Internal Part Valve Cooling Belt Lubrication Flange/Gasket Fitting Unloader Filter	Includes contribution from motor failures. It does not include contribution from loss of power supply to the motor.
Computer (Station Control)	See - Digital Computer Controller (DCC)			

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Computer (Shutdown Systems)	See - Programmable Digital Comparator (PDC)			
Computer Card (Printed Circuit Board - PCB)	See - Boards, Printed Circuit			
Computer PCB Chassis (DCC Computer)	Fails (Any Failure Type)	FF		Printed Circuit Boards (Cards) are not included.
Computer I/O (DCC Computer)	Low Output High Output No Output Erratic Output No Change in Output with Changing Input Failure of NC Contacts to Open Failure of NO Contacts to Close Contacts Close Spuriously Contacts Open Spuriously Fails to Operate Spurious Operation Unavailable due to Maintenance	LO HO NSO EO NC FC FO CS OS OP SP UM	Loose Connection Faulty Board Opto-Isolator Out of Calibration Power Supply Relay	Includes only individual AIs, AOs, DIs and DOs in the computer. Does not include remainder of components on the I/O boards, generic board faults or any other hardware faults in the computer.
Computer Memory Module (DCC Computer)	Fails (Any Failure Type) Forced Outage	FF FP		
Computer Watchdog Timer (DCC/PDC)	Fails (Any Failure Type) Forced Outage	FF FP		

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Computer I/O (PDC Computer)	Low Output High Output No Output Erratic Output No Change in Output with Changing Input Failure of NC Contacts to Open Failure of NO Contacts to Close Contacts Close Spuriously Contacts Open Spuriously Fails to Operate Spurious Operation Unavailable due to Maintenance	LO HO NO EO NC FC FO CS OS OP SP UM	Loose Connection Faulty Board Opto-Isolator Out of Calibration Power Supply Relay	Includes only individual AIs, AOs, DIs and DOs in the computer. Does not include remainder of components on the I/O boards, generic board faults or any other hardware faults in the computer.
Contactor	Fails (Any Failure Type) Fails to Reclose (Remains Open) Closes Spuriously Fails Closed (Fails to Open) Fails Open (Fails to Close) Forced Outage Opens Spuriously Fails to Reopen (Remains Closed) Short Circuit (Coil)	FF CC CS FC FO FP OS OO SC		
Control Absorber Rod/Unit	See “Rod - Reactivity Control”	-	-	-
Controller	Fails (Any Failure Type) High Output Low Output No Output No Change in Output with High Setpoint Setpoint Low Unavailable due to Maintenance	FF HO LO NO NC HS SL UM	Bad Connection Dirty Faulty Board Fitting Fuse Internal Part Out of Calibration Position Indicator	Component, including all subcomponents. Pneumatic controllers include fittings or flanges. Electronic controllers do not include external cable connections.
Cooler	See - Heat Exchanger			

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Damper	Fails (Any Failure Type) Fails Closed (Fails to Open) Fails Open (Fails to Close) Internal Leak External Leak Closes Spuriously Opens Spuriously Unavailable due to Maintenance Unavailable Due to Test	FF FC FO IL XL CS OS UM UT	Blade/Disc Sliding Surface Corroded Bearing Wear/Corrosion Actuator Control Circuit Linkage	Damper includes all subcomponents of the damper and its actuator where applicable.
Demister (Moderator Cover Gas System)	Fails (Any Failure Type)	FF		
Diesel Generator	See “Generator - Diesel”			
Digital Computer Controller	Fails (Any Failure Type)	FF	CPU Storage Device Program error Faulty Board	
Diode	Fails (Any Failure Type) Open Circuit Short Circuit Unavailable Due to Maintenance	FF OC SC UM	Faulty Connection Overheat	Includes component and electrical wiring from last termination point to the component. Does not include electrical terminations.
Direct Contact Cooler (Moderator Cover Gas System)	See - Tanks, All Types and Sizes			
Door	See “Airlock Door”	-	-	-

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Dryer - Air (Heatless and Heat Regenerated)	Fails (Any Failure Type) External Leak Low Flow No Flow High Humidity Low Humidity Fail to Regenerate Regenerate Continuously Unavailable Due to Maintenance Unavailable Due to Test	FF XL LO NO - - - - UM UT	Dessicant Deteriorated Heater Element Control Circuit Solenoid Valve Fitting	Includes receiver, heaters, and associated solenoid valves for alternating air flows between operating and regenerating modes.
Duct	Fails (Any Failure Type) External Leak Low Flow	FF XL LO		
Expansion Joint	Fails (Any Failure Type) External Leak No Flow Low Flow Unavailable due to Maintenance	FF XL NO LO UM	Fatigue Wear Support Bellows Flange/Gasket	Component including all subcomponents and supports.
Fan	Fails (Any Failure Type) External Leak Fails to Start Fails while Running Fails to Restart High Vibration Low Output/Flow Noisy Unavailable Due to Maintenance Unavailable Due to Test	FF XL FS FR RF HV LO NY UM UT	Belt Blade Bearing Control Circuit Expansion Joint	Includes all fan components up to first inlet and outlet connections including bellows. It includes belts where applicable **but does not include fan motor**
Fan/Motor Set	Fails (Any Failure Type) Fails to Start Fails While Running Fails Low Output/Flow	FF FS FR LO		Includes all fan components up to first inlet and outlet connections, bellows, belts where applicable and **the fan motor**

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Filters	Fails (Any Failure Type) High Output Low Output No Output External Leak High Differential Pressure Unavailable Due to Maintenance Unavailable Due to Test	FF HO LO NO XL DP UM UT	Medium Plugged Medium Deteriorated Casing Control Circuit Drive Mechanism Fitting Heater Flange/Gasket	Filter up to inlet and outlet connections including filter vessel itself as a pressure boundary component or any moveable filter media and its drive.
Flame Arrester	Fails (Any Failure Type)	FF		
Fuse	Fails (Any Failure Type) Slow Operation (Slow to Blow) Short Circuit Open Circuit Unavailable Due to Maintenance	FF SO SC OC UM	Link Melted Fuse Holder	The complete fuse but does **not** include the fuseholder.
Gas Chromatograph (Moderator Cover Gas System)	See - Analyser, Gas with Indicator Switch			
Gauge	See “Indicator”			
Generator - Diesel (Class III Standby/Emergency Power Supply)	Fails (Any Failure Type) Fails While Running Fails to Start	FF FR FS		
Generator - Main Turbine/Generator	Fails (Any Failure Type) Fails (Forced Outage) High Vibration External Leak Internal Leak Unavailable Due to Maintenance Unavailable Due to Testing	FF FP HV XL IL UM UT	Winding Short Circuit Winding Open Circuit Seal Stator Cooling Bearing Lubrication Protective Circuit Flange/Gasket	Generator includes stator, rotor, hydrogen cooling and stator cooling as contained within the generator housing boundary.
Grid	Fails (Any Failure Type) Fails (Forced Outage)	FF FP		

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Heater - Electric	Fails (Any Failure Type) High Output Low Output No Output Unavailable Due to Maintenance Unavailable Due to Testing Fails While Running Fails to Start Fails Short Circuit	FF HO LO NO UM UT FR FS SC	Bad Connection Control Circuit Fan/Motor Fitting Flange/Gasket Thermostat Tube Bundle/Coil	Includes heater assembly, element and control wiring.
Heat Exchanger Air Cooler	Fails (Any Failure Type) High Output (High Flow) Low Output (Low Flow) No Output (No Flow) Inadequate Heat Transfer Excessive Heat Transfer Internal Leak External Leak Unavailable Due to Maintenance Unavailable Due to Testing	FF HO LO NO HI HE IL XL UM UT	Vibration Fretting Corrosion Erosion Silt/Crud Tube Flange/Gasket Fitting	Vessel up to inlet and outlet nozzles including all subcomponents such as tube bundle, divider plates and baffles.
Hose - Flexible (Catenary Hoses for FH System)	Fails (Any Failure Type) External Leak No Flow Low Flow	FF XL NF LO		
Igniter (Hydrogen)	Fails (Any Failure Type) Fails to Ignite	FF	Fuse Internal Part Control Circuit	Component including all sub-components.

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Indicator	Fails (Any Failure Type) High Indication Low Indication No Change in Output with Changing Input No Indication Erratic Indication External Leak Open Circuit Unavailable due to Maintenance EMI's Only: Fails to Operate Spurious operation	FF HO LO NC NO EO XL OC UM OP SP	Short Circuit Open Circuit Internal Part Out of Calibration Plugged Inlet Glass Fitting Wiring Flange/Gasket Bulb	Component including all subcomponents.
Indicator - Electronic	See - "Meters"			
Ion Chamber Test Assembly	Fails (Any Failure Type) Erratic Operation Fails to Operate Slow Operation Spurious Operation Unavailable due to Maintenance	FF EO OP SO SP UM	Faulty Connection Seal Shutter Pin Deformed Assembly	The ion chamber including test shutter and shutter control wiring.
Instrument Tubing	No Data			
Inverter	Fails (Any Failure Type) No Output Low Output Short Circuit Open Circuit Erratic Output Spurious Trip Unavailable Due to Maintenance	FF NO LO SC OC EO SP UM	Control Circuit Internal Part	Component, including all subcomponents as a self-contained unit.

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Ladder Logic - Relay	Fails (Any Failure Type) Closes Spuriously Fails Closed Forced Outage Fails Open Opens Spuriously	FF CS FC FP FO OS		
Local Air Coolers (LACs)	See - Heat Exchanger, Cooler	-		
Mechanism - Reactivity Control Rod	Fails (Any Failure Type) Drops Rod Spuriously Withdraws Rod Spuriously Fails to Drop Rod Drops Rod Too Slowly Drops Rod Partially Overtravels on Rod Drop Drops Rod too Quickly Fails to Withdraw Rod Unavailable due to Maintenance	FF DS WS FD SD PD OD DQ FW UM	Clutch Gearbox Internal Part Lost Motion Plates Pulley Shaft Spyroid Gear	Includes drive motor, clutch assembly, pulley, lost motion “dog” plates, gear box, etc. and any other portion of the drive mechanism. Excludes electrical cable terminations to mechanism, the control rod itself and the rod assembly.
Meters (Indicator - Electronic)	Fails (Any Failure Type) High Indication Low Indication No Change in Output with Changing Input No Indication Erratic Indication External Leak Open Circuit Unavailable due to Maintenance EMI’s Only: Fails to Operate Spurious operation	FF HO LO NC NO EO XL OC UM OP SP	Short Circuit Open Circuit Internal Part Out of Calibration Plugged Inlet Glass Fitting Wiring Flange/Gasket Bulb	Component including all subcomponents.
Module - Computer Memory	See - Computer Module			

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Module - Reactivity Control Rod	Fails (Any Failure Type) High Output Low Output No Output Erratic Output Fail to Reset/Repoise Fail to Trip Fails to Operate Spurious Output Unavailable due to Maintenance	FF HO LO NO EO RP FT OP SP UM	Faulty Board Relay Test Circuit	Component, including all subcomponents. Excludes electrical cable terminations.
Motor	Fails (Any Failure Type) Fails to Start Fails while Running Fails to Restart Fails to Stop Short Circuit Unavailable Due to Maintenance Unavailable Due to Test	FF FS FR RF SS SC UM UT	Winding Bearing Insulation Slip Rings/Brushes Dirty Mechanical Failure Protective Circuit Cooler Flange/Gasket	Component including all subcomponents.
Motor Control Centre	Fails (All Modes) Short Circuit Open Circuit Short to Ground Door Fails to Operate	FF SC OC SG DF	Contactor Control Transformer Ground Fault Operating Mechanism Overload Relay Control Circuit Open Circuit Short Circuit Insulation Breakdown Broken Conductor Failed Connector Hinge/Latch	MCC includes all sub-components in the MCC starter control unit such as the contactor proper, the 600-120Vac control transformer, the ground fault detector, etc. **It does not include the 600 V power circuit breaker and MCC bus and power and control fuses.**

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Motor Starter	Fails (Any Failure Type) Fails Closed (Fail to Open) Fails Open (Fail to Close) Fails to Reopen Fails to Reclose Fails to Operate Opens Spuriously Closes Spuriously Unavailable Due to Maintenance Unavailable Due to Test	FF FC FO OO CC OP OS CS UM UT	Contactor Control Transformer Ground Fault Operating Mechanism Overload Relay Control Circuit Open Circuit Short Circuit	Includes all subcomponents inside the self-contained unit such as the contactor, control transformer, overload relay ground fault detector. **It does not include the 600 V power circuit breaker or the power and control fuses.**
Nuclear Generating Station	Trip (Reactor + T/G Trip)	TR		
Orifice	Fails (Any Failure Type) High Output (High Flow) Low Output (Low Flow) No Output (No Flow) External Leak	FF HO LO NO XL	Plugged Worn Flange/Gasket Fitting	Pressure boundary component.
Panel	Fails (Any Failure Type) Forced Outage	FF FP		
Penetration - Mechanical (Piping)	Fails (Any Failure Type) External Leak	FF XL	Seal	Component, including all subcomponents.
Penetration - Electrical Cable	Fails (Any Failure Type) External Leak	FF XL	Seal	Includes all subcomponents in this self-contained unit, except for the pigtail cables
Pipe	Fails (Any Failure Type) Rupture External Leak No Flow Low Flow Unavailable Due to Maintenance	FF RU XL NF LO UM	Corrosion Erosion Fretting Support Overpressure Plugged Fitting	Piping includes all pressure boundary components i.e. nozzles, fittings, valve bodies and bonnets and pump casing and bolting which form or join the pressure boundary.

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Potentiometer Switching Module	Fails (Any Failure Type) High Output Low Output Erratic Output No Output No Change in Output with Changing Input Contacts Fail Closed Contacts Fail Open Open Circuit Short Circuit Fails to Operate Spurious Operation Unavailable Due to Maintenance Unavailable Due to Test	FF HO LO EO NO NC FC FO OC SC OP SP UM UT	Faulty Board Potentiometer Relay	Component, including all subcomponents. Excludes electrical terminations.
Power Supply	Fails (Any Failure Type) High Output Low Output Erratic Output No Output Unavailable due to Maintenance Short Circuit Open Circuit	FF HO LO EO NO UM SC OC	Short Circuit Open Circuit Fuse Wiring Out of Calibration Faulty Board Fan Transformer	Component, including all subcomponents. Excludes electrical terminations.

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Primary Element/Sensor	Fails (Any Failure Type) High Output Low Output Erratic Output No Output No Change in Output with Changing Input Slow Operation Internal Leak External Leak Unavailable due to Maintenance Unavailable due to Test	FF HO LO EO NO NC SO IL XL UM UT	Faulty Conductor Dirty Emitter Fitting Flange/Gasket Inadequate Charge Insulation Breakdown Internal Part Open Circuit Out of Calibration Plugged Sheath	Component, including all subcomponents up to the first fitting, flange where applicable. Does not include electrical connectors. Excludes the test shutter facility of the ion chambers.
Programmable Digital Comparator	Fails (Any Failure Type) Gross Failure Watchdog Parameter problems Software problems Hardware problems Digital Output problem Digital Input problem Analogue Output problems Analogue Input problems Failure to Transfer Unavailable due to Maintenance	FF GF WP SW HW DO DI AO AI FX UM	CPU Storage Device Program Error Faulty Board Keyboard Monitor/Printer Input/Output Device Loose Connection Power Supply	Computer is considered to be a package unit consisting of keyboard, central processor, dynamics and static storage devices (e.g., tape, disk) and output devices (e.g., monitor and printer) and I/O boards. **Individual AIs, AOs, DIs and DOs are not included**.

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Pump	Fails (Any Failure Type) Fails to Start Fails to Restart Fails While Running External Leak Internal Leak Low Output High Output No Output Erratic Output Unavailable Due to Maintenance Unavailable Due to Test	FF FS RF FR XL IL LO HO NO EO UM UT	Control Circuit Impeller/Diaphragm Seal Bearing Drive Mechanism Valve Flange/Gasket Casing Fitting Cooling Lubrication Gas Lock	Includes all intake and discharge piping associated with the pump and internals up to but **excluding** the flange or weld. It includes shaft/impeller driven lube oil pumps, but **excludes** auxiliary lube oil pumps. It does **not** include pump motor failures or electrical cable terminations to the motor.
Pushbuttons (See Switches - All Types)	Fails (Any Failure Type) Contacts Fail Closed (Fail to Open Contacts Fail Open (Fail to Close) Contacts Fail to Reopen Contacts Fail to Reclose Fails to Operate Contacts Open Spuriously Contacts Close Spuriously	FF FC FO OO CC OP OS CS	Dirty Contacts Dirty Bulb Short Circuit Open Circuit	Component including all subcomponents.
Reactor (Nuclear)	Trip (Reactor Trip Due to Other Than Initiating Events)	TR		
Recombination Unit	Fails (Any Failure Type)	FF	Low Gas Pressure	Component including all subcomponents
Recorders	Fails (Any Failure Type) High Output Low Output No Output Erratic Output No Change in output with changing input	FF HO LO NO EO NC	Ink Cartridge Paper Drive Pen Faulty Board	Component including all subcomponents. Excludes electrical cable terminations.

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Rectifiers	Fails (Any Failure Type) No Output Low Output Erratic Output High Output	FF NO LO EO HO	Short Circuit Open Circuit Control Circuit Protective Circuit Fan Out of Calibration	Component including all subcomponents. Excludes electrical cable terminations.
Relay	Relay Fails (Any Failure Type) Contacts Fail Open (Fail to Close) Contacts Fail Closed (Fail to Open) Contacts Fail to Reopen Contacts Fail to Reclose Coil Short Circuit Coil Open Circuit Slow Operation (Time Delay Relay) Contacts Close Spuriously Contacts Open Spuriously Unavailable due to Maintenance	FF FO FC OO CC SC OC SO CS OS UM	Contacts Dirty Contacts Sticking Coil Timer Short Circuit Open Circuit Indicator	Component including all subcomponents.
Resistors (Fixed and Variable)	Fails (Any Failure Type) High Output Low Output Erratic Output No Change in Output with Changing Input Open Circuit Short Circuit Unavailable due to Maintenance Fails to Operate (Pot. Only)	FF HO LO EO NC OC SC UM OP	Bad Ceramic Overheat Potentiometer Dial Tolerance Wiper	Component including all subcomponents.

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Rods - Reactivity Control	Fails (Any Failure Type) Drops Spuriously Withdraws Spuriously Fails to Drop Slow Drop Partial Drop Over-Travel on Rod Drop Quick Drop Fails to Withdraw Unavailable Due to Maintenance	FF DS WS FD SD PD OD DQ FW UM	Cable Control Rod Fitting Guide Tube Push Rod Seal Thimble	Includes control rod, push rod, cable, thimble and guide tube. Excludes drive/drop mechanism and rod control mechanism.
Rupture Disks	Fails (Any Failure Type) Rupture Internal Leak External Leak Unavailable due to Maintenance	FF RU IL XL UM	Diaphragm Punctured Diaphragm Corroded Flange/Gasket	Component including all subcomponents.
Screen (Travelling)	Fails (Any Failure Type) Fails While Running Fails to Start Low Flow Unavailable Due to Maintenance Unavailable Due to Test	FF FR FS LO UM UT	Control Circuit Motor Broken Chain Drive Mechanism Sprays Scraper Lower Housing	Includes motor and all drive components, control circuits for auto operation and cleaning. Does *not* include the solenoid or pneumatic valves associated with back washing.
Seals	See “Airlock Seals”	-	-	-
Sequencer - Class III Loads	Fails (Any Failure Type) Forced Outage	FF FP	-	-

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Signal Modifier	Fails (Any Failure Type) Erratic Output High Output Low Output No Output No Change in Output with Changing Input Unavailable due to Maintenance **Pneumatic relays only:** Fails to Operate Spurious Operation Setpoint High (Snap Acting Type) Setpoint Low (Snap Acting Type)	FF EO HO LO NO NC UM OP SP HS SL	Faulty Board Fitting Flange/Gasket Internal Part Open Circuit Out of Calibration Short Circuit	Component, including all subcomponents. Excludes electrical cable terminations.
Strainer (All Types and Sizes Including Auto-Backwash Types)	Fails (Any Failure Type Fails to Start High Delta P Low Flow No Flow High Flow External Leak Unavailable Due to Maintenance Unavailable Due to Test	FF FS DP LO NO HO XL UM UT	Shear Key Control Circuit Drive Mechanism Gland Packing Silt Load Motor	Includes motor, basket and associated C&I for solenoids which initiate and perform back-washing. Does *not* include the solenoid or pneumatic valves associated with back-washing.
Switches - Pressure Indicating Switches Only	Fails (Any Failure Type) High Output Low Output No Output No Change in output with changing input	FF HO LO NO NC	Bellows/Diaphragm Casing Contacts Dirty Contacts Sticking Fittings Dirty	Component, including all subcomponents up to the first fitting, flange where applicable. Does not include electrical connectors.

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Switches - All Types, Including Pressure Indicating	Fails (Any Failure Type) Erratic Operation Setpoint Low Setpoint High Contacts Fail Closed (fail to open) Contacts Fail Open (Fail to close) Contacts Fail to Reopen Contacts Fail to Reclose Slow Operation Fails to Operate Contacts Open Spuriously Contacts Close Spuriously External Leak Fails to Reset	FF EO SL HS FC FO OO CC SO OP OS CS XL RS	Flange/Gasket Internal Part Out of Calibration Reference Leg	
Switches - Limit	Fails (Any Failure Type) Fails to Operate Spurious Operation Fails to Operate Fails to Reset Erratic Operation	FF OP SP OP RS EO		
Tank	Fails (Any Failure Type) Rupture External Leak Outlet Blocked Inlet Blocked Unavailable Due to Maintenance Unavailable Due to Test	FF RU XL OB IB UM UT	Corrosion Wall Thinning Weld Overpressure Vacuum Flange/Gasket Internal Part	Vessel including inlet and outlet up to the first flange or weld.
Timer - Watchdog	See - Computer, Watchdog Timer			
Timer - Relay	See - Relay, Time Delay			

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Transmitters - Process	Fails (Any Failure Type) High Output Low Output No Output Erratic Output No Change in Output with Changing Input External Leak High Setpoint Low Setpoint Unavailable due to Maintenance	FF HO LO NO EO NC XL HS SL UM	Faulty Board Fitting Flange/Gasket Human Error Mechanical Failure Open Circuit Out of Calibration Reference Leg Short Circuit	Component including all subcomponents. Excludes electrical cable terminations.
Transformer	Fails (Any Failure Type) No Output Low Output High Output Open Circuit Short Circuit Overheated External Leak Gas Accumulation Unavailable Due to Maintenance	FF NO LO HO OC SC TO XL GA UM	Short Circuit Open Circuit Cooling Insulation Housing/Gasket Oil Level	Transformer includes coolers, cooling fans, bushings, current transformers, oil circulating pumps, water circulating pumps, and controls. It also includes protective devices supplied with the transformer such as gas detector and pressure relief devices. **The tap changer is not included.**
Transmission Lines	-	-	-	-
Travelling Screen	See “Screen”	-	-	-

Component	Failure Mode (FM) Description	FM Code	Failure Mechanisms	Boundary Description
Valves	Fails (All Modes) Fails Energized (Sol Valves) Fails De-Energized (Sol Valves Fails Pressurized (Pilot Valves) Fails De-Press (Pilot Valves) High Output Low Output No Output Fails Open (fail to close) Fails Closed (fail to open) Fail to Reopen Fail to Reclose Internal Leak External Leak Slow Operation Fails to Operate Spurious Operation Opens Spuriously Closes spuriously Diaphragm Rupture (Quick Exhaust Valves Only) Unavailable Due to Testing Unavailable Due to Maintenance	FF EN DE PR DE HO LO NO FO FC OO CC IL XL SO OP SP OS CS RU UT UM	Bellows/Diaphragm Body/Bonnet Fitting Flange/Gasket Gearbox Gland Packing Human Error Operating Mechanism Plug/Disc/Blade Position Indicator Seat Stem	**Motor Operated Valve:** Includes contribution from valve operator, but not from power supply to valve operator. Includes contribution from failure of associated limit and torque switches. **Pneumatic Valve:** Includes contribution from valve operator, but not air supply to valve operator. Includes contribution from failure of associated limit and torque switches.
Voltage Regulators				

Table A-4
Component Types and Failure Modes for Undeveloped Events

Component/System Description	Component Type Code	Failure Mode Description	Failure Mode Code
DCC Computers	DCC	Output Fails High	HO
		Output Fails Low	LO
Control and Instrumentation Signals to Components	C&I	Output Fails High	HO
		Output Fails Low	LO
Class III Diesel Generator - DG1	DG1	Fails to Start	FS
		Fails While Running	FR
Class III Diesel Generator - DG2	DG2	Fails to Start	FS
		Fails While Running	FR
Recirculated Cooling Water (RCW) System	RCW	No Pressure	NP
Raw Service Water (RSW) System	RSW	No Pressure	NP
Emergency Water Supply (EWS) System	EWS	No Pressure	NP
Heating, Ventilation and Air Conditioning (HVAC) System	HVA	Room Temp High	HT
Instrument Air Supply to active components	AIR	No Pressure	NP

Appendix B

Methodology for Seismic Fragility Analysis

B.1 Introduction

PSA is an analytical technique to determine severe core damage frequency of a nuclear power plant and risk to the public. In addition, PSA can be used to assess design options to optimize safety. There are many steps to be followed in performing a seismic PSA: determination of seismic hazard at the site, evaluation of seismic local ground motion, response of plant systems and components, fragility analysis of components and structures, accident sequence quantification and uncertainty and sensitivity analyses. The methodology for seismic PSA is detailed in the Section 7 of the main text.

B.1.1 Objectives and Scope

The objective of this appendix is to define the methodology for performing fragility analysis for CANDU nuclear power plants. The methodology is applicable to both CANDU 6 and CANDU 9 reactors. It is also applicable to all civil structures and components (mechanical, electrical…etc.) in the whole project i.e., NSSS, BNSP and BOP.

Fragility calculations for a structure or component require detailed knowledge of this item's capacity, material properties and response under seismic and static loading. Thus, various documents and drawings have to be available for an item before fragility parameters can be accurately calculated. The documents and drawings include: analysis reports, seismic analysis reports, stress analysis reports for different loads (e.g., seismic, thermal…), design calculations, general arrangement drawings and detailed drawings.

Following the introduction and description given in Section B.1, Section B.2 provides the basic formulation for calculating fragility of civil structures. Section B.3 focuses on equipment qualified by analysis, this is divided into: the primary heat transport system, the reactor, fuelling machine and electrical cable trays. Section B.4 deals with fragility of equipment qualified by testing. Relay chatter evaluation is presented in Section B-5. Finally, references used in the Appendix are given in Section B.6. Considerations for fragility calculations for other equipment (e.g. BNSP equipment, BOP equipment, tanks and their supports, etc…) are not included.

B.1.2 Fragility Description

Seismic fragility of a structure, or equipment, is defined as the conditional probability of its failure for a given level of seismic parameter, e.g., Peak Ground Acceleration (PGA). Seismic fragility is represented by a family of curves corresponding to the level of confidence in the parameter values and the model. Typically, the median fragility curve, the 95% confidence fragility curve and the 5% confidence fragility curve are used as shown in Figure B-1. Details

and methods for seismic fragility calculations are discussed in a number of references, for example NUREG-1407 (Reference B-1) and NUREG/CR-2300 (Reference B-2).

The entire fragility curve and its uncertainty is expressed as follows:

$$A = A_m \varepsilon_R \varepsilon_U \quad (1.1)$$

Where:

A = Seismic input parameter (e.g., ground acceleration) corresponding to any given frequency of failure.

A_m = Median seismic input parameter capacity (e.g., median ground acceleration capacity).

ε_R and ε_U = Random variables with unit median and logarithmic standard deviation β_R and β_U. ε_R and ε_U represent inherent randomness about the median and uncertainty in the median value, respectively.

The random variability β_R represents dispersion in the results, which cannot be reduced by gathering more data or more detailed analysis. It is due to the randomness in the earthquake time-history and in the response of the structure or equipment when the earthquake is represented by one input parameter like PGA. On the other hand, the uncertainty β_U, represents dispersion in the results due to inadequate knowledge, lack of data or insufficient analyses and test results. Examples are: predicting the exact strength of materials, the exact strength of structural components, inaccuracies in mass and stiffness modelling or using unrealistic load distributions.

The seismic input parameter, for which fragility of equipment and structures is developed, is chosen to be the peak ground acceleration (PGA) for the site in question. For most of the components analysed, it is sufficient to use the mean fragility curve described by A_m and β_m where β_m is equal to $(\beta_R^2+\beta_U^2)^{1/2}$. According to the fragility model and the parameters A_m, β_R and β_U for a given component, the probability of failure of that structure can be computed for any given PGA value.

A commonly used value, which describes the seismic capacity of a component or structure, is the High Confidence Low Probability Failure (HCLPF) value. It represents, with a 95% confidence, that the probability of failure of a component or structure will not exceed 5%. It is calculated by:

$$\text{HCLPF capacity} = A_m \exp[-1.65(\beta_R + \beta_U)] \quad (1.2)$$

The HCLPF gives a good indication of seismic capacity of a component or structure and also allows for screening of components and structures. This reduces the number of components and structures, which have to be included in the analysis. Normally, a screening value is selected and components with capacity above this are screened out.

As mentioned above, seismic fragility of a component or structure can be expressed in terms of the median ground acceleration A_m and random and uncertainty logarithmic standard deviations, β_R and β_u. However, for structures and equipment it is difficult to directly calculate those fragility parameters. Instead, an intermediate variable, called “factor of safety” (F_m), can be

defined. The factor of safety is defined as the ratio of the ground acceleration capacity to the Design Basis Earthquake (DBE) acceleration used in the design. Thus:

$$A_m = F_m.\ A_{DBE} \quad (1.3)$$

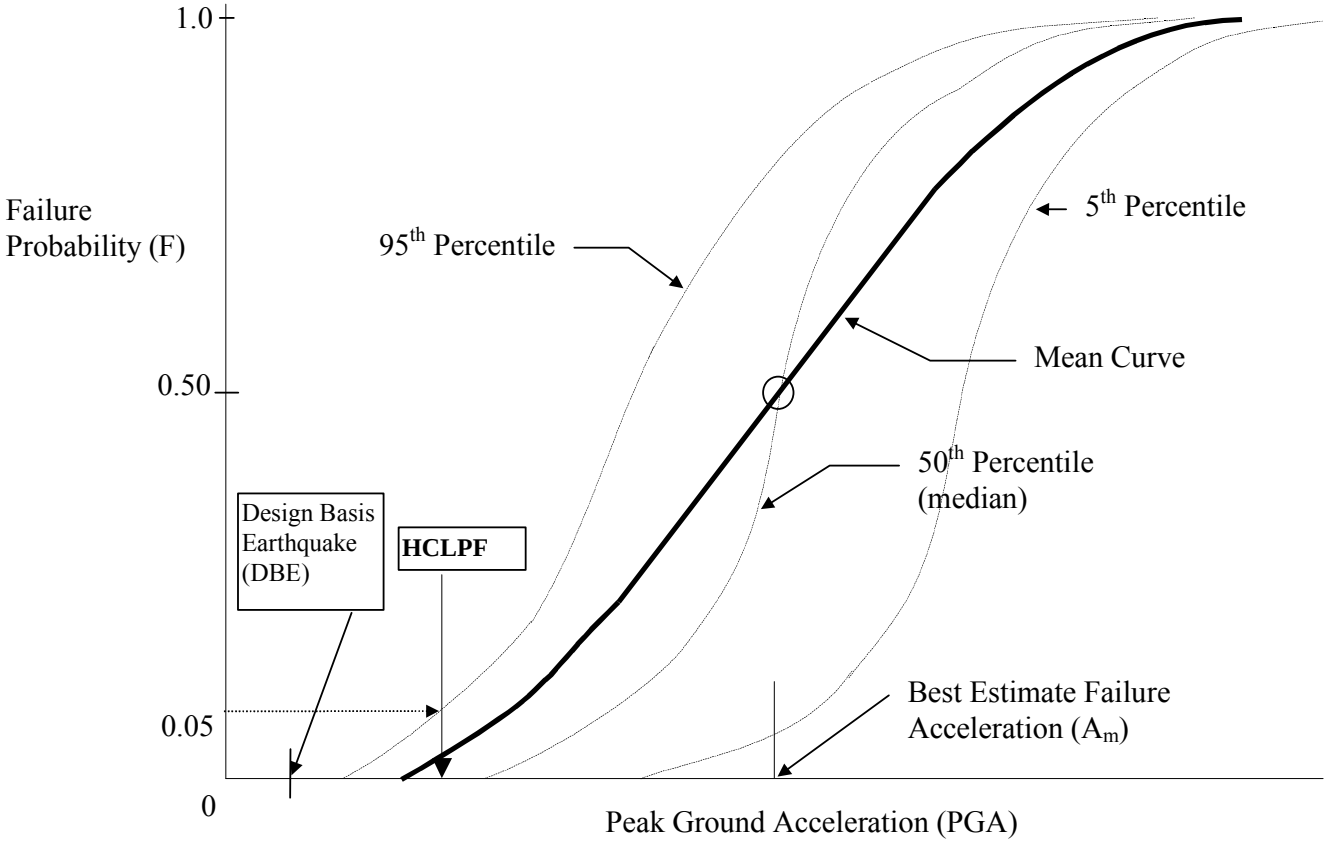
For equipment and structures analysed for DBE, the median factor of safety F_m and variability parameters β_R and β_U based upon DBE stress analysis can be easily computed. Thus the methodology used in this document for computing seismic fragility factors for structures and equipment is called "Factor of Safety Method". This method is also called by IAEA "Scaling Method" as mentioned in the IAEA-TECDOC-724 (Reference B-3). In some sections of the document other methods have been mentioned and used specifically for certain components.

Also it has been recognized that seismic walkdown at site is necessary to assist in fragility analysis of components and structures. Seismic walkdown methods have been detailed in seismic methodoldogy in Section 7 of the main text. Some of the important issues in a seismic walkdown, are:

- Define failure modes for structures and components not expected to have high seismic capacity.
- Observe and record any deficiencies (e.g., missing anchor bolts, excessive cracking of concrete that may reduce seismic capacity of a member….).
- Spatial interactions e.g., non-seismically qualified structures or components above or beside DBE qualified structures or components.

However, fragility calculations are not performed for every structure and component in a typical plant. Instead critical structures and components are selected for fragility analysis. Details of the selection process are given in Section 7 of the main text. For CANDU 9 a preliminary priority study for selection of seismic fragility analysis of structures and components is developed. The first step is to identify the Safe Shutdown Equipment List. These are the components necessary to perform safety functions. For each safety function, the safety system(s) must be identified and then the equipment necessary are listed. Structures housing safety equipment selected are also selected.

Finally, in a PSA analysis if a component has a small contribution to severe core damage frequency (SCDF), it can be screened out. The establishment of a screening criterion should be done by consultation with PSA analysts. Typically, a screening criterion may be selected from the hazard curve as the PGA corresponding to a yearly frequency of 10^{-5}. This PGA value should be compared with HCLPF values of selected structures and equipment in a sensitivity study. The sensitivity study confirms that the screening out of any structure or equipment doesn't significantly affect the SCDF. Also, screening criteria can be based on RLE (Review Level Earthquake). However a specific screening criterion should be determined for each project.



HCLPF is the abbreviation for a High Confidence (95%) of a Low Probability of Failure 5%)

Figure B-1 Fragility Curve

B.2 Civil Structures

B.2.1 Methodology

Several median factors of safety and variability parameters are computed for each design criteria utilized in the design of a structure. These can be grouped into two categories: seismic capacity factors (F_C) and building response factors (F_{RS}).

The seismic capacity factor can be further divided into:

- Strength factor**,** F_S, defined as the ratio of actual member strength to the design forces and logarithmic standard deviation associated with it, β_S.
- Inelastic energy absorption factor, F_μ, related to the ductility of the structure and logarithmic standard deviation associated with it β_μ.

$\therefore F_C = F_S.\ F_\mu$ (2.1)

Typically each logarithmic standard deviation is composed of both random part and uncertainty part and each part should be computed separately. Therefore the logarithmic standard deviation for capacity, β_C, is divided into:

$$\beta_{R,C} = (\beta_{R,S}^2+\beta_{R,\mu}^2)^{1/2} \quad (2.2)$$

Similarly

$$\beta_{U,C} = (\beta_{U,S}^2+\beta_{U,\mu}^2)^{1/2} \quad (2.3)$$

The factor of safety for the structure response, F_{RS} is composed of a number of factors:

- Spectral shape F_{SA}, difference in the response spectra used for design from a median spectrum for the site.
- Damping values F_D.
- Modelling accuracy F_M.
- Combination of modes F_{MC}.
- Combination of earthquake components F_{EC}.
- Method of analysis/testing also called horizontal earthquake direction factor, F_{ED}.
- Soil-Structure interaction F_{SSI}.

As before:

$$F_{RS} = F_{SA}.\ F_D.\ F_M.\ F_{MC}.\ F_{EC}.\ F_{ED}.\ F_{SSI} \quad (2.4)$$

$$\beta_{R,RS} = (\beta_{R,SA}^2 + \beta_{R,D}^2 + ...)^{1/2} \quad (2.5)$$

$$\beta_{U,RS} = (\beta_{U,SA}^2 + \beta_{U,D}^2 + ...)^{1/2} \quad (2.6)$$

The overall factor of safety:

$$\therefore F_m = F_C . F_{RS} \quad (2.7)$$

$$\beta_R = (\beta_{R,C}^2 + \beta_{R,RS}^2)^{1/2} \quad (2.8)$$

$$\beta_U = (\beta_{U,C}^2 + \beta_{U,RS}^2)^{1/2} \quad (2.9)$$

The median seismic capacity:

$$A_m = F_m . A_{DBE} \quad (1.3)$$

Thus median factor of safety and variability calculations are made for each of the parameters affecting capacity and response of a civil structure.

The failure of a structure is defined as a structural damage to the extent that operability of essential equipment cannot be relied on. Another definition of failure is loss of containment. In this section, the median parameters for selected civil structures of a typical CANDU plant are developed. The structures chosen for evaluation are selected because they house equipment essential for plant safety during or after a seismic event, or structures whose failure could result in failure of an essential structure or component. Structures that should be investigated are:

- Containment Structure
- Internal structure
- Reactor Vault
- Service Building
- Emergency Power Supply and Secondary Control Area Building
- Emergency Water Supply Building and Emergency Water Reservoir
- High Pressure Emergency Core Cooling Building
- Turbine Building
- Circulating Water Intake Structure and RSW intake.

Hence, the main steps for a structure seismic fragility analysis are as follows:

- Identify seismic load paths for the structure
- Examine dynamic models for the structure
- Determine failure modes for the structure
- Assess consequences of failure modes and identify critical modes.

B.2.1.1 Median Structure Capacity Factor

Capacity analysis is based on original analyses and test results, ultimate strength and ductility calculations and historical seismic performance of similar components. The primary load

carrying system of the structure has to be identified. Then the critical structural components of this system has to be examined (walls, slabs, columns, masonry block walls, foundations etc). Finally, the expected median capacities and associated variability of the various types of the load-carrying elements should be calculated.

The primary lateral load-carrying systems of the structures for a typical CANDU reactor are constructed from both structural steel and reinforced concrete. The containment structure, concrete internal structure, reactor vault and substructures of all safety related buildings, are all reinforced concrete. The containment structure is also post-tensioned by tendons. Superstructures of many buildings are constructed using braced steel frame or moment resisting frame structures e.g., service building, emergency power supply and secondary control area building, emergency water supply building, high pressure emergency core cooling building, turbine building and circulating water intake structure.

There are main differences between the modes of failure of steel structures versus reinforced concrete structures. For example, steel structures commonly fail as a result of buckling of a brace member or its tensile yield, failure of a bolted or welded connection, or column anchor bolts failure. Concrete structures exhibit different modes of failure; shear failure of cylindrical walls, local failures at interface locations and failure of block walls are few common examples.

There are also differences in the material properties between steel structures and reinforced concrete. Therefore, calculation of capacity factor for seismically qualified steel and seismically qualified concrete structures should take these differences into account. In the next section examples specific for steel structures and concrete structures will be given.

a) Strength Factor

   Strength factor F_s, can be evaluated as follows:

   F_S = (Median Capacity - NOL)/ Design Seismic Demand

   Where NOL is demand due to normal operating conditions or loads. Conservatism in the design seismic demand is normally accounted for in the structure response factors. On the other hand, median seismic demand (response) can be obtained from scaling of design analysis or probabilistic seismic response analysis. In that case, F_S can be given as:

   F_S = (Median Capacity - NOL)/ Median Seismic Demand

   It should also be noted that variability in modelling is predominantly considered all uncertainty and no randomness (i.e., $\beta = \beta_U$).

   Another parameter that affects structural members strength, is material properties. Material properties differ considerably between steel structures and concrete structures. Examples for both structures will be given in the next sections.

b) Structure Inelastic Energy Absorption

The seismic capacity of a structure can be evaluated more accurately if in addition to its strength capacity the inelastic energy absorption of the structure is also considered. The inelastic energy absorption factor F_μ can be evaluated using two methods:

1) Effective frequency/effective damping method
2) Effective Riddell-Newmark method (Reference B-4).

Both methods are to be employed and the average of the two values calculated should be used as the median inelastic energy absorption factor. Early studies indicated that F_μ is function of the ductility ratio, μ, which is defined as the ratio of maximum displacement to displacement at yield. Thus the factors affecting F_μ are:

- Median system ductility
- Frequency of the structure
- Duration of earthquake

Median ductility of a structure is defined by inelastic deformations at the onset of strength degradation of critical members. The deformation at failure is described in terms of story drift, which is the ratio of deformation divided by the element length.

Thus the first step to evaluate the factor of safety for inelastic energy absorption is to determine the median ductility corresponding to failure. For a multi-degree of freedom system the median system ductility is given by:

$$\mu = \Sigma W_i \Delta_{Ti} / \Sigma W_i \Delta_{ei} \quad (2.10)$$

where W_i = that portion of total weight of structure that is located at or assigned to level i (story i).

Δ_{Ti} = median maximum deflection of each story at ultimate capacity of the critical story.

Δ_{ei} = median elastic deflection of each story scaled to reach yield in the critical story.

1) Effective Frequency/Effective Damping Method

This method directly accounts for the following:

- Shape of the input ground motion
- Shifting of the dynamic frequency
- Effect of pinching of the hysteretic loops of concrete shear wall up to failure

Idealized bilinear force-deflection diagram for an elastic-perfectly plastic model is shown in Figure B-2. From the Figure B-2 it can be shown that:

$$V_c = K \delta_y \quad (2.11)$$

$$V_u = K \delta_y + sK. \ (\mu\text{-}1) \delta_y \quad (2.12)$$

$$V_u = K_s. \ \mu\delta_y \quad (2.13)$$

$\therefore K_s/K = [1+ s (\mu -1)]/\mu$ (2.14)

where

K = elastic stiffness or slope of force-deformation curve before yield of steel or extensive cracking of concrete.

sK = plastic stiffness or slope of force deformation curve beyond yield of steel or extensive cracking of concrete.

μ = Ductility ratio defined as the ratio of deformation at ultimate load to deformation at yield δ_y

K_s = secant stiffness.

V_c = Force at yield.

V_u = Ultimate force.

Step 1: the ratio of secant frequency to elastic frequency, f_s/f can be calculated as follows:

$$f_s/f = \sqrt{K_S/K} \quad (2.15)$$

Step 2: Ratio of effective frequency to elastic frequency, f_e/f is:

$f_e/f = (1-A) + A (f_s/f)$ (2.16)

Where

f_e = weighted average of secant and elastic frequencies.

$A = C_f [1- (f_s/f)] \leq 0.85$ (2.17)

$C_f = 2.3$ for strong ground motions with duration greater than 1 second.

Step 3: to calculate effective damping β_e:

$\beta_e = [(f_s/f)/(f_e/f)]. (\beta + \beta_h)$ (2.18)

where

β = elastic damping for structure

β_h = pinched hysteretic damping

$= 0.11 [1- (f_s/f)]$ (2.19)

Step 4: Determination of spectral acceleration $SA_{(f, \beta)}$ corresponding to elastic frequency, f and elastic damping, β. Determination of spectral acceleration $SA_{(fe,\beta e)}$ corresponding to effective frequency, f_e and effective damping, β_e.:

$\therefore F_\mu = [(f_e/f)/(f_s/f)]^2. (SA_{(f, \beta)}/SA_{(fe,\beta e)})$ (2.20)

2) Effective Riddell-Newmark Method

This method is developed from bilinear force deflection relationship. It is modified for post-yield force/deflection curve slope. It explicitly considers the effect of long duration ground motion. From Figure B-3 it can be shown that:

$V_c = K\,\delta_y$ (2.21)

$V_u = K\,\delta_y'$ (2.22)

$V_u = K\delta_y + sK.\ (\mu\text{-}1)\,\delta_y$ (2.23)

$\therefore K\,\delta_y' = K\delta_y + sK.\ (\mu\text{-}1)\,\delta_y$ (2.24)

$\delta_y' = R\delta_y$ (2.25)

where $R = 1 + s\,(\mu - 1)$ (2.26)

The pseudo elasto-plastic relationship shown in Figure B-3 is based on equal area and equal capacity.

$\therefore\ \mu' = 0.5 + [(\mu\text{-}1)(1+R)+1]/2R^2$ (2.27)

Rigid range

$F_{\mu 4} = [SA_{(f,\,\beta)}/PGA].\ (\mu')^{\alpha}$ (2.28)

Amplified acceleration range

$F_{\mu 3} = [(q_a + 1)\,\mu' - q_a\,]^{\gamma a}$ (2.29)

Amplified velocity range

$F_{\mu 2} = C_F\,[(q_v + 1)\,\mu' - q_v\,]^{\gamma v}$ (2.30)

where

$\alpha = 0.13$ for 10% damping

β = percentage of critical damping

$\gamma_a = 0.48\,\beta^{-0.08}$ (2.31)

$\gamma_v = 0.66\,\beta^{-0.04}$ (2.32)

$q_a = 3.0\,\beta^{-0.30}$ (2.33)

$q_v = 2.7\,\beta^{-0.40}$ (2.34)

$C_F = f_k/f$ when $f_k/f \le 1.0$

$= 1.0$ when $f_k/f \ge 1.0$

f_k = knuckle frequency between constant amplified spectral acceleration region and constant amplified spectral velocity region.

$F_{\mu 1}$ = smaller of $F_{\mu 3}$ and $F_{\mu 4}$ (2.35)

F_{μ}' = larger of $F_{\mu 1}$ and $F_{\mu 2}$ (2.36)

$$F_\mu = 1 + C_D (F_\mu' - 1) \quad (2.37)$$

Where $C_D = 0.6$ for long duration earthquakes

= 1.0 for small magnitude short duration event

For computation of logarithmic standard deviation of inelastic energy absorption factor, the following guidelines can be followed:

- Variability (randomness and uncertainty) associated with median story drift: $\beta_R = 0.15$ and $\beta_U = 0.3$
- Randomness of the predicted values by approximate methods

  $$\beta_R = 0.4 [0.06 + 0.03 (F_\mu - 1)] \quad (2.38)$$

- Uncertainty in the inelastic energy absorption model (modelling of hysteretic behaviour)

  $$\beta_U = C_U (F_\mu - 1) \quad (2.39)$$

  where $C_U = 0.05$ to 0.2

B.2.1.2 Median Structure Response Factor

a) Spectral Shape Factor

Median spectral shape factor, F_{SAm}, accounts for difference between design and median site-specific ground response spectrum. The comparison is carried out at dominant structure frequencies. The difference between design and median structure damping is also included in F_{SAm}.

$$\therefore F_{SAm} = SA_d/SA_m \quad (2.40)$$

where

SA_d = Spectral acceleration for design ground response spectrum and design damping.

SA_m = Spectral acceleration for median ground response spectrum and median damping.

b) Damping

As mentioned above, the difference between design and median structure damping is normally included in median spectral shape factor. Thus modelling factor F_D is typically equal 1.0. However, variability is calculated separately and is based on comparison of median and lower bound values from NUREG/CR-0098 (Reference B-6).

i.e. $$\beta = \ln (SA_d/SA_m) \quad (2.41)$$

For structures at or near yield, the following table applies:

Structure Type	Lower Bound %	Median %
Reinforced Concrete	7	10
Prestressed Concrete	7	10
Welded Steel	5	7
Bolted Steel	7	10

c) Modelling

Median modelling factor, F_M, accounts for accuracy of design analysis model. It can account for minor frequency shifts as follows:

$$F_M = SA_m\,(f=f_m)/SA_m\,(f=f_d) \qquad (2.42)$$

where

SA_m = Spectral acceleration for median ground spectrum.

f_m, f_d = median and design frequencies.

Design analysis model is generally considered to be median-centred; therefore F_M is typically equal to 1.0.

Variability in modelling is predominantly considered all uncertainty and is mainly due to the calculated mode shapes and modal frequencies. For concrete structures, the concrete compressive strength and stiffness is a function of the response of the structure and level of earthquake motion. At low and moderate levels of response, usually the stiffness of the structure is above the design values. Close to failure, concrete cracking occurs and the actual frequency of the structure is less than the design value based on uncracked section properties. For steel structures these uncertainties are less pronounced.

β_U of frequency typically ranges from 0.1 to 0.3 depending on structure complexity. For example a simple structure can be reasonably modelled as a single degree of freedom system. For such a system a small shift in frequency will not result in a large change in response and consequently β_U will be on the lower side. β_U of mode shape is usually 0.15.

d) Modal Combination Factor

Median modal combination factor, F_{MC}, accounts for difference between method used for modal combination in design and median method.

$$F_{MC} = V_d/V_m \qquad (2.43)$$

where V_d, V_m are seismic loads with modal responses combined according to design, median methods respectively.

The square root of sum squares (SRSS) combination of modal responses is considered to be median method. On the other hand, absolute sum is an upper bound. Variability due to modal combination is mainly random and is due to phasing. β_R typically ranges from 0.05 to 0.12.

e) Combination of Earthquake components

Median earthquake component combination factor, F_{MC}, accounts for difference between design and median methods.

$$F_{EC} = V_d/V_m \quad (2.44)$$

where V_d, V_m are seismic loads with directional responses combined according to design, median methods respectively.

Current practice is to combine the responses for the three principal earthquake directions by the SRSS method. Alternatively, the directional effects can be combined by taking 100% of the effects due to motion in one direction and 40% of the effects from the two remaining principal directions of motion (100-40-40 method). Combination by SRSS or 100-40-40 methods are both considered median-centred and thus yield a F_{EC} equal 1.0. Variability due to combination of earthquake components is mainly random with β_R typically range of 0.05 to 0.12.

On the other hand, combination of the responses for the three principal earthquake directions can be done by absolute sum method. The absolute sum method is an upper bound method, estimated to be three standard deviations above the median and F_{EC} should be calculated as mentioned above. In that case the variability can be evaluated as follows:

$$\beta_{R,EC} = (1/3) \ln (V_{abs}/V_m) \quad (2.45)$$

For shear walls, the response of the structure in the two principal directions is mainly independent. Consequently, for concrete shear wall structures, the factor of safety is not influenced by the directional component assumptions except for the case of torsional coupling.

f) Soil-Structure Interaction effects

For structures founded on stiff rock, fixed base analysis is considered median-centred. The reason is that there is small difference between actual parameters representing stiff rock when compared to fixed base models. Therefore, a factor of safety of unity is assigned to this parameter with almost no variability.

However an important factor is the effect of a finite size of base slab as compared to a point location. It was observed through limited data that a reduction in average input to the structure is expected when a large stiff base slab is modelled. The reduction in input is a function of both the plan dimensions and building frequency. For a 150-foot plan foundation, the reduction is:

Frequency (Hz)	Reduction
5	1.0
10	0.9
25	0.8

An interpolation can be used for different base slab dimensions and structures with different frequencies.

B.2.2 Buildings and Structures

B.2.2.1 Concrete Structures

The calculation of capacity of concrete structures can be done using lumped mass spring model or finite element model. The important factor is to define the failure mode and the threshold of failure. Also masonry structures are frequently used as interior walls for auxiliary buildings. The failure of load bearing masonry walls may cause catastrophic failure to the structure. Non-load bearing walls are a threat to adjacent equipment. Non-linear analyses are often used to demonstrate the capacity of unreinforced masonry walls.

a) Strength Factor

For concrete structures the strength of structure or element is a function of the concrete material properties, reinforcing steel material properties and the element configuration including geometry and details.

Two examples will be given for calculations of median material properties, for concrete and reinforcing steel, respectively:

Example 1: Concrete Compressive Strength

Most concrete elements capacity is based on concrete compressive strength, f'_c. The design value is usually taken the strength of a concrete test cylinder, tested after 28 days of the mix.

There are two major factors, which justify the selection of a median value for concrete compressive strength over its design strength:

- The concrete mix has an average strength above the design strength.
- Concrete compressive strength increases with ageing of concrete.

The median factor relating the strength of aged concrete to the 28-day strength is typically equal to 1.2. The logarithmic standard deviation β_U ranges of 0.10 to 0.18. Other factors that can affect the evaluation of concrete strength are rate of loading and difference in size between poured concrete and test cylinders. There is a slight decrease in strength for the in-place condition as opposed to the test cylinder strength. On the other hand, there is a slight increase in strength resulting from rate of loading at the seismic response frequencies of the structure. These two factors are usually neglected because their effects are of the same order magnitude and opposite in sign and thus tend to cancel each other.

Example 2: Reinforcing Steel Yield Strength

Determining the median yield strength and variability of reinforcing steel for a nuclear project should be based on tests conducted on reinforcing steel specimens. In the absence of test results, a review of median yield strengths and variability for reinforcement bars used in other nuclear plants should be performed. Reinforcing steel has less variability than concrete and its β_U range of 0.05 to 0.1.

When evaluating the yield strength of reinforcing steel, two other effects must be considered. These are the variation in cross-section areas of the bars and the effects of the rate of loading.

The available literature on these pointed out that the ratio of actual to nominal bar area has a mean value of 0.99 and β_U of 0.024. The rate of loading slightly decreases the yield strength of bars in tension but this effect is neglected in concrete compression.

b) Inelastic Energy Absorption Factor

Reinforced concrete members subjected to cyclic loading rarely exhibit the force-deformation curve of the type shown in Figure B-2. Instead after reaching ultimate strength, reinforced concrete exhibits degradation of strength at larger deformation. Collapse of the structure should be defined by severe strength degradation rather than ultimate strength. Median interstory drift for some common concrete structures are summarised as follows:

Structure Type	Median Drift	B_R	B_u
Shear walls with safety related equipment attached	0.005	0.15	0.30
Without safety related equipment attached	0.007	0.15	0.30
Containment Shell	0.0075	0.15	0.30

B.2.2.2 Steel Structures

Plastic hinges may form on some sections of the steel frame prior to failure. In defining failure of the structure, one must estimate the limit of inelastic deformation that is tolerable before affecting safety related items.

a) Strength Factor

For steel structures and components, the relationship between minimum and median material strength are usually well defined. For example, in past projects, the median yield strength of structural steel was taken to be 1.25 times code specified minimum yield strength with a logarithmic standard deviation of 0.12.

b) Ineslastic Energy Absorption Factor

Braced frame steel structures can vary considerably in ductility depending on which member failed first, the connection or the element.

B.2.2.3 Non-Seismically Qualified Structures

The main difference between seismically qualified structures and non-seismically qualified structures, from fragility methodology point of view, is in the amount of data available. For seismically qualified structures, seismic analysis has been performed and therefore different factors of safety can be easily calculated. For non-qualified structures, on the other hand, these data has not been prepared. Therefore, additional analyses is sometimes required to establish response of non-qualified structures to seismic loads. Also engineering judgement and experience can help assumed capacities and vulnerabilities of non-qualified structures as mentioned in Section B.1.

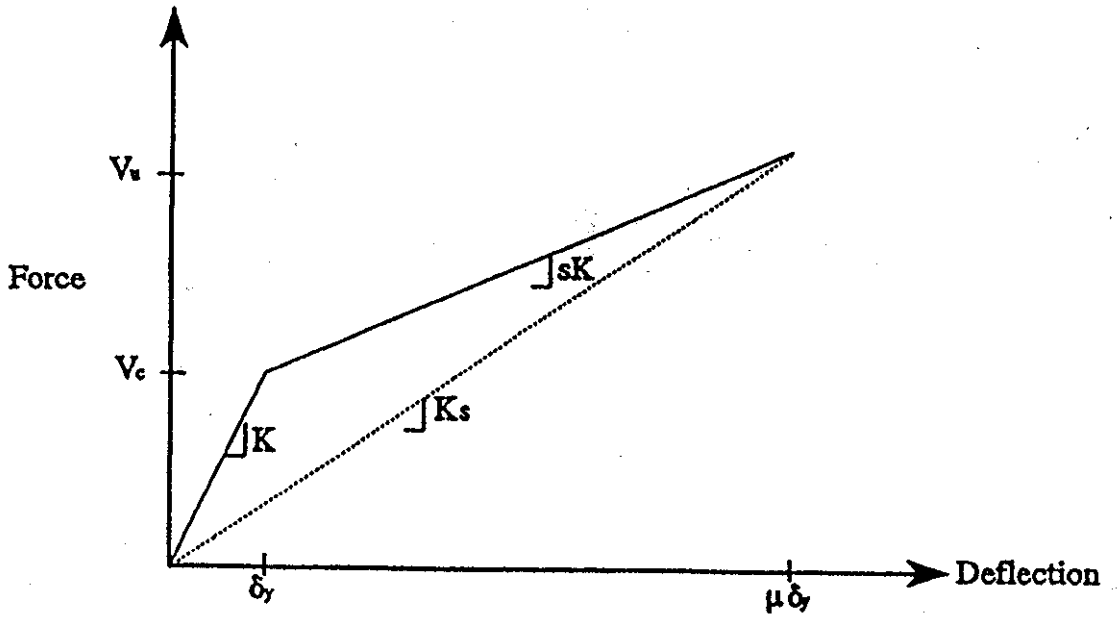


Figure B-2 Force Deformation Relationship, Effective Frequency/Effective Damping

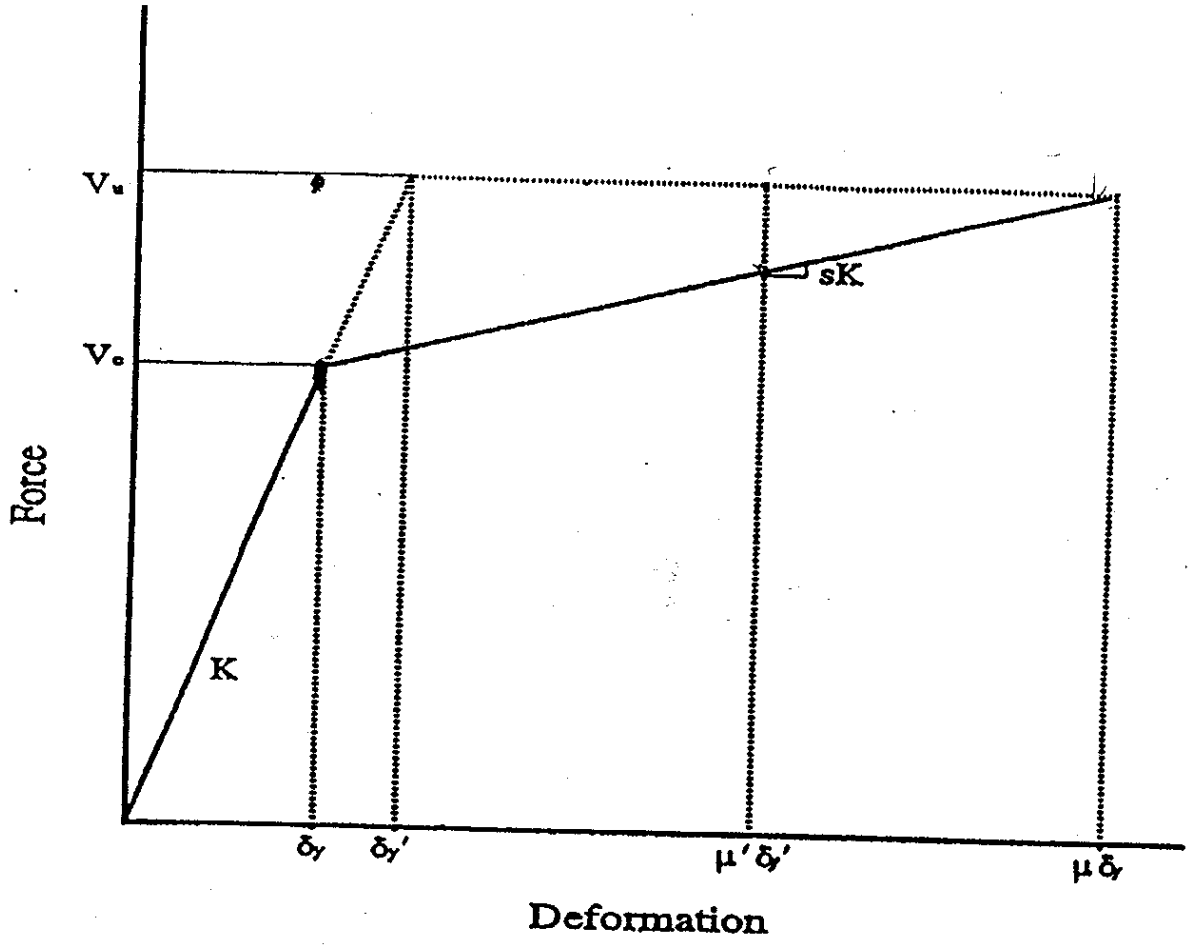


Figure B-3 Force Deformation Relationship, Effective Riddell-Newmark Method

B.3 Equipment Qualified by Analysis

This section deals with the fragility analysis for major equipment qualified by analysis. The methodology common to such equipment is discussed in more detail in the first subsection. Examples of major equipment in the CANDU reactor are given in the remaining subsections.

B.3.1 Seismic Fragility Methodology for Equipment Qualified by Analysis

The seismic fragility of the reactor is defined as the conditional probability of failure for an assumed level of seismic input parameter (e.g., the peak ground acceleration of the DBE). As described in more details in Section B.1, and by using the double lognormal model, the fragility can be concisely described by three parameters; the median capacity of the component A_m and the logarithmic standard deviations β_R and β_U reflecting the randomness and uncertainty in estimating this median capacity. In estimating these fragility parameters, it is computationally easier to work in terms of the factor of safety, F_m as defined in equation (1.3),

$$A_m = F_m . A_{DBE} \quad (3.1.1)$$

The overall median factor of safety of the equipment, F_m, is most conveniently separated into the following three parts:

1) The median factor of safety for the equipment capacity, F_{EC}, and its associated standard deviation parameters β_{REC} and β_{UEC}. This factor is due to safety inherent in the equipment response up to failure given the calculated design stress levels.
2) The median factor of safety for the equipment response, F_{ER}, and its associated standard deviation parameters β_{RER} and β_{UER}. This factor reflects the conservatism in the calculated design stress level given the raw design floor response spectrum.
3) The median factor of safety for the structure response, F_{SR}, and its associated standard deviation parameters β_{RSR} and β_{USR}. This factor reflects the conservatism in calculating the raw design floor response spectrum.

The three median factors of safety are random variables that are multiplied together to yield the overall median factor of safety as follows:

$$F_m = F_{EC} . F_{ER.} F_{SR} \quad (3.1.2)$$

The overall logarithmic standard deviation is combined from the three parts using the Square Root of Sum Squares (SRSS) method for each of the random and uncertainty parameter as follows:

$$\beta_R = (\beta^2_{REC} + \beta^2_{RER} + \beta^2_{RSR})^{½} \quad (3.1.3)$$

$$\beta_U = (\beta^2_{UEC} + \beta^2_{UER} + \beta^2_{USR})^{½} \quad (3.1.4)$$

The above three parts of median factors of safety are in turn influenced by other random variables as will be explained later. For each part, the three fragility parameters should be

estimated separately and then combined with other factors as per the multiplication rule in equation 3.1.2 and the SRSS rule in equations 3.1.3 and 3.1.4.

Having obtained the fragility parameters, an acceptance criteria can be based on the concept of "High Confidence of Low Probability of Failure" (HCLPF) ground motion acceleration as given by equation (1.2), i.e.:

$$\text{HCLPF capacity} = A_m.\ \exp\left[-1.65\ (\beta_R + \beta_U)\right] \quad (3.1.5)$$

B.3.1.1 Equipment Capacity Factor, FEC

The Equipment Capacity Factor F_{EC} represents the factor of safety assuming that the calculated design stress level is median. The equipment seismic capacity factor, F_{EC} consists of two parts, which relate to the strength factor, F_S and the inelastic energy absorption factor, F_μ. The combined effect of those two random variables is calculated by the multiplication rule;

$$F_{EC} = F_S.\ F_\mu \quad (3.1.6)$$

The overall logarithmic random and uncertainty standard deviations parameters are calculated by the SRSS rule:

$$\beta_{REC} = (\beta^2_{RS} + \beta^2_{R\mu})^{1/2} \quad (3.1.7)$$

$$\beta_{UEC} = (\beta^2_{US} + \beta^2_{U\mu})^{1/2} \quad (3.1.8)$$

The following factors make up the equipment capacity factor:

- The Strength Factor, F_S

  It is the ratio of the median strength available to resist seismic input motion to the calculated response due to the design seismic event. It is derived from the equation:

  $$F_S = (P_C - P_N)/P_{EQ} \quad (3.1.9)$$

  where P_C is the median limit state load or stress, P_N is the normal operating load or stress and P_{EQ} is the reference seismic load or stress. The limit load (P_C) is a function of the failure mode. The normal and seismic reference loads (P_N and P_{EQ}) are typically derived from knowledge of the material properties and design stress levels as available in the seismic analysis reports.

  For example, the strength factor for a tensile-type failure mode is based on increasing the code specified minimum yield strength by a factor of 1.25 for Carbon and Stainless steel, 1.2 for low strength bolts and 1.1 for high strength bolts (σ_u> 100 ksi).

  For bending-type failure mode, the factor is 1.50 for rectangular cross sections. More values are given in ASME Code Section III for other cross sections.

  Each variable in equation 3.1.9 has an associated randomness and uncertainty variance parameters. The overall variance on the strength factor is calculated using the "second moment method" which results in the following equation:

$$\beta_S = (P^2_C.\ \beta^2_C + (P_C-P_N)^2.\beta^2_{EQ} + P^2_N.\beta^2_N)^{1/2} \quad /(P_C - P_N) \qquad (3.1.10)$$

It should be noted that the variability in the strength factor is basically due to uncertainty (i.e., all $\beta_R = 0$). For example, $\beta_U = 0.14$ for tensile failure mode, and $\beta_U = 0.11$ for bending failure mode.

- The Inelastic Energy Absorption Factor, F_μ

  A significant increase in the seismic capacity of equipment can be obtained if the inelastic absorption of the structure is considered in addition to the strength capacity. Early studies indicated that the inelastic energy absorption factor was primarily a function of the ductility ratio, μ, which is defined as the ratio of maximum displacement near failure to displacement at first yield. Accurate calculation of the inelastic energy absorption factor may require lengthy nonlinear analysis. However, a simplified approach by Riddle and Newmark (Reference B-4) can provide reasonable values of F_μ by combining existing results from elastic linear analysis with the frequencies, damping, allowable maximum displacements near failure and some recommended values of the structural ductility factor, μ. More details of this simplified approach is given in Section B.2.

  Although the element ductility of component made of steels can be high (e.g., 10 to 20), the overall component ductility is substantially less. For example, the following generic system ductilities are suggested in NUREG/CR-3805 (Reference B-7):

Equipment type	Median ductility, F_μ	Ductility at -1β, $F_{\mu-1\beta}$
Light equipment	1.5	1.36
Heavy equipment	2.0	1.72
Piping	3.0	2.40

  Where $F_{\mu-1\beta}$ is estimated at median value minus one standard deviation.

  The associated randomness variability is estimated as:

$$\beta_R = 0.11\ (F_\mu - 0.5) \qquad (3.1.11)$$

  and the associated uncertain variability is estimated as:

$$\beta_U = \ln (F_\mu/F_{\mu-1\beta}) \qquad (3.1.12)$$

  It should be noted that for brittle and functional failure modes, $F_\mu = 1.0$ and $\beta = 0$.

B.3.1.2 Equipment Response Factor, F_{ER}

The Equipment Response Factor, F_{ER}, depends on a number of factors related to the assumed raw design floor response. Each factor is a random variable with its own median and variability parameters. The following factors make up the equipment response factor:

- The Qualification Method factor, F_{QM}

  The Qualification Method factor is a measure of the conservatism involved in the type of analysis (equivalent static or dynamic) used in the seismic qualification of the equipment. The response spectrum method is mostly used for the dynamic analysis of major equipment. In many cases, a generic envelope spectrum is used to qualify the equipment. There are two sources of conservatism and variability in the dynamic analysis.

  The first source of conservatism results from comparing the actual floor spectrum used to the reference floor spectrum. If generic spectra are used, the F_{QM} is the ratio of the spectral acceleration from the generic spectrum divided by the spectral acceleration from the reference (DBE based) spectrum evaluated at the component fundamental frequency or frequencies on a mode-by-mode basis.

  The second source of conservatism results from the practice of peak broadening and smoothing of floor spectra. Not many detailed studies have been conducted to define the range of this factor, but the following generic factors are suggested:

Frequency range	factor F	variability parameter, β
5 – 10 Hz	1.20	0.09
10 – 20 Hz	1.15	0.05
> 20 Hz	1.00	0.00

- The Damping factor, F_D

  This factor takes advantage of the increased damping level at or near failure as compared with the design damping level used in the design of the equipment. The basis for calculating the required parameters is similar to that in Section B.2.

- The Modelling factor, F_M

  Modelling of complex systems is usually based on using nominal dimensions, masses and material properties in such a manner that further refinement of the finite element model will not significantly alter the calculated response. However, the representation of the boundary conditions may have a significant effect on the results. If it is judged that the analyst has done his best job, the modelling factor is assumed equal to unity (i.e., F_M =1). The modeling variability may be based on uncertainty in calculating the equipment frequency and mode shapes. The parameter, β_U ranges from 0.1 to 0.2 for frequency, and from 0.05 to 0.15 for mode shape. The combined effect should be calculated by the SRSS rule.

- The Mode Combination factor, F_{MC}

  The modal combination technique utilized for most dynamic analysis is the SRSS method, which is considered, median-centred. Hence, the Mode Combination factor is unity (i.e., F_{MC} =1.0). The variability is considered to be all randomness due to the random phasing of modes. The parameter, β_R can be take equal to 0.15 for multi-mode flexible equipment,

β_R=0.1 for single mode flexible equipment and β_R=0.0 for rigid equipment (i.e., frequency > 33 Hz).

- The Earthquake Component Combination factor, F_{ECC}

  The SRSS method is mostly used to combine the dynamic response from earthquakes in three orthogonal directions. Like the Mode Combination above, the Earthquake Component Combination factor is unity (i.e., F_{ECC} =1.0), and the variability is considered to be all randomness. The parameter, β_R is calculated as follows:

  β_R= 1/3 ln (P_{abs}/P_{med}) (3.1.13)

  where P_{abs}= force or stress of interest from absolute sum of all 3 directional components

  P_{med}= force or stress of interest from the SRSS of all 3 directional components

  A conservative generic value of β_R = 0.18 can be assumed.

  The overall median factor F_{ER} is calculated by the multiplication rule as follows:

  $F_{ER} = F_{QM}. F_D. F_M. F_{MC}. F_{ECC}$ (3.1.14)

The overall logarithmic standard deviation is calculated by the SRSS rule of all the contributing factors similar to equation 3.1.7 and 3.1.8 above.

B.3.1.3 Structural Response Factor, FSR

The Structural Response Factor, F_{SR} defines the effect of the conservatism of the structural analysis and the development of floor response spectra on the actual equipment response. The structure response factors as they are related to structural capacity are dealt with in Section B.2. However, the floor response spectra are typically generated using time-history methods, whereas the structural loads are usually developed using a response spectrum analysis. The variables used to generate floor response spectra are the only variables of interest relative to equipment failure. The applicable variables for equipments are:

- The Spectral Shape factor, F_{SS}

  When time-history analyses are conducted, the resulting spectra are required to envelop the DBE ground motion spectra. The Spectral Shape factor F_{SS} is taken as the ratio of the spectrum resulting from the time-history motion to the DBE ground response spectrum.

- The Damping factor, F_D

  The effect of increased damping at or near failure on the Damping factor, F_D and its variability is calculated in a manner similar to the structural response of Section B.2.

- The Modelling factor, F_M

  The Modelling factor, F_M and its variability are calculated in a manner similar to the structural response of Section B.2.

- The Mode Combination factor, F_{MC}

  If the modal superposition time-history is used to develop the floor spectra, the phasing of modes is directly included. Hence, the Mode Combination factor is unity (i.e., F_{MC} =1). However, there is a random variability due to the infinite number of earthquakes.

- The Earthquake Component Combination factor, F_{ECC}

  The Earthquake Component Combination factor, F_{ECC} and its variability are calculated in a manner similar to the structural response of Section B.2.

- Soil-Structure Interaction, F_{SSI}

  The Soil-Structure Interaction, F_{SSI} and its variability are calculated in a manner similar to the structural response of Section 2.

- The Ground Motion Incoherence, F_{GMI}

  For stiff structures with long basement plan dimensions, the Ground Motion Incoherence, F_{GMI} removes the conservatism associated with the analysis assumption of spatially coherent ground motion. The factor can be assumed equal to unity for steel structures, but it is typically greater than one for stiffer concrete structures.

- The Inelastic Structure Response, F_{IR}

  As the civil buildings approach failure, the spectral accelerations can get higher or lower than a scaled linear floor spectra depending on the frequency content and the structural characteristics of the building. Unless a nonlinear analysis is conducted, the Inelastic Structure Response factor is assumed equal to unity. A composite variability parameter β= 0.2 can be assumed for floors at or above the C.G. of the structure (Reference B-7). A value of β= 0 is taken at the basement level. For floors between the base and the C.G. of the structures, the value can be derived by linear interpolation.

  The overall median factor F_{ER} is calculated by the multiplication rule as follows:

  $$F_{SR} = F_{SS}. F_{D}. F_{M}. F_{MC}. F_{ECC}. F_{SSI}. F_{GMI}. F_{IR} . \quad (3.1.15)$$

  The overall logarithmic standard deviation is calculated by the SRSS rule of all the contributing factors similar to equation 3.1.7 and 3.1.8 above.

B.3.2 HT Process Equipment

This section covers the HT system motor pump-set, the steam generator (SG) and the feeders. The basic approach to the calculation of their seismic fragility is similar, but each component is sufficiently different from the others in terms of safety requirements or design features to warrant a separate treatment of each one.

B.3.2.1 Feeders

B.3.2.1.1 Load Combinations

Loading seen by a feeder pipe during the DBE include deadweight, temperature, internal pressure, channel creep, and cold springing, in addition to the seismic inertial forces and E/F seismic deflections when the F/M is latched on.

B.3.2.1.2 Components to be Evaluated

Components that need to be evaluated include the feeder pipe itself and supports between the feeder coupling and the header nozzle. Of particular importance are the first and the second bends immediately downstream of the outlet E/F where the temperature is the highest and the potential for wall thinning is the most. Because there are different pipe sizes, bend configurations, and degrees of wall thinning, it may be necessary to investigate several feeders.

For the supports, the components include support members, bolts, and weldment. There may be more than one support type. For this reason, more than one support may have to be investigated.

B.3.2.1.3 Failure Modes and Failure Criteria

For the supports, the failure mode is over-stress. The failure criterion is the maximum stress theory.

For the feeder elbow, the failure mode is also over-stress, but the failure criterion is the maximum shear stress theory. A finite element of the feeder bend will be required to perform a detailed stress analysis.

Fragility calculations are as described in Section B.3.1.

B.3.2.2 HT System Motor Pump-set

In CANDU 6, the HT system motor and pump-set is restrained laterally at the motor by three horizontal restraints spaced at 120^{o} apart. Vertically, the motor pump set squats on the reactor inlet header via two vertical pump discharge legs. There are also two spring hanger rods suspending the motor. The hanger rods are tensioned so that the motor pump set does not impose any appreciable weight on the header during normal operation. The pump suction line, the discharge legs, and the header are all well restrained and supported.

From existing stress reports, it is known that the effects of pipe break forces on the pipes, the pump, and the supports are far more severe than the seismic effects. One can infer that the pump, the HT piping associated with the pump, and their supports have a high seismic margin in strength and may be screened out. A fragility calculation is needed to verify this assumption.

The critical components which are relatively unaffected by the pipe break forces are the shaft, the bearings, and the motor.

The motor manufacturer is required to guarantee his motor good for a horizontal seismic acceleration typically up to 2.5g. The motor is well restrained. For this reason, the motor may be screened out. This will be verified as part of the detailed fragility calculation.

The bearings manufacturer provides maximum loads and maximum allowable loads for the bearings. The former are the bearings ultimate capacity, which will be used in the fragility calculations.

The shaft needs to be evaluated for:

- Its deflections during an earthquake to ensure that the air gaps remain open;
- Stress in the coupling to ensure structural integrity of the coupling; and
- Seismic bearing loads so that the bearings are not overloaded.

Consequently, the median seismic capacity of the motor pump set will be determined using the smallest of the following margins:

$$\frac{\text{Air Gap}}{\text{Seismic Deflection}}$$

$$\frac{\text{Ultimate Bearing Load}}{\text{Seismic Bearing Load}}$$

$$\frac{\text{Yield Stress in Coupling}}{\text{Seismic Stress in Coupling}}$$

Note: yield stress, instead of ultimate stress, is used because the shaft has to remain elastic at all times. The seismic margin will be multiplied by various factors of safety and PGA to obtain the median seismic capacity. Then, uncertainty parameters and randomness parameters will be used to obtain HCLPF and CDFM (Conservative Deterministic Failure Margin).

The motor and pump set will undergo a simulated post-LOCA loop test. The vibrations during the test are prolonged and severe. It may be possible to screen out the motor and pump set based on the results of the simulated post-LOCA loop test.

B.3.2.3 Steam Generator

The Main Steam Line (MSL) is qualified up to the Main Steam Header. An earthquake induced MSLB (Main Steam Line Break) is required to be considered in conjunction with the seismic event.

The critical components in the SG (Figure B-4), which need to be evaluated, are the internals, the lateral supports, the vertical column, and the anchor bolts.

The failure modes are over-stress and loss of stability.

The failure criterion is the maximum stress theory.

Loading to be considered are the MSLB effects, deadweight of the SG, seismic inertial forces of the SG, and piping forces and moments due to piping deadweight, thermal, and seismic effects.

Fragility calculations are as described in Section B.3.1.

B.3.3 Reactor Assembly

B.3.3.1 Description

The CANDU Pressurized Heavy Water Reactor is basically a horizontal tube heat exchanger. The calandria and shield tank is shown in Figure B-5. The core of the reactor contains a number of fuel channels, which are contained in and supported by a horizontal cylindrical vessel known as the calandria vessel. The calandria contains the heavy water moderator, and is surrounded by light water in the vault (CANDU 6) or in a shield tank (CANDU 9). The calandria is supported by a flat circular end shield which is directly connected to the vault wall at each end for CANDU 6, or indirectly through another flat circular end wall which encloses and supports the shield tank in CANDU 9 as shown in Figure B-6. The whole assembly is vertically supported to the vault wall by annular support shell and plate ring at the two ends. Additional axial restraint against seismic motion is provided by axial restraint bolts connecting the calandria vessel (and shield tank) to the end wall (and vault wall) respectively (see figures B-7 and B-8). The basic design criteria for the reactor assembly are:

- To provide support to the whole reactor assembly via the embedment in the walls of the reactor vault.
- To provide support to the fuel channels by the end shields.
- To provide support to the reactivity control units and piping attached to the reactor.
- To provide shielding to the fuelling machine vault.
- To contain the moderator and shield cooling system water.
- To meet the allowable service limits under all design and service loading conditions. The loads include pressure, temperature, seismic, static and dynamic mechanical loads over the specified life of the plant.

B.3.3.2 Failure Modes

Several potential failure modes due to seismic effects should be investigated such as:

1. Failure of seismic (calandria or shield tank) restraint in the axial direction.
2. Excessive plastic deformation in the support shell and plate ring.
3. Calandria (or shield tank) shell overstress particularly at the connections between the main and sub shells.

4. Calandria tube failure at the tube sheet.
5. Pressure tube failure at the rolled joint locations.
6. Failure of the position assembly, which fixes the fuel channel in the axial direction by connecting it to the fixed end shield.
7. Brittle failures of welds and/or pullout of anchor bolts.

The reactor components are typically designed according to the ASME Boiler and Pressure Vessel code, which provides reasonable factors of safety on material strength and allows for energy absorption due to the ductility of the material and system components. Furthermore, some equipment is governed by LOCA loading conditions, which provide substantial margin for seismic loading. However, the analyst should be aware of brittle and functional failure modes, which may otherwise nullify the significant contribution of ductility to the seismic strength capacity of the equipment. Therefore, special attention should be given to the last item above (i.e., brittle anchor failure of the axial seismic restraint).

B.3.4 Fuelling Machine

B.3.4.1 Description

The major elements of the refuelling system are a pair of identical fuelling machines (F/M), which operate at both ends of the reactor and bring new fuel from the new fuel ports to the reactor, and carry irradiated fuel to the spent fuel ports. The fuelling machine head, a pressure vessel containing the new or irradiated fuel during its transport, can be supported either by a bridge system such as that used in CANDU 6, or by a mobile carriage such as that suggested for CANDU 9 (Figure B-9). In the later design, the mobile carriage positions the fuelling machine head at the selected lattice location in the X (transverse) and Y (vertical) locations, engages the seismic locking mechanisms, and then advances the fuelling machine head in the Z (axial) direction. Once the head arrives at the pre-stop position, X and Y measurements are established. If necessary, the head is retracted clear of the end fitting and X and Y homing corrections are carried out by the fine X and Y carriage drives, respectively. The repositioned fuelling machine is then advanced to contact the end fitting. At this point, a standard CANDU fuelling sequence commences.

The CANDU 9 carriage is designed to the requirements of the CAN/CSA N285.0 (General Requirements for Pressure Retaining Systems and Components in CANDU Nuclear Power Plants) and CAN/CSA N285.2 (Requirements for Class 1C, 2C and 3C Pressure Retaining Components and Supports in CANDU Nuclear Power Plants). These standards recognize the unique design of CANDU fuel handling systems and allow pressure vessel supports such as the carriage to be designed in accordance with the ASME Boiler and Pressure Vessel Code, Section III, Subsection NF.

The carriage assembly structure consists of six main sub-assemblies: the base, turntable, columns, outer elevator, inner elevator and guide plate. The base is a structure on two wheels, which provides the X motion. The turntable provides the rotation freedom of the carriage. The

column sub-assembly is bolted on the top of the turntable and has Y guide tracks along their front and backsides. The outer elevator is positioned between the columns and allows the vertical movement of the fuelling machine. The inner elevator moves relative to the outer elevator to provide the Z motion of the carriage.

The cradle and F/M head of CANDU 9 (Figure B-10) are supported by the inner elevator. The upper guide beam is supported by the concrete F/M vault and restraints the top end of the F/M carriage against Z (axial) displacement when the carriage is in transit, and prevents further lateral displacements when seismic locks are engaged. Similar arrangement (with different details) applies for CANDU 6.

As illustrated above, the fuelling machine is a complex structure because of many moving parts, springs, ballscrews, etc. Furthermore, it has many modes and configurations during its operations. Two main scenarios of operation have to be considered:

- Unattached Case

  This is a typical case of off-reactor scenario, where the F/M snout is not clamped onto any end fitting or any service port. The analysis involves the idealization of many parts in the F/M sub-assemblies by using beam, spring and mass finite elements. The evaluation and lumping of masses and stiffness and imposing the correct kinematical relationships between the moving parts require a great deal of attention and experience. Seismic analysis models for CANDU 9 and CANDU 6 have been developed.

- Attached Case

  This is a typical case of on-reactor scenario representing a fuelling sequence. In this case, two fuelling machines are attached to an arbitrary fuel channel. In turn, the fuel channel is attached to the reactor. Therefore, in addition to the seismic finite element models of two F/M, the fuel channel and reactor components are idealized as beams, springs and mass elements.

  In a seismic event, the forces transmitted between the fuelling machine and the end fitting are controlled by different springs in the F/M head assembly and/or the seismically excited masses of the fuel channel and reactor components. The lumped mass models provide the accelerations and forces in different parts to help identify some probable failure modes. It is important to check if any soft spring in the F/M head will bottom out. This may cause high forces being exerted on the end fitting leading to damage of the fuel channel.

B.3.4.2 Failure Modes

In addition to previously discussed failure modes, other modes that are unique to the F/M design has to be considered in both the attached and unattached cases:

1. Failure of the trunnions at the cradle-F/M head support.
2. Failure of pitch spring and loss of balance of the F/M head.
3. Failure of bolts that connect the cradle to the F/M head.

4. Failure of the yaw spring, resulting in uncontrolled yaw motion of the F/M head and impact of the F/M ram with the columns.
5. Bottoming out of the Z-spring.
6. Failure of the gear-pinion of the lower turntable.
7. Failure of the base wheel flanges and anti-lift hooks due to lateral movement and/or rocking.
8. Failure of the ball nut of the ballscrew.
9. Stress concentration and cracking of the seismic lock pins and seismic lock holes.
10. Large uncontrolled movement and the impact of the whole carriage with its surrounds when it is in transit.

The fuelling machine is made of steel that provides substantial margin for seismic loading. However, the analyst should be aware of brittle and functional failure modes, which may otherwise nullify the significant contribution of ductility of steel components Therefore, special attention should be given to the possibility of brittle failure of weldment and bolts at connections and the Z-spring attachment.

B.3.5 Electrical Cable Trays

To evaluate fragility of cable trays, failure modes and weak links have to be identified and the corresponding fragility parameters need to be assessed.

B.3.5.1 Failure Modes

Electrical cables of various sizes are usually grouped together and installed in steel trays, which are then mounted onto cable tray support racks. In the cable tray system, the ladder type steel trays are designed mainly for the purpose of bundling the cables. Loading carried by the steel trays is relatively small whereas the strength of the steel trays is high. Therefore, it is unlikely that failure will be initiated in the steel trays during a seismic event. In CANDU 6 design, the support racks consist of CANTRUSS members connected together by brackets and bolts to form the planar frames. They are anchored to the floor or the ceiling of the concrete buildings. To strengthen the racks in the out of plane direction, longitudinal bracing is applied. In some support frames, lateral bracing is also used to take a large portion of the seismic lateral forces of the cable trays. During a seismic event, the support frames have to sustain vertical as well as horizontal loads. Failure could occur due to excessive stress; deformation is rarely a concern for cable trays. The potential failure modes are identified as follows:

- Anchor bolts pull out for the tray support frame legs;
- Stability of the bracing members; and
- Excessive stresses in the frame legs and overload to the frame member connections.

B.3.5.2 Weak Links

Generally speaking, the steel trays themselves have high strength capacities provided their splicing is adequate. Efforts to search for weak links in the cable tray system should be focused on the support racks especially the anchorage. The complete collapse of the cable tray system is unlikely if the anchorage can sustain all the loads. In the recent CANDU 6 design, the cable trays are seismically qualified by detailed analysis. Seismic qualification analysis results are helpful to find the weak links. For the generic equipment such as cable trays, fragility analysis is usually performed on a group of components selected through sampling process supplemented by the plant walkdown.

B.3.5.3 Determination of Seismic Capacity

The scaling method as described in Section B.3.1 is applied to evaluate seismic fragility of the cable trays. The fragility of the cable trays is derived through the safety factors, which include the capacity factor, the cable tray response factor and the structural response factor.

The capacity factor is determined from the strength factor and the inelastic energy absorption factor. For the strength factor, it has to be assessed from the ultimate strength of the system with capacity reduction due to dead weight. Inelastic energy absorption should be considered for the ductile overstress failure mode. However, in the case of the brittle anchorage pullout and brace buckling failure modes, inelastic behaviour is insignificant, therefore, ductility credit cannot be taken to increase the capacity.

The cable tray response factor considers the aspects related to the response determination for the given floor response spectra:

- Modelling aspects, e.g., the cable mass and its distribution, idealisation of the anchorage and the frame member connections as well as the stiffness of the steel trays.
- Method of analysis.
- Combination of earthquake components.
- Mode combination.
- Spectral shape.
- Damping. (Note that the design analysis damping could be very conservative since the cable trays have very high-energy dissipation capability resulting in high damping value).

In addition, the conservatism in the generation of the floor response spectra needs to be addressed. This structural response factor can be determined in accordance with the method in Section B.2.

The randomness and uncertainty are represented by the logarithmic standard deviations β_R and β_U whereas the median capacity A_m is determined by the scaling factors discussed above. The fragility curves of the cable trays are explicitly described by the three parameters.

HCLPF (the high confidence of a low probability failure) equivalent PGA can be calculated by the following formula:

$$HCLPF = A_m e^{-1.65(\beta_R + \beta_U)} \quad (3.5.1)$$

HCLPF capacity can also be calculated from

$$HCLPF = A_m e^{-2.33\beta_C} \quad (3.5.2)$$

where $\beta_C = (\beta^2_R + \beta^2_U)^{1/2}$.

B.3.6 Non-Seismically Qualified Equipment

Non-Seismically Qualified (NSQ) equipment is not required to perform safety functions. For this reason, they do not have detailed seismic analysis, design or test reports. Therefore, the fragility evaluation for NSQ equipment is based on using simple modelling and conservative assumptions. The dominant failure mode in most NSQ equipment is due to functional failure and/or structural failure.

The structural failure mode is estimated by anchorage calculations. It should be noted here that the inelastic energy absorption factor at anchors is 1.0 and the associated randomness and uncertainty parameters are all zero.

For equipment which are not amenable to analysis and would have to be qualified by test, the following suggestions are given for estimating the median capacity:

- Some of the equipment may also be used in other safety systems and are qualified. It is worthwhile to make use of the qualification results.
- Failing that, use generic data, as explained below.
- If the generic data give too low a median capacity, consider seismic qualification provided it is cost effective.
- Conduct a walkdown.

When generic data or experienced base data are used, the median seismic capacity for the equipment functionality is estimated from the design floor response spectrum and the reference spectrum. The reference spectrum is based on survival data of similar equipment subjected to earthquakes at industrial facilities. The reference spectrum provides a reasonable description of the ground motion level to which the earthquake experience data demonstrate seismic ruggedness. This methodology of using experience database is documented in (Reference B-5).

The median capacity of the equipment is modelled in terms of the factor of safety, F_m as follows:

$$A_m = F_m . \ A_{DBE} \quad (3.6.1)$$

The overall median factor of safety of the equipment, F_m, is calculated by the multiplication of three parts:

$$F_m = F_{EC}.\ F_{ED.}\ F_{SR} \quad (3.6.2)$$

Where:

1. F_{EC}: The equipment capacity factor. It is equal to the ratio of the actual seismic capacity to the reference spectrum.
2. F_{ED}: The experience data factor. It is equal to the ratio of the reference spectrum to the design floor response spectrum FRS.
3. F_{SR}: The structure response spectrum factor. It is equal to the ratio of the design floor response spectrum FRS to the median centred FRS.

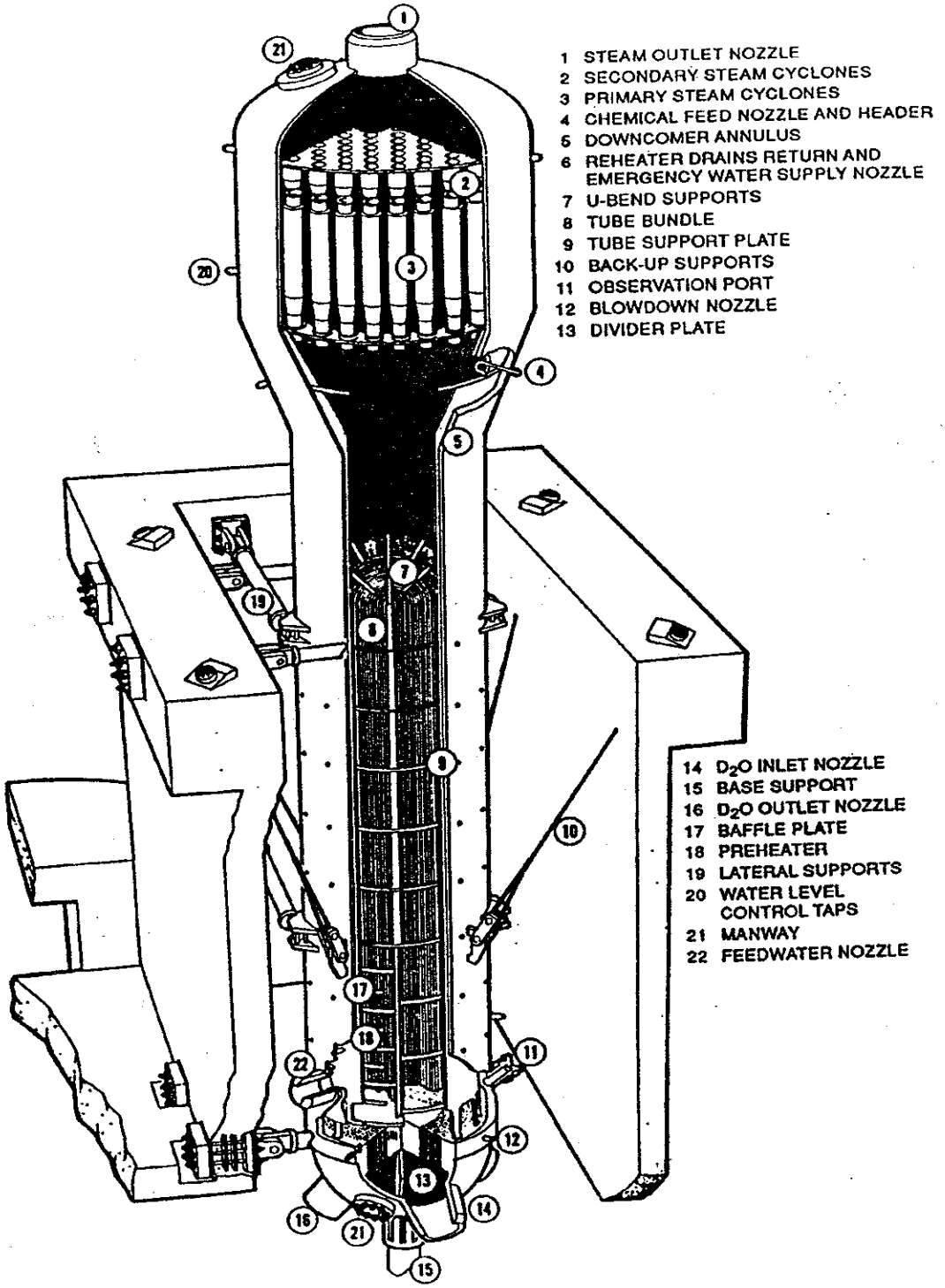


Figure B-4 Heat Transport System Steam Generator (Typical)

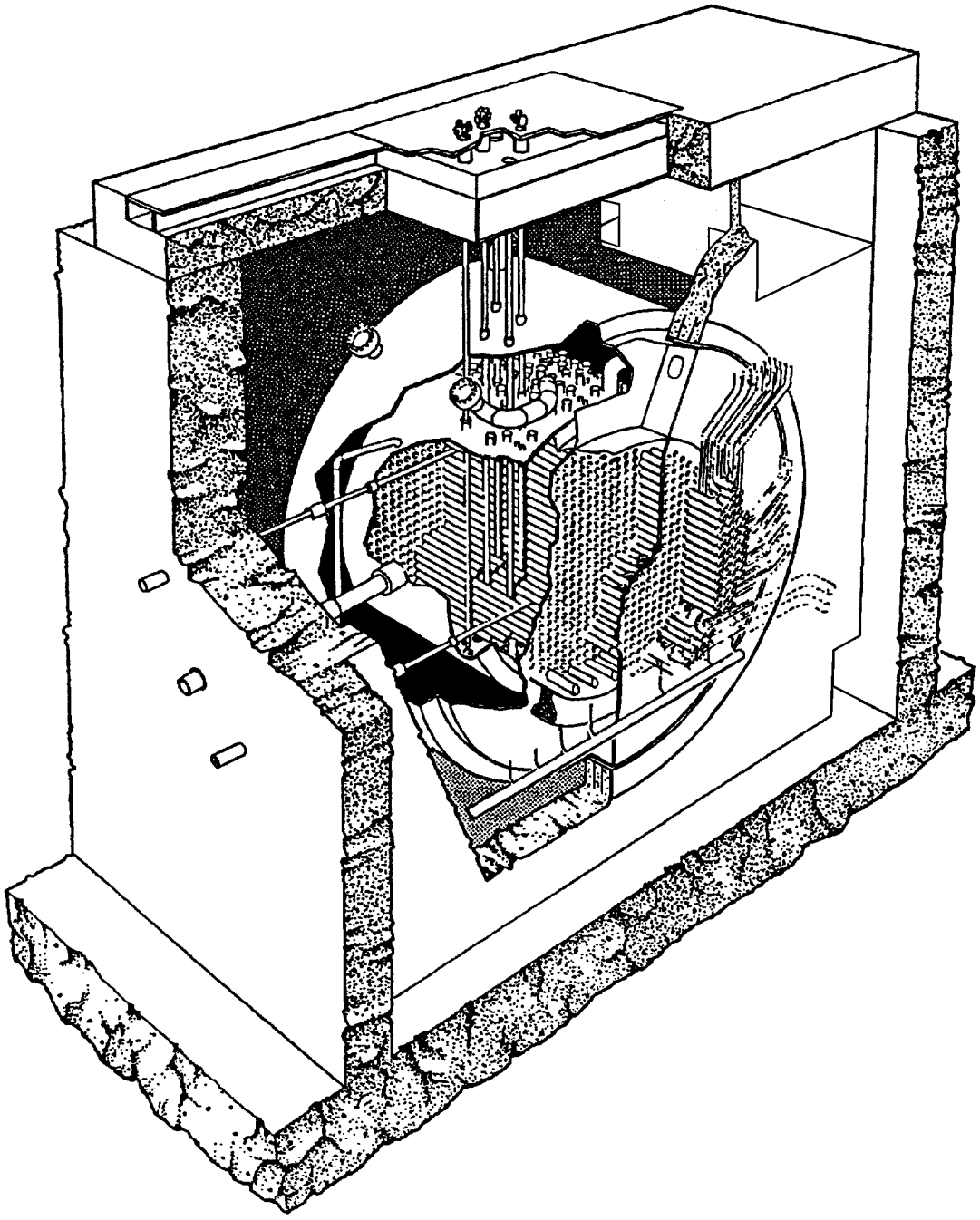


Figure B-5 Calandria and Shield Tank - General Arrangement

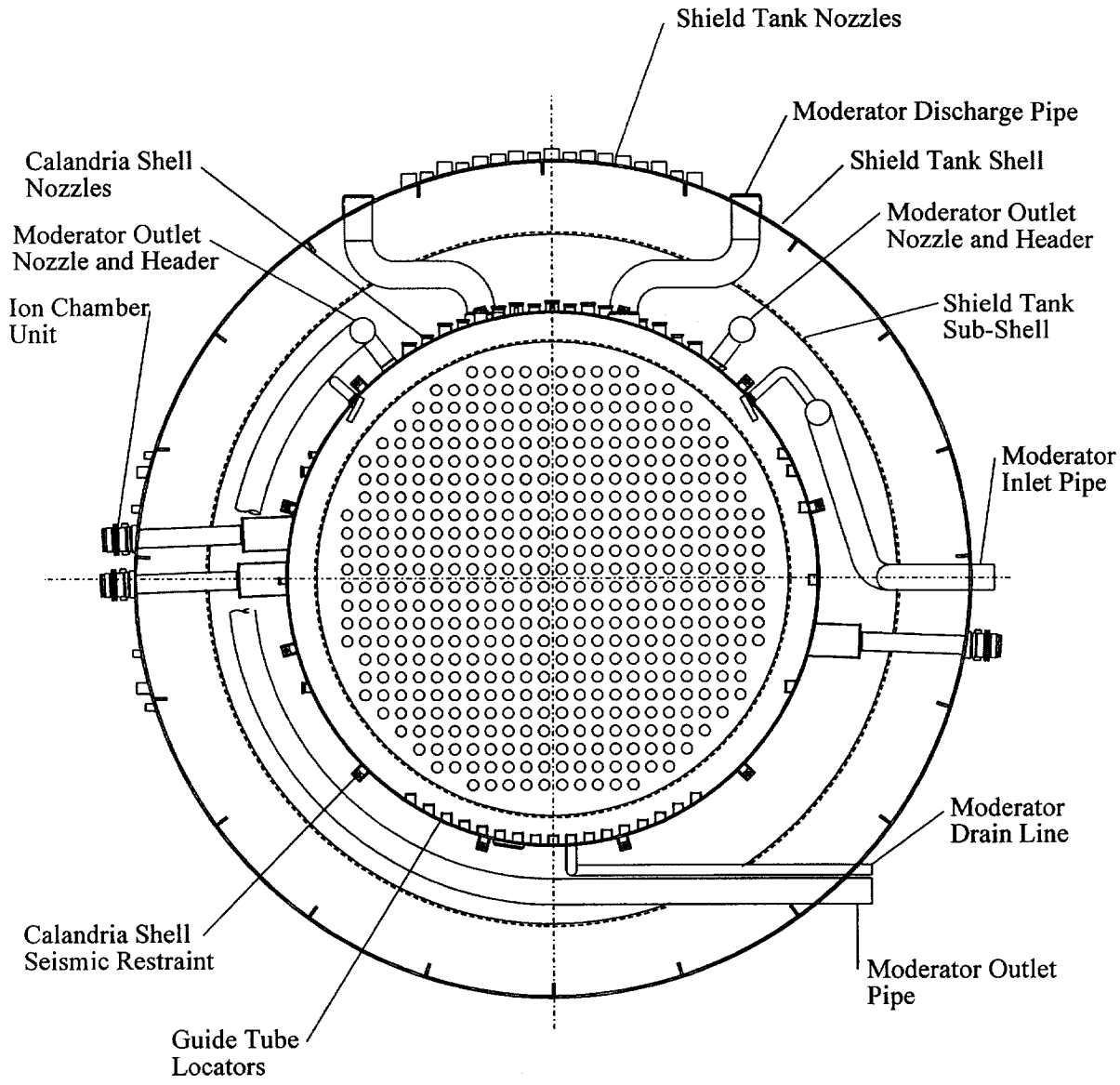


Figure B-6 Transverse Cross Section (CANDU 9)

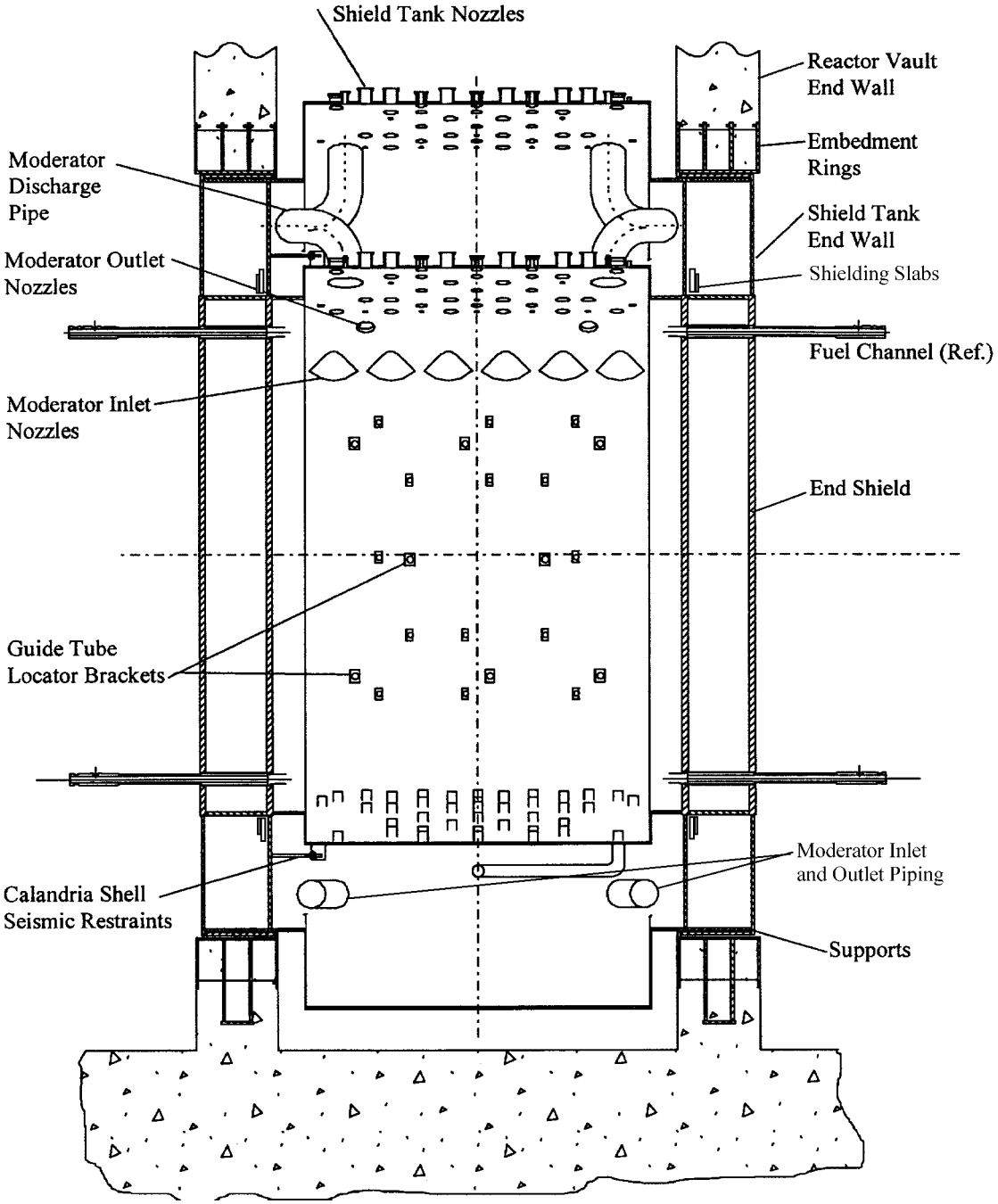


Figure B-7 Axial Cross Section (CANDU 9)

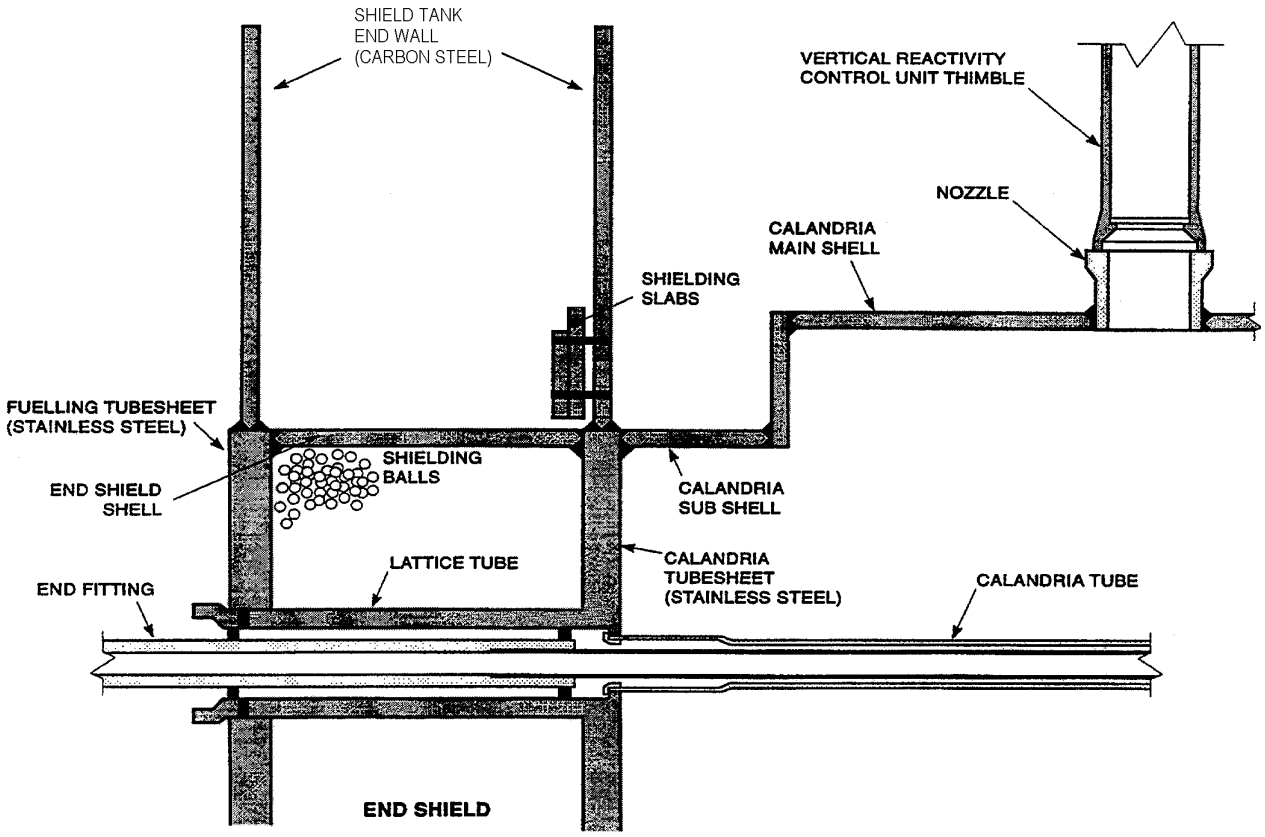


Figure B-8 Cross Section Through End Shield, End Wall and Calandria Vessel (CANDU 9)

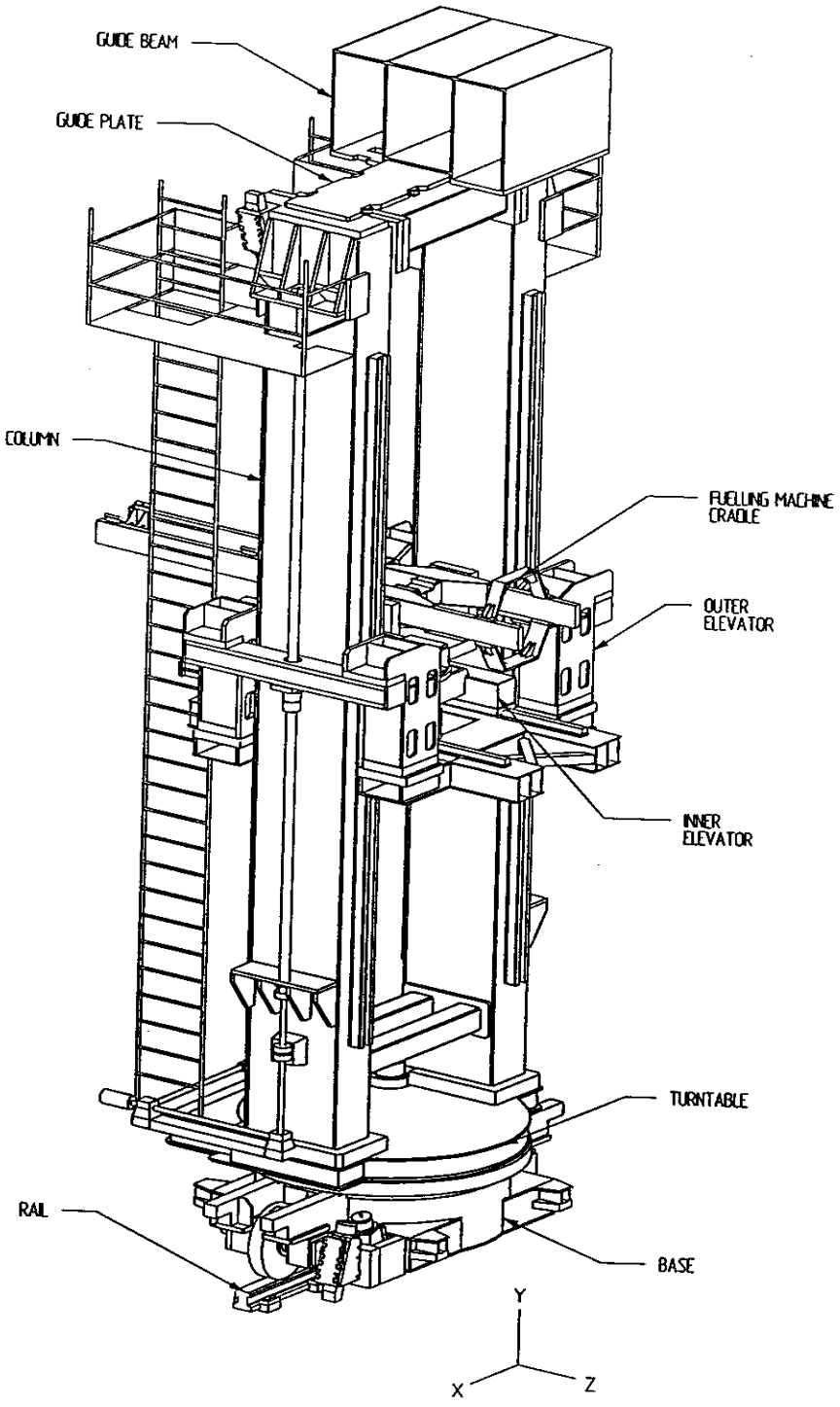


Figure B-9 Fuelling Machine - General Arrangement in CANDU 9

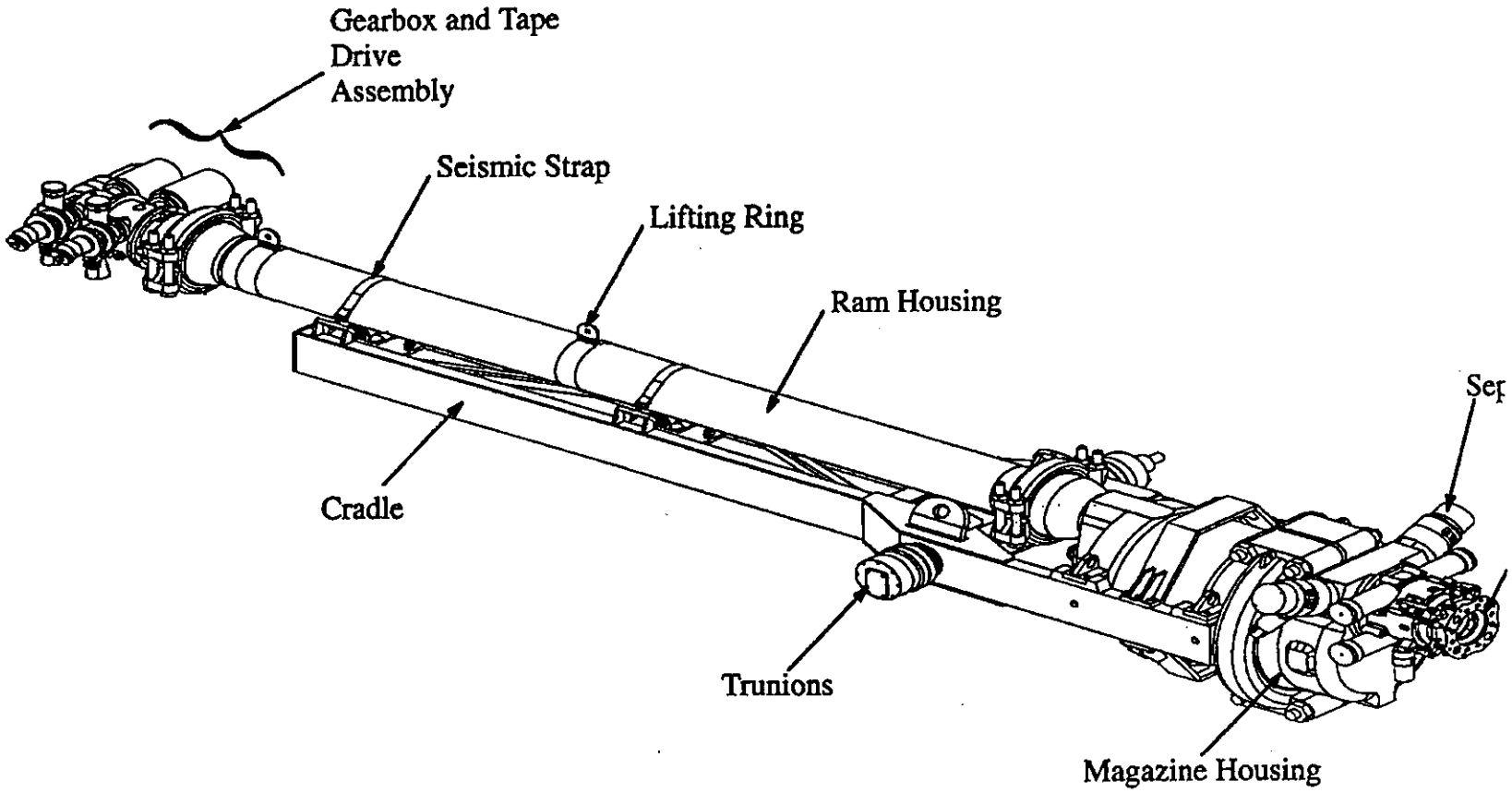


Figure B-10 F/M Head-Cradle Arrangement in CANDU 9

B.4 Equipment Qualified by Testing

This section covers cabinet mounted I&C and electrical equipment. The qualification can be device based or assembly based.

In the assembly base method of qualification, the cabinet will be fully loaded and live loaded during the test. The Required Response Spectrum (RRS) is an envelope FRS.

In the device base method of qualification, the equipment and the cabinet are qualified separately. In the qualification of the cabinet, the cabinet will be instrumented and loaded with dummy weights to simulate the masses of the equipment. The test not only proves the seismic qualification of the cabinet, but also provides information about the natural frequencies, damping, amplification, mode shapes and transmissibility, etc. These dynamic characteristics of the cabinet are then used to generate in-cabinet response spectra for seismic qualification of the equipment.

Cabinets are usually well constructed and resilient. Experiences have shown that as long as the cabinet does not collapse, the equipment mounted inside usually continue to function. Therefore, a cabinet can be screened out, provided that:

- The supports are rigid, and the anchor bolts are strong and have a ductile mode of failure;
- Neighbouring cabinets are either bolted together or well separated, to avoid pounding;
- Equipment mounting is rigid so that there will be no further amplifications; and
- Cables are anchored to the cabinet at point of entry, to prevent pulling of the terminals.

It is desirable to screen out as many equipment qualified by test as possible from the PSA model, for two reasons. First, AECL's qualification tests usually have a factor of safety of at least 2.5. The test levels usually can meet the RLE screening criterion. Second, the median capacity or the fragility level of the equipment is usually not known from the qualification test.

This report provides a lower bound estimate of the HCLPF from the test results, and an estimate of the median capacity A_m.

a) Lower Bound Estimate of HCLPF

As the design moves up from the PGA, through the GRS, the FRS, and the RRS, to the TRS, factors of safety are built-in to specify the requirements at each level. But uncertainties are also incurred along the way. The process can be represented schematically by the following expressions:

$$A_{j+1}=A_j\times F_j\times\varepsilon_j \quad (4.1)$$

$$A_k=A_1\times(F_1\times F_2\times F_3\times....\times F_k)\times(\varepsilon_1\times\varepsilon_2\times\varepsilon_3\times....\times\varepsilon_k) \quad (4.2)$$

$$\varepsilon_{ij}=\varepsilon_i\times\varepsilon_{i+1}\times\varepsilon_{i+2}\times....\times\varepsilon_j=\exp(-\alpha\beta_{ij}) \quad (4.3)$$

where A_{j+1} is the target acceleration at the $(j+1)^{th}$ level of design, whereas F_j is the factor of safety and ε_j is the uncertainty, both at the j^{th} level. α prescribes a confidence level. α=1.65

for a 95% confidence level; α=2.33 for a 99% confidence level $\beta_{ij} = \sqrt{\beta_i^2 + \beta_{i+1}^2 + ... + \beta_j^2}$.

Represents a best estimate of β_i to β_j, under the assumption that they are uncorrelated.

A seismic qualification test, be it an assembly test or a device test, conducted properly meeting the requirements (IEEE and CSA standards) is accepted on the ground that the test has a sufficient margin above the target level and has a low degree of uncertainty. In other words, an acceptable test should leave no doubt about the qualification. This will be so, because

$$\prod_k F_k \times \prod_k \varepsilon_k > 1 \tag{4.4}$$

Therefore,

$$\text{HCLPF} > \text{PGA} \times F_{test} \times \varepsilon_{test} \tag{4.5}$$

where

$$F_{test} = \frac{\phi(\text{TRS})}{\phi(\text{FRS})} \text{ is a measure of the margin between the test and the demand} \tag{4.6}$$

$$\phi(\text{TRS}) = \int w(f)\,\text{TRS}(f)\,df = \int \tau(f) \times \text{TRS}(f)\,df \tag{4.7}$$

$$\phi(\text{FRS}) = \int w(f)\text{FRS}(f)\,df = \int \tau(f) \times \text{FRS}(f)\,df \tag{4.8}$$

where w(f) is a weighting function, which can be chosen as the transfer function τ(f), and ϕ(TRS) maps a function into a number so that a ratio between two functions becomes defined. Directional components are to be combined by the SRSS method.

There are three advantages to define the factor of safety F in the above manner:

F is well behaved;

The dynamic properties of the structure are used;

The transformation is a measure of energy.

Seismic tests are highly repeatable and highly reliable. The test uncertainty ought to be small. IEEE requires only a 10% margin. Therefore, β is to be estimated to meet a 10% margin.

The right-hand-side of Eq. (4.5), equal to $\text{PGA} \times F_{test} \times \varepsilon_{test}$, gives a lower bound estimate of the HCLPF and can be treated as 90% of HCLPF.

b) Median Capacity

A median capacity can be estimated from the test results using the following expression:

$$A_m = \frac{\text{TRS}_c}{\text{RRS}_c} \times F_D \times F_{RS} \times \text{PGA} \tag{4.9}$$

where the subscript c denotes peak clipping. Peak clipping is required if the response spectra are highly peaked. In Eq. (4.9),

$RRS_c = RRS \times C_c \times D_R$

$TRS_c = TRS \times C_T \times C_I$

F_D and F_{RS} are factors of safety related to damping and response defined previously.

Numerical values of the parameters are summarized in the table below.

Factors	Values	β_R	β_U	Remarks
F_D	1.40 1.95	0.09 0.09	0.22 0.28	Cat. B* Cat. A/C
F_{RS}	1.13	0.25	0.19	
C_I	1.1	0	0.05	
C_T	1.0	0	0	
C_C	1.0	0	0	
D_R	1.0	0	0.04	

*Seismic Categories.

B.5 Relay Chatter Evaluation

Relay chatter is either unacceptable or objectionable for the following reasons:

- Causing failure of a safety function.
- Giving misleading indications to invoke incorrect operator actions.
- Causing a component to fail to actuate to the correct position.
- Causing untimely actuation of a component.

NUREG/CR-5499 (Reference B-8) gives guidance for performing relay chatter analysis. This report suggests the following evaluation procedures:

- Develop a seismic relay list, which includes not only seismically qualified relays but also non-qualified relays to evaluate the effects of relay chatter on the function of non-qualified systems.
- Search the list for bad actor relays. Replace them with modern rugged, qualified solid state relays.
- Review circuit logic, system safety functions, and operator recovery actions for screening evaluation.
- Screen relays based on generic relays ruggedness, or qualification results, or fragility results if they are available.
- Screen relays based on effects on plant (i.e., circuit logic and/or operator recovery actions).

- Conduct relay walkdown to ensure the relay cabinets are anchored properly, relays are mounted securely inside the cabinet, there is no unacceptable local flexibility, and there is no cabinet interactions such as pounding.
- Include all the relays which cannot be screened out in the PSA model. The median capacity of the relay may have to be estimated from the generic data.

B.6 References

B-1. Chen et al., 1991, "Procedural and Submittal Guidance for Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities", NUREG-1407, US Nuclear Regulatory Commission.

B-2. Hickman et al., 1983, "PRA Procedure Guide: A Guide to the performance of Probabilistic Risk Assessment for Nuclear Power Plants", NUREG/CR-2300. Prepared by American Nuclear Society and the Institute of Electrical and Electronics Engineers. US Nuclear Regulatory Commission.

B-3. IAEA, 1993, "Probabilistic Safety Assessment for Seismic Events", IAEA-TECDOC-724.

B-4. Riddell R. and Newmark N.M., 1979, "Statistical Analysis of the Response of Nonlinear Systems Subjected to Earthquakes", Report UILU 79-2016, University of Illinois, Urbana, Illinois.

B-5. Salmon M.W. and Kennedy R.P, 1994, "Meeting Performance Goals by the Use of Experience Data", UCRL-CR-120813. Prepared for LLNL and US-DOE.

B-6. Newmark N.M. and Hall W.J, 1978, "Development of criteria for seismic review of Selected Nuclear Power Plants", NUREG/CR-0098, Prepared by Newmark Consulting Engineering Services, Urbana, IL, USA, US Nuclear Regulatory Commission.

B-7. Kennedy R.P. et al., 1984, Volume 1, "Engineering Characterization of Ground Motion. Task 1, Effects of Characteristics of Free-Field Motion on Structural Response", 1985. Volume 2, "Engineering Characterization of Ground Motion, Task 2, Effects of Ground Motion Characteristics on Structural Response Considering Localized Structural Nonlinearities and Soil-Structure Interaction Effects", NUREG/CR-3805, Prepared by Structural Mechanics Associates, Newport Beach, CA USA, Woodward-Clyde Consultants, Walnut Creek, CA USA, US Nuclear Regulatory Commission.

B-8. Hardy G.S. and Ravindra M.K., 1990, "Guidance on Relay Chatter Effects", NUREG/CR-5499, Prepared by Lawrence Livermore Laboratory, USA, US Nuclear Regulatory Commission.

Appendix C

Example of Fire Event Scenario Calculation

C.1 High Voltage Switchgear Room in the Turbine Building (Room T-111)

The following calculation is solely an example to show the application of the fire methodology (see Section 8) to calculate the severe core damage frequency in a high voltage (HV) switchgear room.

C.1.1 Description of the Area

The high voltage switchgear room has an area of 720 m^2. It is assumed that all cables for the Group 1 system pass through this area.

It is considered that there are a sufficient number of fire detectors to ensure the detection of a fire in its early stages. It is also considered that this area has a manually actuated water spray system. Fire hoses and a sufficient number of portable fire extinguishers are also assumed to be available for manual fire fighting.

It is judged that this room contains a significant amount of cables, when the cable risers are considered. In addition to the cables, the following equipment is located in this area:

- two Class IV 11.6KV switchgear buses,
- two Class IV 6.3KV switchgear buses,
- four 11.6 KV/6.3 KV transformers, and
- two Class III 6.3 KV switchgears.

C.1.2 Estimation of Fire Frequency

The ignition sources in this room are cables, six high voltage switchgears and four transformers, as well as transient fires and welding/cutting-induced fires. The distribution panel is not considered in this analysis. The values for fire events frequencies are based on CANDU fire database (Reference C-1) which was developed as part of the GPSA.

The fire frequency is estimated to be 3.16×10^{-4}/yr (this number is based on CANDU fire database adjusted based on fire-retardant cables and the area of the plant being assessed).

The fire frequency of transformers can be estimated as follows:

F (XMFR) = (# of transformers in the room)/(total # of transformers in the plant)× transformer fire frequency

= $4/76\times1.17\times10^{-2}$

$= 6.16\times10^{-4}$/yr

The total number of transformers in the plant is obtained from the fire protection database.

The fire frequency of the high voltage switchgears can be estimated as follows:

F (HSWGR) = (# of high voltage switchgear in the room)/(total # of high voltage switchgear in the plant)×transformer fire frequency

$= 6/6\times3.99\times10^{-3}$

$= 3.99\times10^{-3}$/yr

The total number of high voltage switchgears is obtained from the fire protection database.

The transient and welding and cutting fire frequencies are estimated below.

F (transient) = (# of rooms in this fire zone)/(total # of rooms in the plant)×transient fire frequency

$= 1/262\times3.34\times10^{-2}$

$= 1.27\times10^{-4}$/yr

F (W/C cable) = (# of rooms)/(total # of rooms in the plant)×fire frequency (W/C cable fire)

$= 1/262\times2.45\times10^{-3}$

$= 9.35\times10^{-6}$/yr

F (W/C transient) = (# of rooms)/(total # of rooms in the plant)×fire frequency (W/C transient fire)

$= 1/262\times2.65\times10^{-2}$

$= 1.01\times10^{-4}$/yr

Thus the total fire frequency in this room is estimated to be 5.16×10^{-3}/yr.

C.1.3 Fire Scenarios

In developing the fire scenarios for this fire zone, it is essential to assemble detailed cable routing information, since the major concern for this zone is the damage of cables due to fire. In this analysis, the information is not available, and the scenarios have to be developed that are based on some simple assumptions.

The ignition sources in this fire zone are:

- self-ignited cable fires,
- fires originating in transformers,
- switchgears and panels,
- cable fires caused by welding and cutting,
- transient fires, and

- transient fires caused by welding and cutting.

Self-ignited cable fires can be initiated in any cable tray. Since it is assumed that all cables going to the cable tray room pass through this area along the cable risers, it is considered that all Group 1 safety system cables are located here, including control and monitoring functions. The fraction of the total number of cables that are safety related is assumed to be 0.6.

If the self-ignited cable fire occurs in the cable trays that carry the even or odd train, then it will damage the cables in the cable tray before any fire suppression activity can be initiated. The fire detectors installed in this area will generate fire alarms and send a signal to the automatic fire suppression systems. Fire-fighting activities will also start upon the initiation of the fire alarm. If fire detection fails, then the fire will propagate to other cable trays, becoming a large fire that is not mitigated by fire-fighting activity. If automatic or manual fire suppression is not successful, then the fire will propagate to the upper cable trays in series. Finally, the hot gases generated by the fires will damage the other train, which is located in another cable tray. A preliminary estimation shows that it would take about 55 minutes for the hot gases to damage the cable trays that carry the other train. It is considered that the cables of one train are separated from those of the other train at least by 1.5 m. Therefore, radiant energy alone cannot cause damage to the other train cables.

When self-ignited fires occur in cable trays that do not carry safety related cables, they will first damage cables in that cable tray. If the fire detection or suppression systems fail, then the fire will first damage one of the safety related odd or even train cable trays, after which it will damage the other cable trays. A preliminary estimation shows that it takes about 5 minutes to damage the adjacent safety related cables, and about 55 minutes to damage both odd and even cable trains.

The heat release rate of transformers is quite dependent on the type of transformer. The dry-type transformer is known to have a very low heat release rate, and any fire that is present is not likely to be explosive. A fire in a dry transformer is known to be barely able to sustain itself. The oil-type transformer has quite a high heat release rate, and any fire that is present can easily propagate to other combustible materials. To simplify the evaluation, it is assumed that a severe transformer fire can cause cables that are situated above the transformer to burn, if the fire is not suppressed at an early stage. The small fires are assumed not to propagate or cause damage of other equipment.

Fires in high voltage switchgear are not generally known to propagate to the cables above, if both of the following conditions are met:

- the fire is not explosive, and
- the switchgear either has no ventilation, such as a ventilation louver, or the top penetration seals are fire rated.

The high voltage switchgear considered in this analysis is judged to have ventilation, and it is assumed that the top penetration seals are not fire rated. Therefore, it is considered that a fire in the switchgear can propagate to the cables above, if the fire is not suppressed at an early stage. The fire suppression system installed in this area is considered to be a manually actuated fire

spray system. As such, the first activity for fire suppression will be manual fire suppression using the portable fire extinguishers. If this activity is successful, then it is considered that the fire can damage only the equipment in which it originated. If this activity is not successful, then the fire spray system is assumed to be manually actuated. When the spray system is actuated, it is assumed that the electrical cabinets in the sprayed area become unavailable due to the ingression of sprayed water into the cabinet. It is assumed here that the manual actuation system functions in such a way that it can spray water only on the cabinets that are affected by the fire. If the fire spray system fails, then the fire will propagate to the cables above, causing damage to all cables in the room, will result in the loss of all Group 1 systems.

Cable fires caused by welding and cutting will have scenarios that are similar to the self-ignited cable fires. However, while welding and cutting work is being performed, it is usual to block the fire alarms and fire suppression systems, in order to avoid spurious actuation of these systems. Therefore, in this case, automatic fire suppression is assumed to be ineffective, although the manual fire suppression probability would be greater than that for self-ignited fires, since the firewatcher for the job will suppress the fire as soon as the fire initiates. In this case, it is assumed that the manual fire suppression probability has the same reliability as that of automatic fire suppression.

The transient fires can also cause damage to or ignite the cables, or these fires can cause damage to transformers and switchgears. It is assumed that the lowest cable trays in this area have an elevation of at least 3 m above floor level, with the exception of the cable tray risers. It is estimated that a small transient fire can cause damage to cable trays, but that it cannot ignite the cables that are located higher than 3.0 m. A large fire can cause damage to or ignite the cables. It is considered that if the fire is not suppressed at an early stage, then the transient fire will damage the cables above the fire, and if it is not suppressed within 55 min., then the large transient fire will ignite cables and grow fully, resulting in damage to all the cables in the room.

Transient fires can also cause damage to switchgears and transformers, if these fires occur within a critical distance. Since it is judged that transient fires cannot cause damage to more than two cabinets, the impact of damage to this equipment is not considered further.

Transient fires caused by welding and cutting have the same fire scenarios as above, except that the fire alarms are not active, and the firewatcher will detect and suppress the fire with the same reliability as the automatic fire detections and suppression systems.

If the fire continues to grow, it will damage the other train on its cable tray, and the fire may propagate to other rooms or fire zones, if there are no fire barriers or if the fire barriers are failed. However, the propagation of the fire to other areas will not degrade the safety function of the plant. Therefore, fire propagation from this room to other rooms or fire zones is not considered here.

C.1.4 Fire Scenario Event Tree

The fire scenario is shown on the fire scenario event trees (see Figures C-1 and C-2), and the descriptions of the headings and the branch probabilities are presented below.

Heading T111: Fires in Room T111

This heading represents the frequency of fire occurring in the HV switchgear room T111. The fire frequency is estimated to be 5.16×10^{-3}/yr.

Heading SIG: Not Self-Ignited Cable Fires

This heading represents the fraction of the total fire frequency that is attributable to cable fires in room T111. The fraction is estimated as follows:

F (SIG) $= 3.16\times10^{-4}/5.16\times10^{-3}$

$= 6.13\times10^{-2}$

Heading SWGR: Fires Not in High Voltage Switchgear Gear

This heading represents the fraction of the remaining fire frequency that is attributable to the switchgear fire frequency in room T111. The fraction is estimated as follows;

F (SWGR) $= 3.99\times10^{-3}/(5.16\times10^{-3} - 3.16\times10^{-4})$

$= 0.82$

Heading XMFR: Fires Not in Transformers

This heading represents the fraction of the remaining fire frequency that is attributable to the transformer fire frequency in room T111. The fraction is estimated as follows:

F (SWGR) $= 6.16\times10^{-4}/(5.16\times10^{-3} - 3.16\times10^{-4} - 3.99\times10^{-3})$

$= 0.72$

Heading TR: Not Transient Fires

This heading represents the fraction of the remaining fire frequency that is attributable to the transient fire frequency in room T111. The fraction is estimated as follows:

F (TR) $= 1.27\times10^{-4}/(5.16\times10^{-3} - 3.16\times10^{-4} - 3.99\times10^{-3} - 6.16\times10^{-3})$

$= 0.53$

Heading WIC: Not Welding/Cutting Induced Cable Fires

This heading represents the fraction of the remaining fire frequency that is attributable to the frequency of cable fires due to welding/cutting in room T111. The fraction is estimated as follows:

F (WIC) $= 9.35\times10^{-6}/(5.16\times10^{-3} - 3.16\times10^{-4} - 3.99\times10^{-3} - 6.16\times10^{-4} - 1.27\times10^{-4})$

$= 8.4\times10^{-2}$

The upper branch of this heading represents the remaining fire frequency, i.e., welding/cutting-induced transient fire frequency.

Heading SR: Fires not in the Safety Related Cables or Areas

This heading represents the fraction of safety-related cables to the total cables located in this fire zone. At the time of the analysis, the detailed information about the cables located in this area is not available and thus it cannot be estimated using the design information. Considering that a lot of the normal operating system performs the role of the safety function, a factor of 0.6 is assigned based on the engineering judgement.

Heading WID: Fires not Occurring within Critical Distance of the Cable Trays

This heading represents the likelihood that the transient fires can occur within a critical distance of the cable trays. It is assumed that about 50% of the vacant floor area is overshadowed by overhead cables, with the lowest elevation of the cable trays being 3.0 m. Therefore, the factor for the transient fires would be 0.5.

Heading SF: Not Severe Fires

This heading represents the likelihood of a severe fire, once it has ignited in the ignition source. The severity factor for the transient fires is estimated to be 0.3.

Heading FD: Fire Detection

The fire detection system consists of sensors and protection panels. Only one fire detector is given credit for fire detection.

For the sensors, a generic failure rate of 0.005 is used. The fire protection panel generally performs the function of; 1) processing detector input, 2) sending an alarm signal to the MCR, 3) actuating auto fire suppression systems, and 4) sending signals to close the dampers. Each function is assumed to have a failure rate of 0.01. There could be other causes of detection failure, such as that the detection system is unavailable due to maintenance or loss of power to the control panels, but it is assumed that these other factors are negligible. The failure probability of fire detection is estimated below:

P(FD) = P(failure of sensor) + P (failure of fire protection panel in processing detector input) + P(failure of fire protection in sending the alarm signal)

= 0.005 + 0.01 + 0.01

= 0.025

Heading EMFS: Early Manual Fire Suppression

This heading represents the failure probability of early manual fire suppression, with the condition that fire detection is successful. Self-ignited cable fires that occur in the non-safety-related cable trays can damage a train of adjacent safety related cables, if the fire is not suppressed within 5 minutes.

For fires in HV switchgear, it is assumed that it will take 5 minutes to cause damage to overhead cable trays, the same as that for transient fires.

Transient fires can also cause damage to the cables; within 5 minutes for severe transient fires, and within 10 minutes for small fires.

The probability of manual non-suppression within 5 minutes is 0.8, and the probability for suppression within 10 minutes is 0.7 [2]. However, a transient fire is likely to occur as a result of some operator activities in the area; therefore, the operator(s) is (are) likely to be present in the vicinity of the fire origin, thus enhancing the fire suppression reliability. Taking this presence into account, the failure probability of early manual suppression is assigned to be 0.3 [2].

For the case of welding fires, the failure probability of the early fire suppression system is assumed to be the same as that of the automatic suppression system, i.e., 0.07.

Heading MAFS: Manual Actuation of Fire Spray System

This heading represents the failure probability for the manual actuation of the fire spray system that is installed in this room. The failure probability has two components: the failure of the operator(s) to manually actuate the fire suppression system, and the hardware failure of the water spray system. The failure of the operator(s) to initiate the fire spray system is judged to be negligible, considering that this event already presupposes the success of fire detection and the failure of early manual fire suppression. The failure rate of the hardware is assigned a value of 0.05.

Heading LMFS: Late Manual Fire Suppression

This heading represents the failure probability of late manual fire suppression, with the condition that fire detection is successful. As described above, the hot gas layer that develops can damage all the cables located in this area—the preliminary estimate shows that this will take about 55 minutes. Reference C-2 showed that the probability of manual non-suppression for this case is 0.15.

Heading CCDP: Conditional Severe Core Damage Probability

From the fire scenarios developed for room T111, five fire damage states (FDSs) are defined. FDS1 describes the state in which fires that originate from any ignition source cause damage to cables that are associated with a train/channel of Group 1 safety systems, resulting in loss of that train/channel of safety related systems. The CCDP was calculated above and is estimated to be 1.07×10^{-3}.

FDS2 describes the state in which operators actuate the fire suppression system manually after the failure of early manual fire suppression. The CCDP is dependent on the capability of the spray header to be actuated only for the area in which the fire is burning. It is assumed here that manual actuation would ensure that the spray header is actuated for the specific fire area. In this case, the sprayed water would not cause additional damage to the electrical equipment, due to the ingress of water. The CCDP for FDS2 is estimated to be 1.07×10^{-3}, which is the same value as for FDS1, the state for damage to a train/channel of safety related systems.

FDS3 describes the state in which fires that originate from any ignition source fully develop, generating hot gas layers that can damage cables, resulting in damage to all the cables in the

room. It is assumed that the Group 1 system is entirely unavailable—the CCDP is estimated to be 9.87×10^{-3}, as described above.

FDS4 describes the state in which fires that originate from the transformers do not propagate to damage other equipment or cables. There are four transformers in this room, and the impact of damage will be different for each one. The worst case is judged to be damage to 5314-T1; therefore, the CCDP for this damage state is estimated by assuming that this transformer is damaged. The CCDP for FDS4 is estimated to be 1.54×10^{-6}.

FDS5 describes the state in which fires that originate from the switchgears are suppressed before they can cause damage to other equipment or cables. As described above, there are six switchgears, and the impact of damage will be different for each. The worst case is judged to be damage to 5323-BUE; therefore the CCDP for this damage state is estimated by assuming that this switchgear is damaged. The CCDP for FDS5 is estimated to be 1.66×10^{-4}.

C.1.5 Results of the Analysis

The severe core damage frequency (SCDF) due to fires in room T111 is estimated to be 1.64×10^{-6}/yr. The dominant contributor is a switchgear fire, which contributes 68.2% (1.12×10^{-6}/yr) of the total SCDF for T111. The self-ignited cable fire contributes 23.6% (3.88×10^{-7}/yr) of the total SCDF for T111. The contribution from other ignition sources is considered to be negligible.

The dominant fire scenario involves fires that originate in one of the switchgears in T111, and that are not suppressed at an early stage, causing damage to cables, and resulting in damage to a train/channel of safety related systems. This scenario contributes 35.3% (5.80×10^{-7}/yr) of the total SCDF. The second dominant fire scenario involves fires that originate in one of the switchgears, that are not detected and are able to fully develop, resulting in the loss of all cables in the room. This fire scenario contributes 23.1% (3.80×10^{-7}/yr) of the total SCDF.

As shown above, the dominant fire scenarios are related to switchgear fires. The switchgear fire scenario is developed, assuming that the switchgears have some ventilation and that the top penetration is not fire-rated, resulting in fire propagation to cables above. If there is no ventilation, or if the top penetration is fire-rated, then it is usually considered that fire propagation from the switchgear to the cables above is not likely. A sensitivity study has been performed assuming that a switchgear fire will not propagate to the cables above, and the resulting SCDF is estimated to be 1.18×10^{-6}/yr.

Fire retardant cables are known to have a self-ignited cable fire frequency that is at least ten times lower than the value that is used in the analysis. If all cables located in this zone are considered to be fire retardant, then the SCDF is estimated to be 1.29×10^{-6}/yr.

By combining values for non-propagating switchgears and fire-retardant cables, the SCDF is estimated to be 8.32×10^{-7}/yr.

One potential issue concerning fires in this room is the manually actuated fire spray system. In the analysis, it is assumed that the actuation of the fire spray system will be confined to the area

that is affected by a fire, and that the actuation would not affect the function of other electrical equipment. This functionality would be implemented by the use of fusible links in the spray headers, so that the water would only be sprayed after the temperature of the fuse reaches its melting point. A sensitivity study assumed that the sprayed water renders other electrical equipment unavailable, and showed that the SCDF is significantly higher than that of the base case. The SCDF for this case is estimated to be 7.48×10^{-6}/yr.

C.2 References

1. AECL, 2002, Generic CANDU Probabilistic Safety Assessment – Reference Analysis, AECL Report 91-03660-AR-002.
2. J.A Lambright et al., 1988, Fire Risk Scoping Study: Current Perception of Un-addressed Fire Risk Issues, NUREG/CR-5088.

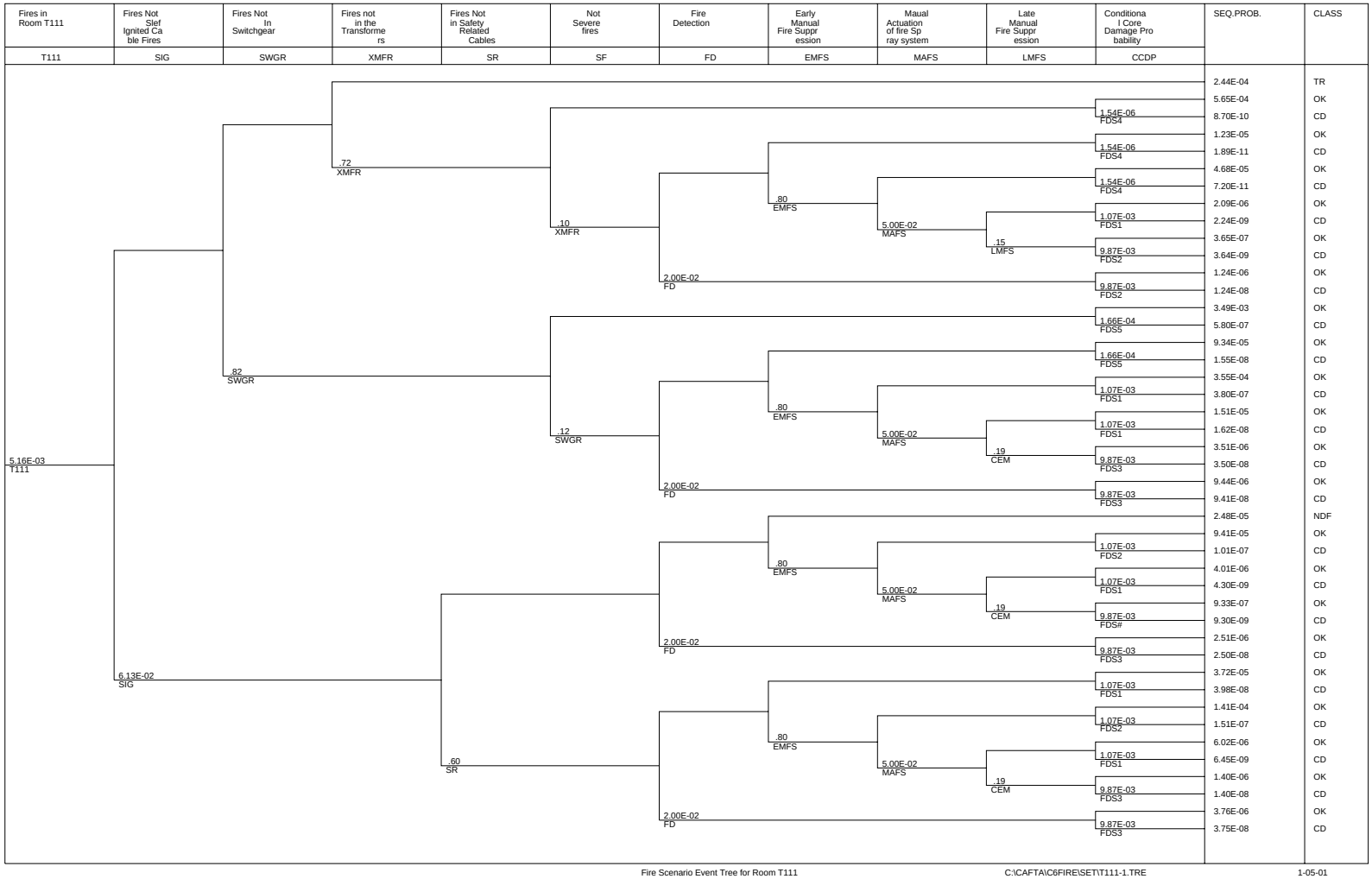


Figure C-1 Fire Scenario Event Tree for FT111 (1)

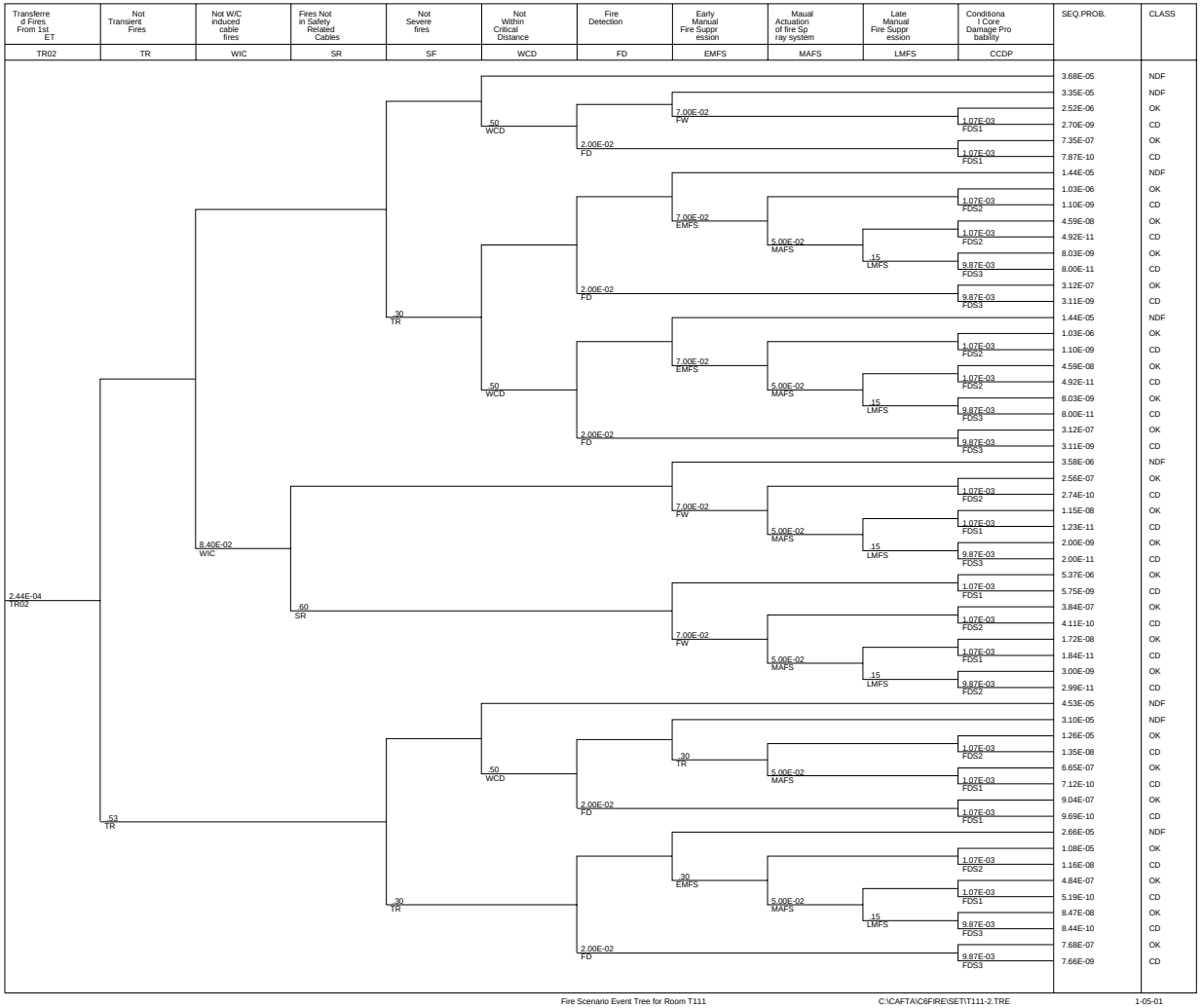


Figure C-2 Fire Scenario Event Tree for FT111 (2)

Appendix D

Example of Flood Scenario Calculation

D.1 Detailed Analysis of Flooding Due to CCW Line Breaks at FL-T01 (Condenser Area)

The following calculation is solely an example to show the application of the flood methodology (see Section 9) to calculate the severe core damage frequency in a condenser area.

The flood area is defined as the open area around the condenser to the top of the turbine building. The flood area also includes the HP feed water heater area.

The PSA-credited equipment located in this area consists of the condensate pumps and the auxiliary condensate pump. However, the flooding concern in this area is the potential propagation of the flood to other areas, since the flooding sources are unlimited and the flooding flow rate is judged to be quite high. The detailed analysis of the flooding scenarios for the flood area is described below.

D.1.1 Flooding Frequency

As described in Section 9, the flooding sources in this area consist of the condenser cooling water, raw service water, and firewater. The condenser cooling water system in this area consists of one inlet square concrete duct, one outlet square concrete duct, four 90-in. inlet pipes to each condenser, four 90-in. outlet pipes from each condenser, four condensers, eight isolation MOVs, and eight expansion joints that are located at the inlet and outlet of each condensers. The inlet and outlet concrete ducts pass below the basement of the turbine building, and are therefore not considered as a flooding source in this analysis.

As per the WASH 1400 aproach (reference D-1, see also Section 9) each inlet and outlet pipe can be considered as one segment. The strainers and filters are considered to be included in the segment. The condensers can be considered as tanks. Thus, the flooding frequency due to the condenser cooling water lines can be estimated as follows:

Fpipe (CCW) $= 8\times1.0\times10^{-9}/\text{hr}\times8760\ \text{hr/yr} = 7.0\times10^{-5}/\text{yr}$

Fcond (CCW) $= 4\times2.7\times10^{-8}/\text{hr}\times8760\ \text{hr/yr} = 9.46\times10^{-4}/\text{yr}$

Fexj (CCW) $= 8\times2.5\times10^{-4}/\text{yr} = 2.0\times10^{-3}/\text{yr}$

Fv/v (CCW) $= 8\times1/18\times1.7\times10^{-7}/\text{hr}\times8760\ \text{hr/yr} = 6.62\times10^{-4}/\text{yr}$

The failure frequency of expansion joints is obtained from the generic data for LWR plants, and the rupture frequency of tanks is used for the failure frequency of condensers. The rupture frequency of tanks is obtained from the generic data for LWRs, see Reference D-2 and Section 9.

The total flood frequency due to the CCW lines is estimated to be 3.68×10^{-3}/yr. As described in Section 9, the flooding frequency can be categorized as follows:

Fccw (large) $= 0.1\times3.68\times10^{-3}/\text{yr} = 3.68\times10^{-4}/\text{yr}$

Fccw (med.) $= 0.3\times3.68\times10^{-3}/\text{yr} = 1.10\times10^{-3}/\text{yr}$

Fccw (small) $= 0.6\times3.68\times10^{-3}/\text{yr} = 2.21\times10^{-3}/\text{yr}$

The area contains 26 fire hose cabinets and 13 wet-pipe sprinklers. Each of the fire lines connecting the fire hose cabinets and each wet pipe sprinkler is considered to be a segment. There are 19 manual valves that are related to fire hose cabinets and 13 manual valves that are related to wet-pipe sprinklers. Thus, the flooding frequency is estimated to be as follows:

Fpipe(FW) $= (26 + 13)\times1.0\times10^{-9}/\text{hr}\times8760\text{ hr/yr} = 3.42\times10^{-4}/\text{yr}$

Fv/v(FW) $= 1/18\times(19 + 13)\times1.3\times10^{-8}/\text{hr}\times8760\text{ hr/yr} = 2.02\times10^{-4}/\text{yr}$

Therefore, the total flooding frequency due to the firewater line is estimated to be 5.44×10^{-4}/yr, and the flooding frequency can be categorized as follows:

Ffw (large) $= 0.1\times5.44\times10^{-4}\text{E-4/yr} = 5.44\times10^{-5}\text{E-5/yr}$

Fccw (med.) $= 0.3\times5.44\times10^{-4}\text{E-4/yr} = 1.63\times10^{-4}\text{E-4/yr}$

F.ccw (small) $= 0.6\times5.44\times10^{-4}\text{E-4/yr} = 3.26\times10^{-4}\text{E-4/yr}$

The total flooding frequency for the flood area FL-T01 is estimated to be 4.22×10^{-3}/yr.

D.1.2 Flood Growth and Flood Scenarios

In this flood area, there are two flooding sources: condenser cooling water, and firewater (as described in Section 9). The flood scenario is dependent on the flooding sources; the flood scenario for the condenser cooling water source only is described below.

D.1.2.1 Flood Due to CCW Line Breaks

If a CCW pipe break occurs, then it will first flood the basement floor pit, at an elevation of 81.70 m above sea level. There are three level switches that detect and alarm any unusual water level in the turbine building. If the water level in the condenser pit in the turbine hall basement continues to rise, then the CCW pump will be automatically stopped.

If the CCW pumps do not automatically stop and operators fail to stop the pumps or fail to isolate the flooding by closing the condenser isolation valves, then the flood level will continuously rise.

The CCW pipes located here connect the concrete duct to the condensers, and are 90 inches in diameter. The normal flow rate of this pipe to the inlet and outlet of the condensers is 542.1 m^3/min. The maximum flood rate would be the lower of the pump run-out flow rate and the orifice flow rate. The orifice flow rate for the line is estimated using the following equation:

$Q_{F.R.}$ $= 0.525\times10^{-7}C\times D^2\times(Dp/\rho)^{½}$
$= 0.525\times1\times90^2\times(30/65.5)^{½}$
$= 2878\ ft^3/sec. = 4894\ m^3/min.$

For the above equation, the differential pressure Dp at the inlet of the condenser is assumed to be 30.0 psig and ρ (65.5 lb/ft^3) is the density of the seawater. The Dp of the outlet pipe would be much less than that of the inlet, and the pipe- break flow of the outlet pipe would be significantly lower than that of the inlet pipe. However, in this preliminary analysis, the pipe-break flow rate estimated above is conservatively applied to all CCW pipe breaks for simplification.

As described in Section 9, the flood flow rate due to CCW pipe breaks can be categorized as follows:

Q_{ccw} (large) $= 4894\ m^3/min$
Q_{ccw} (medium) $= 4894/3\ m^3/min$ $= 1631.3\ m^3/min.$
Q_{ccw} (small) $= 2680/6\ m^3/min$ $= 815.7\ m^3/min.$

The major PSA-credited equipment in this area consists of the main and auxiliary condensate systems. The height of the condensate extraction pump is assumed to be 7.6 ft from the basement. The floodable space, past which the condensate pumps are damaged, can be estimated as follows:

F.V. (condensate pumps) = (floodable surface of the FL-T01)×(vacancy factor)×(critical height)

Floodable surface of the FL-T01 = surface of the TB – surface of FL-T02
$= 87.63\times68.20 - 23.7\times28.1$
$= 5310.4\ m^2$

Therefore,

F.V. (condensate pumps) $= 5310.4\times0.6\times2.316$
$=7381\ m^3.$

When the CCW pumps fail to stop automatically on a TB basement high level signal, the available time for operators to stop the pumps manually is as follows:

Top (large) $= 7381\ m^3/\ 4894\ m^3/min$ $= 1.51$ min.
Top (medium) $= 7381\ m^3/1631.6\ m^3/min$ $= 4.52$ min.
Top (small) $= 7381\ m^3/815.7\ m^3/min$ $= 9.05$ min.

The CCW pumps can be stopped at the MCR—it does not take more than 5 minutes to perform the action if the situation is diagnosed. The failure rate of operators to stop the flood is estimated based on Section 9 to be as follows:

HEP (large-CSP) = 1.0

HEP (medium-CSP) = 1.0

HEP (small-CSP) = 1.0

If the flood flow is not isolated, then the flood level will continue to rise. The FL-T01 flood area is connected to FL-T02 (RCW heat exchanger areas) via two series of doors and steam barrier walls (at an elevation of 85.50 m above sea level), to FL-T03 (feed water pump area) via two series of doors and steam barrier walls, and to FL-T04 (instrument air area) via a door and steam barrier walls (at an elevation of 87.50 m above sea level).

FL-T02 has a RCW heat exchanger pit. A high water level signal in the pit from the switches 67134-LS4491, LS4492, and LS4493 automatically trips the operating RSW pumps, and isolates the RCW heat exchanger valves. For the flood in FL-T01 to propagate to FL-T02, the flood level needs to reach an elevation of 87.50 m first, from which it can then propagate via the door to stair No. 4, then propagating further to FL-T02 via door. The flood can also propagate to FL-T02 under the doors. (If the doors are steam-tight, then there is no gap under the door. It is assumed that the doors are not steam-tight doors).

The flooding of FL-T01 also can propagate to FL-T02 if the steam barrier walls are failed, although the failure probability is judged to be so low, that this propagation scenario can be screened out. (This judgement is based on the assumption that there are no cable or piping penetrations between these two areas that are not properly sealed). The floodable volume for this scenario can be estimated as follows:

F.V. (RCW HX propagation) = F.V. of FL-T01 (to the elevation of the propagation path)

$= 5310.4\ m^2 \times 0.6 \times 5.801\ m$

$= 18483.4\ m^3$

If both doors from FL-T01 to FL-T02 are left open, then the RCW heat exchanger pit will be flooded. Thus, the time required for the flood level to reach the propagation level can be estimated as follows:

Tpro. (large-left open) $= 18483.4\ m^3/4894\ m^3/min = 3.78$ min.

Tpro. (medium-left open) $= 18483.4\ m^3/1631.6\ m^3/min = 11.3$ min.

Tpro. (small-left open) $= 18483.4\ m^3/815.7\ m^3/min = 22.7$ min.

The failure rate of operators to stop the flood is estimated to be the following (see Section 9):

HEP (large-RCWHX-left open door) = 1.0

HEP (medium-RCWHX-left open door) = 1.0

HEP (small-RCWHX-left open door) = diagnosis error + execution error

$= 1.0E\text{-}1 + 0.2 \times 0.2 = 1.4 \times 10^{-1}$

For estimating the error, it is assumed that it will take about 5 minutes to stop the CCW pumps, including the recovery action of the second operator.

If any one of the doors is closed, then additional time is required for the RCW heat exchanger pit to be flooded. The additional time can be estimated by assuming that there is a 1ft. curb around the pit, or by assuming that the level switch activates the RSW auto-stop signal when the elevation reaches 1ft., as follows:

Tadd (RSWP stop) = (floodable area of FL-T02)/(flow rate under the door)

Floodable area of FL-T02 = $23.7 \times 28.1 \times 0.3048$ (1ft)$\times 0.6 = 121.8$ m^3

Flow rate under door = $448.8(0.7021 + 0.0074\ W)\ a\ W\ \{2g(H-a)\}^{0.5}$ gpm.

$= 448.8\ (0.7021 + 0.0074 \times 4) \times 0.125 \times 4 \times \{2 \times 32.2 \times 4\}^{0.5}$

$= 2635$ gpm $= 9.97$ m^3/min.

where a = floor undercut (ft)

W = door width (ft)

g = 32.2 ft^2/sec

H = flood depth

Thus Tadd (RSWP stop) = 121.8/9.97 =12.2 min.

Therefore, the total time available for operators to stop the flood before it causes an automatic stop of the RSW pumps can be estimated as follows:

Top (large-under door)	= 3.78 min. + 12.2 min.	= 16.0 min.
Top (medium-under door)	= 11.3 min. + 12.2 min.	= 23.5 min.
Top (small-under door)	= 22.7 min. + 12.2 min.	= 34.9min.

The failure rate of operators to stop the flood is estimated based on Section 9, and is estimated as follows:

HEP (large-RCWHX-under door) = 1.0

HEP (medium-RCWHX-under door) = diagnosis error + execution error

$= 1.0 \times 10^{-1} + 0.2 \times 0.2 = 1.4 \times 10^{-1}$

HEP (small-RCWHX-under door) = diagnosis error + execution error

$= 1.0 \times 10^{-2} + 0.2 \times 0.2 = 5.0 \times 10^{-2}$

The flood also can propagate to FL-T03 (feed water pump area) via two doors in series. If both doors are left open, then the flood level of FL-T03 would be similar to that of FL-T01, and the feed water pumps would be damaged if the flood reaches the critical height of the pumps. The floodable volume of this area can be estimated as follows:

Floodable volume of FL-T01 & FL-T03 = floodable volume of FL-T01 + floodable volume of FL-T03

Floodable volume of FL-T01 = (floor area of FL-T01)×(vacancy factor)×(ceiling height at 85.50-m-elevation level or below) + (floor area of FL-T01 at 87.50-m-elevation level)×(vacancy factor)×(critical height of the feed water pumps)

$= 5310.4\ m^2 \times 0.6 \times 5.801\ m + 46.9\ m \times 87.63 m \times 0.6 \times 1\ m$

$= 18483.4\ m^3 + 2466\ m^3 = 20949\ m^3$

Floodable volume of FL-T03 = (floor area)×(vacancy factor)×(critical height)

$= 616\ m^2 \times 0.6 \times 1.0 = 369.6\ m^3$

Therefore, the total floodable volume of FL-T01 & T03 is

$= 20949 + 369.6 = 21318.6\ m^3$

The time available for operators to isolate the flood before damage occurs to the feed water pumps due to flood propagation via the door (which is assumed that it has been left open) can be estimated as follows:

Top (large-left open door) $= 21318.6\ m^3/4894\ m^3/min = 4.4$ min.

Top (medium-left open door) $= 21318.6\ m^3/1631.6\ m^3/min = 13.1$ min.

Top (small-left open door) $= 21318.6\ m^3/815.7\ m^3/min = 26.1$ min.

The failure rate of operators to stop the flood is estimated as follows (as per Section 9):

HEP (large-FWP-left open door) = 1.0

HEP (medium-FWP-left open door) = 1.0

HEP (small-FWP-left open door) = diagnosis error + execution error

$= 1.0 \times 10^{-1} + 0.2 \times 0.2 = 1.4 \times 10^{-1}$

If any one of the doors in series is closed, then the flood requires additional time to propagate under the doors. The flood propagation flow rate from FL-T01 to FL-T03 under the doors can be estimated above as 9.97 m^3 (assuming that the average flood height is 4 ft). Thus, the available time for operators to isolate the flood before the feed water pumps are damaged due to flood propagation for this scenario can be estimated as follows:

Top (large-under door) $= 20949\ m^3/4894\ m^3/min + 369.6\ m^3/9.97\ m^3/min = 41.4$ min

Top (medium-under door) $= 20949\ m^3/1631.6\ m^3/min + 369.6\ m^3/9.97\ m^3/min = 50.0$ min.

Top (small-under door) $= 20949\ m^3/815.7\ m^3/min + 369.6\ m^3/9.97\ m^3/min = 62.8$ min.

The failure rate of operators to stop the flood is estimated as follows:

HEP (large-FWP-under door) = diagnosis error + execution error

$= 1.0 \times 10^{-3} + 0.2 \times 0.2 = 4.1 \times 10^{-2}$

HEP (medium-FWP-under door) = diagnosis error + execution error

$= 1.0\times10^{-3} + 0.2\times0.2 = 4.1\times10^{-2}$

HEP (small-FWP-under door) = diagnosis error + execution error

$= 1.0\times10^{-3} + 0.2\times0.2\times0.2 = 9.0\times10^{-3}$

A flood due to a CCW pipe break could also propagate to FL-T04 via a door. The time available for the operators to isolate the flood is expected to be similar to that estimated for FL-T03, and the HEP for isolating the flood before instrument air is damaged can be summarized as follows:

HEP (large-IA-left open door) = 1.0

HEP (medium-IA-left open door) = 1.0

HEP (small-IA-left open door) $= 1.4\times10^{-1}$

HEP (large-IA-under door) $= 4.1\times10^{-2}$

HEP (medium-IA-under door) $= 4.1\times10^{-2}$

HEP (small-IA-under door) $= 9.0\times10^{-3}$

If the flood is not isolated, then the flood level will rise up to affect the next elevation (96.10 m) of the turbine building. The major area of concern at this elevation is the RCW pump area (FL-T05). There are at least two doors between FL-T01 and FL-T05. If both doors are left open and the flood is not isolated until the flood level reaches this area, then it is assumed that the RCW pumps will be damaged due to the flood. The floodable volume for the propagation scenario can be roughly estimated as follows:

F.V. (96.10m) = F.V.(87.50m) + F.V.(addition)

F.V. (87.50m) $= 18483.4\ m^3$

F.V. (addition) = (floor area of 87.50-m-elevation level)×(vacancy factor)×(critical height)

$= 87.63\times47.9\times0.6\times(96.10 - 87.50) = 21206.8\ m^3$

Therefore, F.V. (96.10m) $= 18483.4 + 21206.8 = 39687.0\ m^3$

The time available for operators to isolate the flood can be estimated as follows:

Top (large-left open door) $= 39687\ m^3 / 4894\ m^3/min = 8.1$ min.

Top (medium-left open door) $= 39687\ m^3/1631.6\ m^3/min = 24.3$ min.

Top (small-left open door) $= 39687\ m^3/815.7\ m^3/min = 48.7$ min.

The failure rate of operators to stop the flood is estimated as follows (as per Section 9):

HEP (large-RSWP-left open door) = 1.0

HEP (medium-RSWP-left open door) = diagnosis error + execution error

$= 1.0\times10^{-1} + 0.2\times0.2$

$= 1.4\times10^{-1}$

HEP (small-RSWP-left open door) = diagnosis error + execution error
$= 1.0\times10^{-3} + 0.2\times0.2$
$= 4.1\times10^{-2}$

If the doors are closed, then the flood could propagate to the RCW heat exchanger pit area via the stairs. The additional time available would be similar to that estimated for flood propagation from FL-T01 to FL-T02. Thus, the total available time for operators to isolate the flood before the RSW pumps are automatically stopped due to flood propagation under the door at this level is estimated as follows:

Top (large-under door) = 8.1 min+ 369.6 m^3/9.97m^3/min = 45.2 min
Top (medium-under door) = 24.3 min+ 369.6 m^3/9.97m^3/min = 61.4 min.
Top (small-under door) = 48.7 min+ 369.6 m^3/9.97m^3/min = 85.8 min.

The failure rate of operators to stop the flood is estimated as follows (as per Section 9):

HEP (large-RSWP-under door) = diagnosis error + execution error
$= 1.0\times10^{-3} + 0.2\times0.2$
$= 4.1\times10^{-2}$

HEP (medium-RSWP-under door) = diagnosis error + execution error
$= 1.0\times10^{-3} + 0.2\times0.2\times0.2$
$= 9.0\times10^{-3}$

HEP (small-RSWP-under door) = diagnosis error + execution error
$= 1.0\times10^{-4} + 0.2\times0.2\times0.2$
$= 8.1\times10^{-3}$

The flood level could continue to rise if the flood is not isolated. However, for the flood to propagate to the elevation level described above, additional space must be flooded, in addition to the failure of the flood barriers. If the additional volume is flooded, then this action would allow additional time for operators to intervene. Considering the automatic stop of the CCW pumps, the failure rate of flood barriers, such as doors that are left open, the allowable reaction time for operators, and the limited additional PSA-credited equipment that is located above, it is judged that flood propagation to a higher elevation can be neglected.

D.1.3 Estimation of the Severe Core Damage Frequency

The flood scenarios due to CCW line breaks are shown in Figures D-1, D-2 and D-3. The scenarios resulted in six flood damage states (FDS). Event trees were constructed for each specific FDS (with the mitigating systems being available or unavailable, depending on the flood scenario). The IE frequency is assigned a value of 1.00. The CCDP will be calculated by summing all the SCDFs for each particular event tree.

FDS1 describes the state in which the flood causes damage to the condensate and auxiliary condensate extraction pumps. The CCDP for this damage state is estimated to be 3.57×10^{-5}.

FDS2 describes the state in which the flood causes damage to the condensate system. The flood is not isolated until it rises sufficiently to propagate to the RCW heat exchanger area or the RCW pumps area, resulting in the unavailability of the RCWS. The CCDP for this damage stage is estimated to be 9.87×10^{-3}.

The FDS3 describes the state in which the flood rises sufficiently to propagate to the instrument air area, resulting in the unavailability of the instrument air, in addition to rendering the condensate extraction pumps inoperable. The CCDP of this damage state is estimated to be 1.94×10^{-3}.

The FDS4 describes the state in which the flood propagates to the instrument air area and the RCW pumps/RCW heat exchangers area, causing both systems to become unavailable, in addition to rendering the condensate extraction pumps inoperable. The CCDP for this damage state is estimated to be 9.87×10^{-3}.

The FDS5 describes the state in which the flood rises sufficiently to propagate to the feed water pumps area, resulting in damage to the feed water pumps, in addition to rendering the condensate pumps inoperable. The CCDP for this damage state is estimated to be 4.03×10^{-5}.

The FDS6 describes the state in which the flood causes damage to both the feed water pumps and the instrument air, in addition to rendering the condensate pumps inoperable. The CCDP for this state is estimated to be 1.94×10^{-3}.

The SCDF due to the flood is estimated, by multiplying each CCDP by its corresponding flood scenario frequency. The total SCDF from the flood in TB01 due to CCW line breaks is estimated to be 1.11×10^{-8}/yr.

D.2 References

D-1. USNRC, 1975, WASH-1400, Reactor Safety Study – An Assessment of Accident Risks in US Commercial Nuclear Power Plants, USNRC Report, NUREG – 75/014.

D-2. IAEA, 1988, Component Reliability Data for Use in Probabilistic Safety Assessment, IAEA Report, IAEA-TECDOC-478.

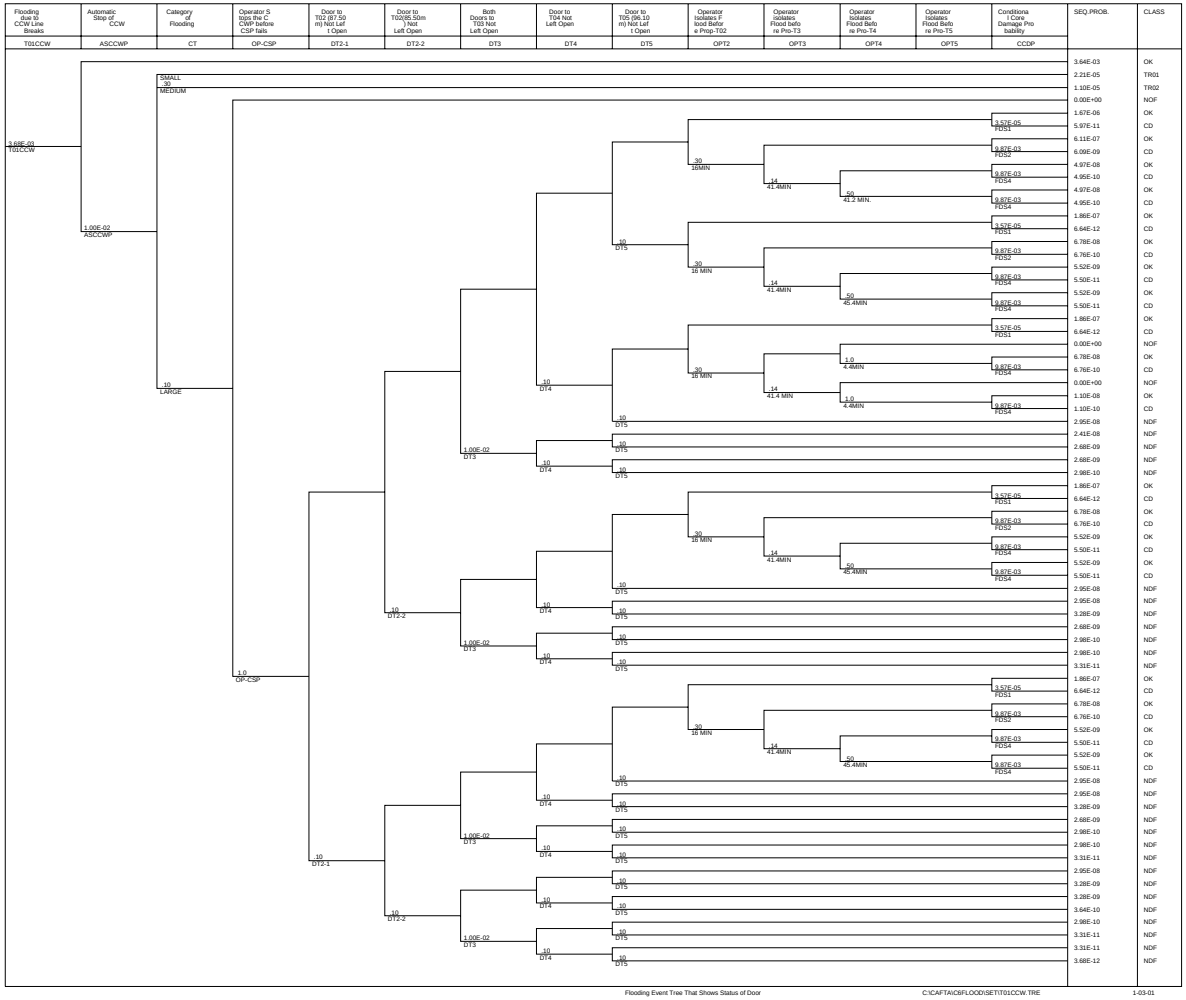


Figure D-1 Flood Scenario Event Tree for FL-T01 (1/3)

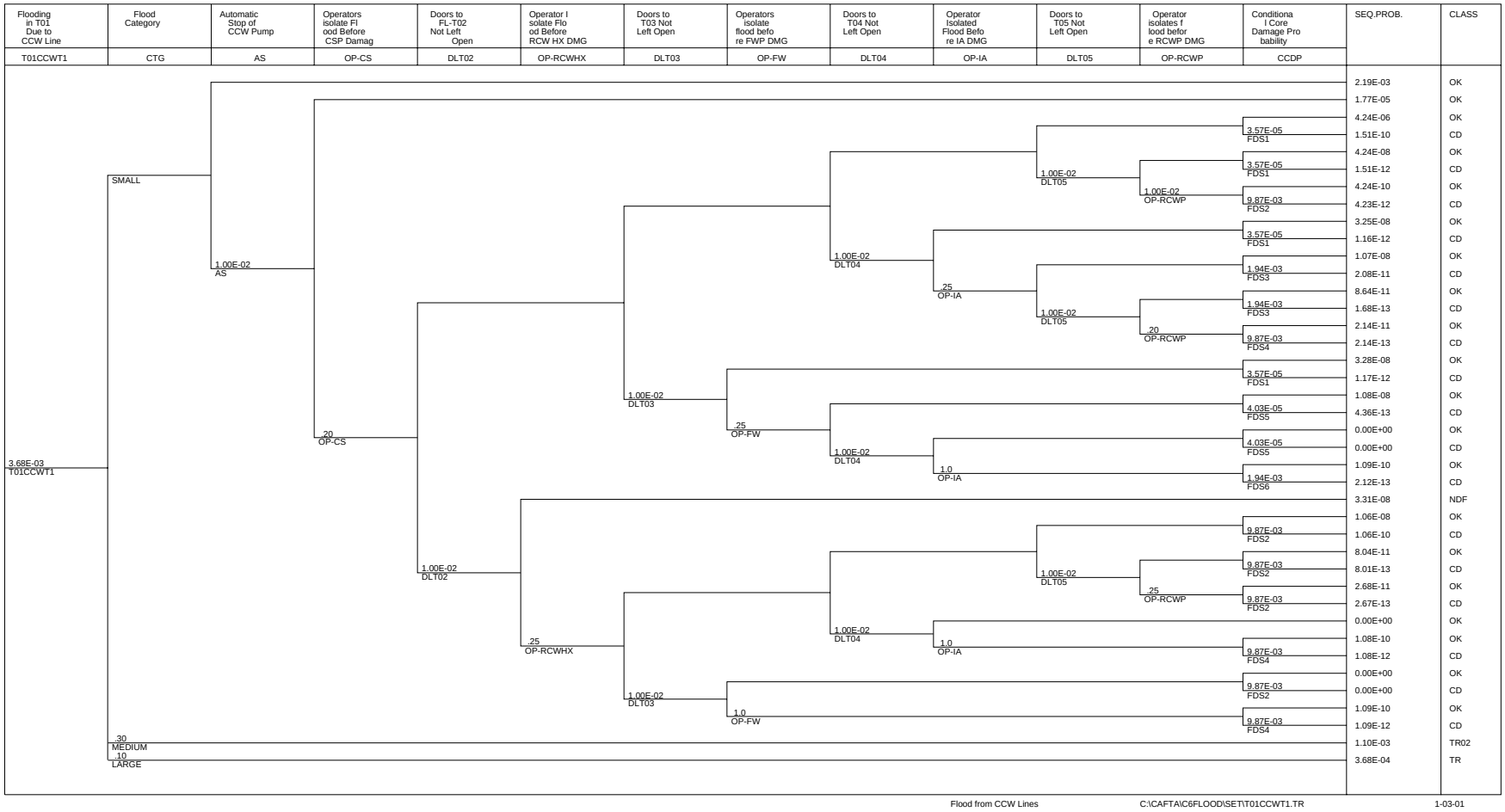


Figure D-2 Flood Scenario Event Tree for FL-T01 (2/3)

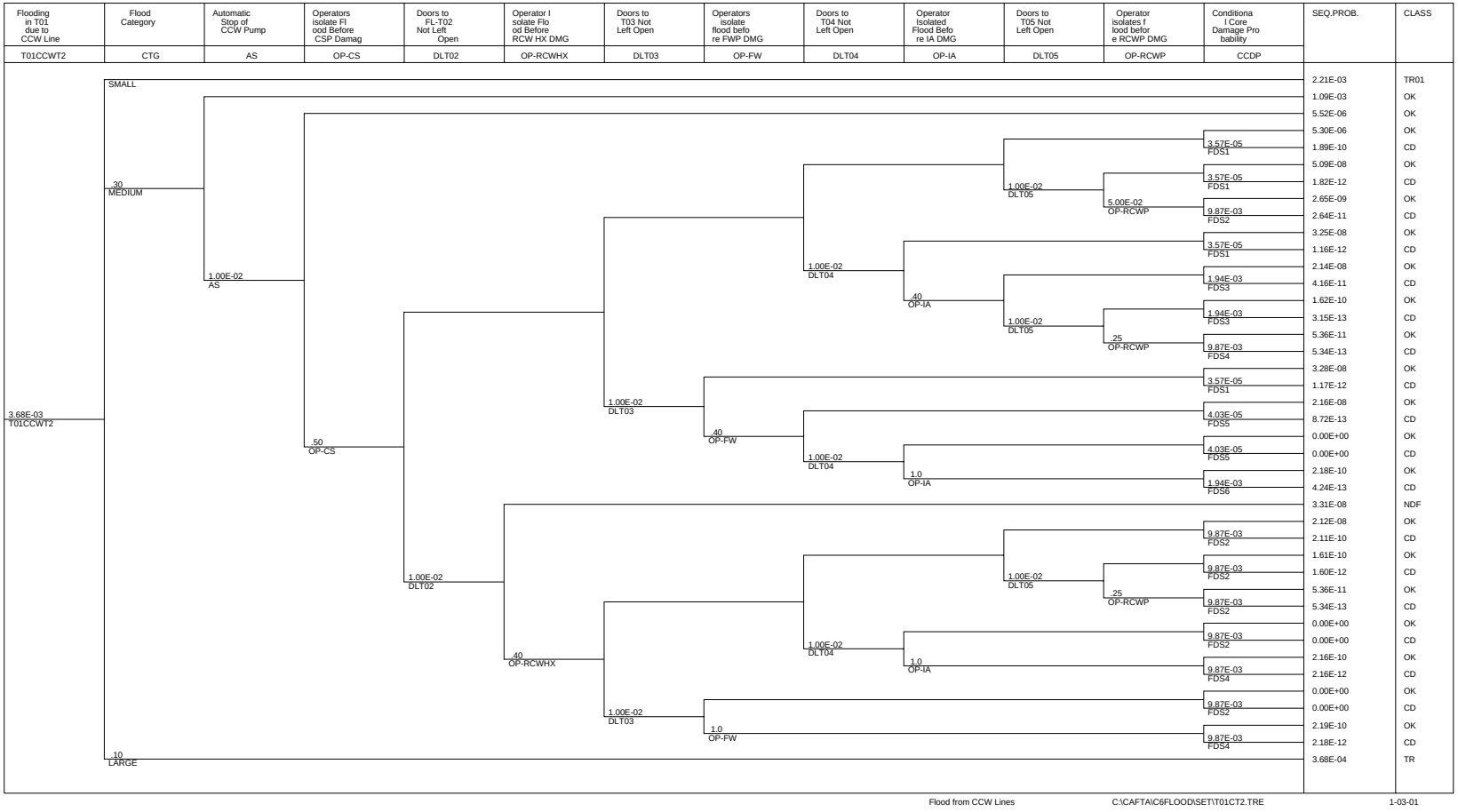


Figure D-3 Flood Scenario Event Tree for FL-T01 (3/3)

Appendix E

General CANDU Single Unit Design Description

E.1 Introduction

The CANDU reactor is a nuclear power plant of the pressure tube type, which utilizes heavy water as a coolant and as a moderator. In common with other thermal power plants, nuclear fuel produces heat, which is subsequently converted into electrical energy. With the CANDU design, the fission reaction in the natural uranium fuel produces heat that is removed by a flow of pressurized heavy water coolant. This heat is transferred to ordinary water in steam generators to produce steam, which drives a turbine and an electrical generator. Most of the electricity produced is supplied through a distribution grid to end consumers while a small fraction is used to drive equipment in the plant.

The following is the description of the major systems in a CANDU nuclear power plant with specific reference to single unit CANDU 6 (700 MWe class reactor) and in some instances CANDU 9 (900 MWe class reactor).

The CANDU fuel cycle and the CANDU 6 flow diagram are presented in Figures E-1 and E-2, respectively.

E.2 Major Systems

E.2.1 Nuclear Steam Supply System

A CANDU nuclear steam supply system's power production process starts like that of any other NSSS, i.e., with controlled fission in the reactor core. However, unlike other reactors, the CANDU reactor is fuelled with natural uranium fuel that is distributed among several hundred fuel channels. Each six-meter-long fuel channel contains 12 fuel bundles. The fuel channels are housed in a horizontal cylindrical tank (called a calandria) that contains a cool heavy water (D_2O) moderator at low pressure. Fuelling machines connect to each fuel channel, as necessary, to provide on-power refuelling; this eliminates the need for refuelling outages. The on-power refuelling system can also be used to remove a defective fuel bundle, in the unlikely event that a fuel defect develops. CANDU reactors have systems to identify and locate defective fuel.

Pressurized heavy water (D_2O) coolant is circulated through the fuel channels and steam generators in a closed circuit. The fission heat produced in the fuel is transferred to the heavy water coolant flowing through the fuel channels. The coolant carries the heat to steam generators, where it is transferred to light water to produce steam. The steam is used to drive the turbine generator to produce electricity.

The NSSS is shown in Figure E-3.

E.2.1.1 Reactor

The reactor comprises a stainless steel horizontal cylinder (called the calandria), which is closed at each end, by end shields. The end shields support the horizontal fuel channels that span the calandria, and provide personnel shielding. The calandria is housed in and supported by a light-water filled, steel-lined concrete structure (the reactor vault), which provides thermal shielding. The calandria contains a heavy water (D_2O) moderator at low temperature and pressure, reactivity control mechanisms, and several hundred fuel channels.

E.2.1.2 Fuel Handling System

The fuel handling system refuels the reactor with new fuel bundles without interrupting normal reactor operation; it is designed to operate at all reactor power levels. The system also provides for the secure handling and temporary storage of new and irradiated fuel.

E.2.1.3 Heat Transport System

The heat transport system (HTS) circulates pressurized heavy water coolant (D_2O) through the reactor fuel channels to remove heat produced by fission in the uranium fuel. The heat is carried by the reactor coolant to the steam generators, where it is transferred to light water, in order to produce steam. The coolant leaving the SGs is returned to the inlet of the fuel channels.

E.2.1.4 Moderator System

Neutrons produced by nuclear fission are moderated (slowed) by the D_2O in the calandria. The moderator D_2O is circulated through systems that cool and purify it, and that control the concentrations of soluble neutron absorbers used for adjusting the reactivity.

E.2.1.5 Reactor Regulating System

This system controls the reactor power to within specific limits, and ensures that station load demands are met. The system also monitors and controls power distribution within the reactor core to optimize fuel bundle and fuel channel power within their design specifications.

E.2.2 Balance of Plant

E.2.2.1 Feedwater and Steam Generator System

The steam generators transfer heat from the heavy water reactor coolant to light water (H_2O) to form steam, which drives the turbine generator. The low-pressure steam exhausted by the low-pressure turbine is condensed in the condensers by a flow of condenser cooling water. The feedwater system processes condensed steam from the condensers, and returns the steam to the SGs via pumps and a series of heaters.

E.2.2.2 Turbine Generator System

The turbine generator system comprises steam turbines that are directly coupled to an alternating current electrical generator operating at synchronous speed.

The steam turbine system is a tandem compound unit, generally consisting of a double flow, high-pressure turbine and three double flow, low-pressure turbines, which exhaust to a high vacuum condenser for maximum thermal efficiency. The condenser may be cooled by sea, lake or river water, or by atmospheric cooling towers.

The electrical generator is a high efficiency hydrogen-cooled machine that is arranged to supply alternating current at medium voltage to the electric power system.

E.2.2.3 Electric Power System

The electric power system comprises a main power output transformer, unit and service transformers, and a switchyard. This system steps up (increases) the generator output voltage to match the electric utility's grid requirements for transmission to the load centres, and also supplies the power needed to operate all of the station services.

The main switchyard portion of the electric power system permits the switching of outputs between transmission lines, and comprises automatic switching mechanisms, and lightning and grounding protection to shield the equipment against electrical surges and faults.

E.2.3 Safety Systems

Four special safety systems (shutdown system number 1 (SDS1), shutdown system number 2 (SDS2), the emergency core cooling system (ECCS) and the containment system) are provided to minimize and mitigate the impact of any postulated failure in the principal nuclear steam plant systems. Safety support systems provide services as required (electric power, cooling water and compressed air) to the special safety systems.

E.3 Major Systems Descriptions

E.3.1 Reactor Assembly

The CANDU reactor assembly includes several hundred channels that are contained in and supported by a horizontal cylindrical tank known as the calandria. The calandria is closed and supported by end shields at each end. Each end shield comprises an inner and outer tubesheet joined by lattice tubes at each fuel channel location, and a peripheral shell. The inner space of the end shields is filled with steel balls and water, and is water-cooled. The fuel channels, which are supported by the end shields, are located on a square lattice pitch. The calandria is filled with a heavy water moderator at low temperature and pressure. The calandria is located in a light-water-filled shield tank. In the case of the CANDU 6 design, the calandria is a steel lined, water-

filled concrete vault, while CANDU 9 and most other CANDU designs utilize a water-filled steel shield tank.

The calandria assembly schematic is presented in Figure E-4.

Horizontal and vertical reactivity measurements and control devices are located between rows and columns of fuel channels, and are perpendicular to the fuel channels.

Each fuel channel supports 12 fuel bundles in the reactor core. The fuel channel assembly includes a zirconium-niobium alloy pressure tube, a zirconium calandria tube, stainless steel end fittings at each end, and four spacers that maintain the separation of the pressure tube and the calandria tube. Each pressure tube is thermally insulated from the cool, low-pressure moderator by the CO_2-filled gas annulus formed between the pressure tube and the concentric calandria tube.

Each end fitting incorporates a feeder connection, through which heavy water coolant enters and leaves the fuel channel. Pressurized heavy water coolant flows around and through the fuel bundles in the fuel channel, and removes the heat generated in the fuel by nuclear fission. Coolant flow through adjacent channels in the reactor is in the opposite direction.

During on-power refuelling, the fuelling machines gain access to the fuel channel by removing the closure plug and the shield plug from both end fittings of the channel to be refuelled.

E.3.2 Fuel

The CANDU 6 fuel bundle consists of 37 fuel elements that are arranged in circular rings. Each element consists of natural uranium in the form of cylindrical pellets of sintered uranium dioxide contained within a Zircaloy 4 sheath, which is closed at each end by an end cap. The 37 elements are held together by end plates at each end to form the fuel bundle. The required separation of the fuel elements is maintained by spacers that are brazed to the fuel elements at the transverse mid-plane. The outer fuel elements have bearing pads that are brazed to the surface of the elements that form the outer circumference of the fuel bundle, in order to support the bundle in the pressure tubes.

The element fuel bundle is presented in Figure E-5.

E.3.3 Fuel Handling System

The fuel handling system:

- provides facilities for the storage and handling of new fuel;
- refuels the reactor remotely, while it is operating at any level of power; and
- transfers the irradiated fuel remotely from the reactor to the storage bay.

E.3.4 Moderator System

About four per cent of reactor thermal power is distributed in the moderator. The largest portion of this heat comes from gamma radiation; additional heat is generated by the moderation (i.e., the slowing down) of the fast neutrons produced by fission in the fuel, and a small amount of heat is transferred to the moderator from the hot pressure tubes.

The moderator system includes two 100 per cent capacity pumps, two 50 per cent flow capacity heat exchangers cooled by recirculated cooling water, and a number of control and check valves. Connections are provided for the purification, liquid poison addition, heavy water (D_2O) collection, supply, and sampling systems.

The moderator pump motors are connected to the medium voltage Class III power supply. In addition, each pump has a pony motor, which is capable of driving the pump at 25 per cent speed, and which is connected to the Class II power supply. In the event of a loss of Class IV power, the power to the main motors is lost and they are not sequenced to re-start automatically. The pony motors will be started on Class II. The cooling water supply to the heat exchangers is re-established after three minutes at a reduced flow rate, following a total failure of Class IV power. The rate of heat removal is sufficient to limit the increase of moderator temperature in the calandria to an acceptable value during a failure of Class IV power, and the subsequent reactor shutdown.

The heavy water in the calandria functions as a heat sink in the unlikely event of a loss-of-coolant accident (LOCA) in the HTS that coincides with a failure of emergency core cooling.

The moderator system is shown in Figure E-6.

The series/parallel arrangement of the system lines and valves permits the output from either moderator pump to be cooled by both of the heat exchangers, and ensures an acceptable level of moderator cooling, when either of the two pumps is isolated for maintenance. Reactor power must be reduced to about 60 per cent if one moderator heat exchanger is isolated.

The primary functions of the moderator system are to:

- provide moderator cooling,
- control the level of heavy water in the calandria, and
- maintain the calandria inlet temperature within specific limits.

E.3.5 Heat Transport System

The HTS circulates pressurized D_2O coolant through the fuel channels to remove the heat produced by fission in the nuclear fuel. The coolant transports the heat to steam generators, where it is transferred to light water to produce steam, in order to drive the turbine. Two parallel HTS coolant loops are provided in the CANDU 6 system. The heat from half of the several hundred fuel channels in the reactor core (380 in the CANDU 6 reactor, 480 in the CANDU 9

reactor) is removed by each loop. The CANDU 6 reactor has two inlet and two outlet headers per loop while CANDU 9 has two inlet headers and one outlet header per loop. D_2O is fed to each of the fuel channels through individual feeder pipes from the inlet headers, and is returned from each channel through individual feeder pipes to the outlet headers. Each HTS loop is arranged in a "figure of 8" configuration, with the coolant making two passes, in opposite directions, through the core during each complete circuit, and with the pumps in each loop operating in series. The coolant flow in adjacent fuel channels is in the opposite direction. The HTS piping is fabricated from corrosion-resistant carbon steel.

The pressure in the HTS is controlled by a pressurizer, which is connected to the outlet headers at one end of the reactor. Valves provide isolation between the two loops in the event of a LOCA.

Figure E-7 shows the HTS, which contain the following key features:

- The SGs consist of an inverted U-tube bundle within a cylindrical shell. Heavy water coolant passes through the U-tubes. The steam generators include an integral preheater on the secondary side of the U-tube outlet section, and integral steam separating equipment in the steam drum above the U-tube bundle. A section through the SG is presented in Figure E-8.
- The heat transport pumps are vertical, centrifugal motor driven pumps with a single suction and double discharge.
- Cooling of the reactor fuel, in the event of an electrical power supply interruption, is maintained by the rotational momentum (flywheels) of the heat transport pumps during reactor power rundown, and by natural convection flow after the pumps have stopped.
- No chemicals are added to the HTS for the purpose of reactivity control.
- Carbon steel piping, which is ductile, and is relatively easy to fabricate and to inspect, is used in the HTS.
- Radiation exposure to personnel is low due to the low fuel defect rate, and is minimized by designing for maintenance, by applying stringent material specifications, by controlling the reactor coolant chemistry, and by providing radiation shielding.

E.3.6 Pressure and Inventory Control System

The heat transport pressure and inventory control system consists of a pressurizer, D_2O feed pumps, feed and bleed valves, and a D_2O storage tank.

This system provides:

- pressure and inventory control for each HTS loop,
- overpressure protection, and
- a controlled degassing flow.

Heavy water in the pressurizer is heated electrically to pressurize the vapour space above the liquid. The volume of the vapour space is designed to cushion pressure transients, without allowing excessively high or low pressures in the HTS.

The pressurizer also accommodates the change in volume of the reactor coolant in the HTS, from zero power to full power. This feature permits the reactor power to be increased or decreased rapidly, without imposing a severe demand on the D_2O feed and bleed components of the system.

When the reactor is at power, the pressure is controlled by the pressurizer; heat is added to the pressurizer via the electric heaters to increase the pressure, and heat is removed from the pressurizer via D_2O steam bleed, in order to reduce pressure. The coolant inventory is adjusted by the feed and bleed circuit. Pressure can also be controlled by the feed and bleed circuit, whenever the pressurizer is isolated at low reactor power, and when the reactor is shut down. This feed and bleed circuit is designed to accommodate the changes in coolant volume that take place during heat-up and cool-down.

The pressure and inventory control system is presented in Figure E-9.

E.3.7 Shutdown Cooling System

The shutdown cooling system (SDCS) is capable of

- cooling the HTS from 177°C down to 54°C, and holding the system at that temperature indefinitely,
- providing core cooling during maintenance work on the SGs and heat transport pumps, when the HTS is drained down to the level of the headers, and
- being put into operation with the HTS at full temperature and pressure.

The shutdown cooling system consists of two independent circuits, one located at each end of the reactor. Each circuit consists of a pump and a heat exchanger that are connected between the inlet and outlet headers of both HTS loops. The system is normally full of D_2O, and is isolated from the HTS by power-operated valves.

The shutdown cooling pumps are sized so that no boiling can occur in any of the fuel channels at decay power level. For normal cool-down, steam from the SGs bypasses the turbine and flows into the turbine condenser to reduce the HTS temperature to 177°C in about 30 minutes.

For cool-down from 177°C to 77°C, the isolating valves at the reactor headers are opened, and all heat transport pumps are kept running. The heat transport pumps force a portion of the total core flow through the shutdown cooling heat exchangers, where the flow is cooled by recirculated cooling water flowing around the heat exchanger coils.

At 77°C, the heat transport pumps are shut down, and the SDCS pumps are started. The system is then cooled to 54°C. D_2O can be drained down to a level that is just above the reactor headers, if required for the maintenance of the SGs or pumps.

The SDCS is presented in Figure E-10.

E.3.8 Reactor Regulating System

The fundamental design requirement of the reactor regulating system (RRS) is to control the reactor power at a specified level and, when required, to manoeuvre the reactor power level between set limits at specific rates. The RRS combines the reactor's neutron flux and thermal power measurements, reactivity control devices, and a set of computer programs to perform three main functions:

- monitor and control total reactor power to satisfy station load demands,
- monitor and control the reactor flux shape, and
- monitor important plant parameters and reduce reactor power at an appropriate rate, if any parameter is outside specified limits.

E.3.8.1 Control

Reactor Regulating System action is controlled by digital computer programs, which process the inputs from various sensing devices and activate the appropriate reactivity control devices. All measurement and control devices are located perpendicular to and between rows or columns of fuel channels, in the low-pressure moderator.

E.3.8.2 Computer Programs

The principal computer programs employed provide the following functionality:

- reactor power measurement and calibration,
- the demand power routine,
- reactivity control and flux shaping,
- the setback routine,
- the stepback routine, and
- the flux mapping routine.

E.3.8.3 Instrumentation

The principal instrumentation utilized for reactor regulation includes

- the ion chamber system,
- the self-powered, in-core, flux detector system, and
- thermal power instrumentation.

The nuclear instrumentation systems are designed to measure reactor neutron flux over the full operating range of the reactor. These measurements are required as inputs to the RRS and to the safety systems. The instrumentation for the safety systems is independent of that utilized by the RRS.

E.3.8.4 Reactivity Control Devices

Short-term global and spatial reactivity control is provided by

- light water zone control absorbers,
- mechanical control absorbers,
- adjusters, and
- soluble poison addition to and removal from the moderator.

The zone control system maintains a specified amount of reactivity in the reactor, this amount being determined by the specified reactor power setpoint. If the zone control system is unable to do this, then the program in the RRS calls on other reactivity control devices. Adjusters are removed from the core for positive reactivity shim. Negative reactivity is provided by the mechanical control absorbers, or by the automatic addition of poison to the moderator.

E.3.8.5 Stepback/Setback Routines

In addition to controlling reactor power to a specified setpoint, the RRS also monitors a number of important plant parameters. If any of these parameters is outside specified limits, then reactor power is reduced. This power reduction may be fast (stepback) or slow (setback), depending on the possible consequences of the particular parameter excursion. The power reduction/shutdown functions provided by the RRS are completely separate and independent of the two special safety shutdown systems.

E.3.8.6 Ion Chamber System

Three ion chambers are employed in the RRS for measuring neutron flux in the range from 10^{-7} to 15 per cent of full power. Compensation is not required, since adequate discrimination against gamma rays is achieved by employing appropriate materials in the detector, and by gamma shielding in the construction of the ion chamber housings. These ion chambers are located in housings at one side of the core. In addition to one ion chamber for the RRS, each housing also contains an ion chamber and shutter for SDS1. Each of the three channels consists of an ion chamber and amplifier unit. The solid-state amplifiers upgrade the ion chamber outputs to suitable input signal levels for processing in the control computers. Three similar ion chambers, mounted on the other side of the core, provide inputs to SDS2.

E.3.8.7 Self-Powered In-Core Flux Detectors

In the high power range (above 15 per cent power), self-powered in-core flux detectors provide the required spatial flux information that is not available from the ion chambers.

Two types of in-core detectors are used in the reactor: one type uses platinum as the sensitive emitter material, while the other uses vanadium. The sheaths of both types are made of Inconel. The platinum detectors are fast acting and sensitive to both neutrons and gamma rays, and because of their prompt response to flux changes, they are used in the RRS and in the two shutdown systems. The vanadium detectors are sensitive to neutrons, but because of a relatively slow response to flux changes, they are used only in the flux mapping system.

The in-core flux detectors of the regulating system and of SDS1 are mounted vertically in the core, while those of SDS2 are mounted horizontally in the core.

E.3.8.8 Light Water Zone Control Absorbers

Light water (H_2O) is a neutron absorber (poison) in the heavy water cooled and moderated CANDU reactor. The liquid zone control system takes advantage of this fact to provide short-term global and spatial reactivity control in the CANDU reactor core.

The liquid zone control system in the reactor consists of six tubular, vertical zone control units that span the core. Each zone control unit contains either two or three zone control compartments, providing a total of 14 zone control compartments in the reactor. The zone control units are located such that the 14 zone control compartments are distributed throughout the core, thereby dividing the core into 14 zones for the purposes of flux control. Flux (power) in each zone is controlled by the addition or removal of light water to or from the liquid zone control compartment in that zone. This is accomplished by controlling the level of light water in the liquid zone control compartment.

E.3.8.9 Mechanical Control Absorbers

Four mechanical control absorbers, mounted above the reactor, can be driven in or out of the core at variable speeds, or they can be dropped by gravity into the core, between columns of fuel channels, by releasing a clutch. These absorbers are normally parked out of the core; they are driven in to supplement the negative reactivity from the light water zone control absorbers, or they are dropped to effect a fast reduction in reactor power (stepback). When inserted, the mechanical control absorbers also help to prevent the reactor from going critical when the shutoff rods of SDS1 are withdrawn, and they remain interlocked in this inserted position, until SDS1 is energized and available.

E.3.8.10 Adjusters

Adjusters are cylindrical neutron absorbing rods. A CANDU reactor typically has 21 vertically mounted adjuster rods, which are normally fully inserted between columns of fuel channels for flux shaping purposes.

The removal of adjusters from the core provides positive reactivity to compensate for xenon build-up following large power reductions, or in the event that the on-power refuelling system is unavailable. The adjusters are capable of being driven in and out of the reactor core at variable speed to provide reactivity control. The adjusters are normally driven in banks, the largest bank containing five rods.

E.3.9 Feedwater and Main Steam System

E.3.9.1 Feedwater System

Feedwater from the regenerative feedwater heating system is supplied separately to each steam generator. The feedwater is pumped into the SGs by three 50 per cent capacity multi-stage feedwater pumps, with the flow rate to each SG being regulated by feedwater control valves. A check valve in the feedwater line to each SG is provided to prevent backflow, in the unlikely event of feedwater pipe failure. One auxiliary feedwater pump is provided, and can supply four per cent of the full power feedwater requirements either during shutdown conditions, or if the main feedwater pumps become unavailable.

The chemistry of the feedwater to the SGs is precisely controlled by demineralization, deaeration, oxygen scavenging, and pH control. A blowdown system is provided for each steam generator, which allows impurities collected in the SGs to be removed, in order to prevent their accumulation and possible long-term corrosive effects.

The feedwater system is presented in Figure E-11.

E.3.9.2 Steam Generators and Main Steam Systems

Reactor coolant (heavy water) flows through small tubes (arranged in an inverted, vertical U-tube bundle) within each of the four steam generators, and transfers heat to the re-circulated water outside the tubes, thus producing steam. Moisture is removed from the steam by steam-separating equipment located in the drum (upper section) of the SG. The steam then flows via four separate steam mains, through the reactor building wall to the turbine, where they connect to the turbine steam chest.

The steam pressure is normally controlled by the turbine governor valves, which admit steam to the high-pressure stage of the turbine. If the turbine is unavailable, then up to 70 per cent of full power steam flow can bypass the turbine and go directly to the condenser. During this operation, pressure is controlled by the turbine bypass valves. Auxiliary bypass valves are also provided to permit up to 10 per cent of full power steam flow (during low power operation).

Steam pressure can be controlled by discharging steam directly to the atmosphere via four atmospheric steam discharge valves, which have a combined capacity of 10 per cent of the full power steam flow. These valves are used primarily for control during the warm-up or cool-down of the HTS.

Overpressure protection for the steam system is provided by four safety relief valves that are connected to each steam main.

The steam system is presented in Figure E-12.

E.3.9.3 Turbine Generator System

The system consists of a turbine generator unit and associated condensing and feedwater heating systems.

Steam produced in the SGs enters the high-pressure turbine, and its water content increases as it expands through this high-pressure stage. Upon leaving this stage, the steam passes through separators, where the water is removed; the steam then passes through reheaters, where it is heated by live steam taken directly from the steam mains. The reheated steam then passes through the low-pressure turbines into the condenser, where it condenses to water. The water is then returned to the SGs via the feedwater heating system.

E.3.9.4 Steam Turbine

The steam turbine system is a tandem compound unit, directly coupled to an electrical generator by a single shaft. It comprises one double-flow, high-pressure cylinder followed by external moisture separators, live steam reheaters, and three double-flow, low-pressure cylinders. The turbine is designed to operate with saturated inlet steam. The turbine system has main steam stop valves, governor valves, and reheat intercept and emergency stop valves. All of these valves close automatically in the event of a turbine protection system trip.

E.3.9.5 Generator

The generator is a three-phase, four-pole machine. The generator typically operates at 1800 r.p.m. to serve 60 cycle electrical systems, and at 1500 r.p.m. to serve 50 cycle systems. The generator will vary according to a country's local conditions and manufacturer.

The associated equipment consists of a solid state automatic voltage regulator that controls a thyristor converter, which supplies the generator field via a field circuit breaker, generator slip rings and brush gear.

The main power output from the generator to the step-up transformer is by means of a forced-air-cooled, isolated phase bus duct, with tap offs to the unit service transformer, excitation transformer, and potential transformer cubicle.

Power is transmitted from the generator terminals to the main output transformer and the unit service transformer at the generator nominal operating voltage.

E.3.10 Electric Power System

E.3.10.1 Power Classification

The station services power supplies are classified in the order of their levels of reliability requirement. The reliability requirement of these power supplies is divided into four classes that range from uninterruptible power, to that which can be interrupted with limited and acceptable consequences.

The CANDU 6 electrical power system is presented in Figure E-13.

E.3.10.1.1 Class IV Power Supply

Power to auxiliaries and equipment that can tolerate long duration interruptions without endangering personnel or station equipment is obtained from the Class IV power supply. This class of power supply comprises

- Two primary medium voltage buses, each connected to the secondary windings of the system service and unit service transformers in such a way that only one bus is supplied from each transformer.
- Two medium voltage buses supplied from the secondary windings of two transformers on the primary medium voltage buses. These buses supply the main heat transport pumps, feed pumps, circulating water pumps, extractor pumps and chillers.

A complete loss of Class IV power will initiate a reactor shutdown.

E.3.10.1.2 Class III Power Supply

Alternating current (AC) supplies to auxiliaries that are necessary for the safe shutdown of the reactor and turbine are obtained from the Class III power supply, with a standby diesel generator back-up. These auxiliaries can tolerate short interruptions in their power supplies. This class of power supply comprises

- Two medium voltage buses supplied from the secondary windings of the two transformers on the Class IV primary medium voltage buses. These buses supply power to the pumps in the service water system, emergency core cooling system, moderator circulation system, shutdown cooling system, HTS feed lines, steam generator auxiliary feed line, and the air compressors and chillers.
- A number of low voltage buses.

E.3.10.1.3 Class II Power Supply

Uninterruptible AC supplies for essential auxiliaries are obtained from the Class II power supply, which comprises:

- Two low voltage AC three-phase buses, which supply critical motor loads and emergency lighting. These buses are each supplied through an inverter from a Class III bus via a rectifier in parallel with a battery;
- Three low voltage AC single-phase buses, which supply AC instrument loads and the station computers. These buses are fed through an inverter from Class I buses, which are fed from Class III buses via rectifiers in parallel with batteries.

In the event of an inverter failure, power is supplied directly to the applicable low voltage bus and through a voltage regulator to the applicable instrument bus. If a disruption or loss of Class III power occurs, then the battery in the applicable circuit will provide the necessary power without interruption.

E.3.10.1.4 Class I Power Supply

Uninterruptible direct current (DC) supplies for essential auxiliaries are obtained from the Class I power supply, which comprises:

- Three independent DC instrument buses, each supplying power to the control logic circuits and to one channel of the triplicated reactor safety circuits. These buses are each supplied from a Class III bus via a rectifier in parallel with a battery;
- Three DC power buses, which provide power for DC motors, switchgear operation and for the Class II AC buses via inverters. These DC buses are supplied from Class III buses via a rectifier in parallel with batteries.

The station battery banks are all continuously charged by the Class III power supply. In the event of a Class III power disruption, the battery banks will provide power to their connected buses.

E.3.10.2 Standby Generators

Standby power for the Class III loads is supplied by two (or more) diesel generator sets, housed in separate rooms with fire resistant walls. Each diesel generator can supply the total safe shutdown load of the unit. The Class III shutdown loads are duplicated, with one complete system being fed from each diesel generator. In the event of a failure of Class IV power, the two diesel generators will start automatically.

The generators can be up to speed and ready to accept a load in less than two minutes. The total interruption time is limited to three minutes. Each generator automatically energizes half of the shutdown load through a load sequencing scheme. There is no automatic electrical tie between the two generators, nor is there a requirement for them to be synchronized. In the event of one generator failing to start, the total load will be supplied from the other generator.

E.3.10.3 Emergency Power Supply System

The emergency power supply system (EPS) can provide all shutdown electrical loads that are essential for safety.

This system and its buildings are seismically qualified to be operational after an earthquake. The system provides a backup for one group of safety systems (SDS2, emergency water supply system (EWS), secondary control area (SCA)) if normal electric supplies become unavailable or if the main control room (MCR) becomes uninhabitable. The system comprises two diesel generating sets that are housed in separate fire resistant rooms; they are self-contained, and are completely independent of the station's normal services. There is adequate redundancy provided in both the generating distribution equipment and the loads.

E.3.11 Station Instrumentation and Control

Digital computers are used for station control, alarm annunciation, graphic data display and data logging. The system consists of two independent digital computers (DCCX and DCCY), each capable of station control.

Both computers run continuously, with programs in both machines being switched on, but with only the controlling computer's outputs being connected to the station equipment. In the event that the controlling computer fails, the control of the station is automatically transferred to the “hot standby” computer.

E.3.12 Safety Systems

E.3.12.1 Overall Requirements

Like most metals, fuel sheaths weaken at very high temperatures. Therefore, fuel sheath integrity is at risk if a component failure causes the cooling of the fuel to be reduced relative to the power that it produces.

If such a failure occurs, then the reactor process systems can often stop the failure’s course or moderate its effects. Special safety systems back up the reactor process systems. The safety systems are independent of the process systems and of each other, both functionally and physically, and are not used in the day-to-day operation of the plant. They can, if needed, shut down the reactor (shutdown systems), refill the reactor fuel channels with coolant and remove residual or "decay" heat from the fuel (emergency core cooling system), and prevent release to the environment of radioactivity that may escape from the reactor (containment systems).

Supporting these special safety systems are systems that provide alternate sources of electrical power (emergency power supply system) and cooling water (emergency water supply system).

A fundamental requirement of the CANDU safety design is to provide complete physical separation and functional independence of the special safety systems from the process system and from each other.

E.3.12.2 Safety Grouping

To provide defence against low probability incidents such as local fires or missiles (turbine blades, etc.), the station safety systems and safety support systems are separated into two groups that are functionally and physically independent of each other. Each group is designed to perform the following functions:

- shut down the reactor;
- remove decay heat from the reactor;
- limit the release of radioactive material; and
- supply the necessary information for post-accident monitoring.

The following systems provide these safety functions:

- SDS1 in Group 1 and SDS2 in Group 2, which shut down the reactor.
- The process systems, including normal electric power and service water systems in Group 1 and the EWS and EPS in Group 2 to remove decay heat.
- The main control room or the secondary control area, which is used for post-accident monitoring.

Additional in CANDU 6, the ECCS is located in Group 1 while the containment system belongs to Group 2.

E.3.12.3 Shutdown Systems

There are two ”full capability” reactor shutdown systems, each capable of shutting down the reactor during any postulated accident condition.

The two shutdown systems are functionally and physically independent of each other and of the reactor regulating system, in the following manner:

- Functional independence is achieved by utilizing different shutdown principles; i.e., solid shutoff rods for SDS1, and direct liquid poison injection into the moderator for SDS2.
- Physical independence of the shutdown systems is achieved by positioning the shutoff units vertically through the top of the reactor, and by positioning the poison injection tubes horizontally through the sides of the reactor.

E.3.12.3.1 Shutdown System Number 1

Shutdown system number 1 is the primary method of quickly shutting down the reactor, when certain parameters enter an unacceptable range. This shutdown system employs a logic system, which is independent of those utilized by SDS2 and the RRS, and which senses the requirement for a reactor trip. The shutdown system then de-energizes the direct current clutches to release the absorber element portion of the shutoff units, allowing them to drop between the columns of

fuel channels, into the moderator. Each shutdown rod is equipped with a spring that provides an initial acceleration.

The design philosophy is based on triplicating the measurement of each variable, and initiating a protection action when any two of the three trip channels is tripped by any variable or combination of variables.

Typical variables (trip parameters) that can initiate a reactor trip through SDS1 are

- high neutron power;
- low gross coolant flow;
- high heat transport pressure;
- high rate log neutron power;
- high building pressure;
- low steam generator level, and
- low pressurizer level.

E.3.12.3.2 Shutdown System Number 2

An alternate method of quickly shutting down the reactor is the rapid injection of poison (concentrated gadolinium nitrate solution) into the moderator through horizontal tubes that enter one side of the calandria, and that terminate as nozzles that span the calandria, between rows of fuel channels. There are six SDS2 poison injection nozzles in a CANDU 6 reactor. This shutdown system employs an independent logic system that senses the requirement for a reactor shutdown and opens fast-acting valves located in the line between a high-pressure helium tank and the poison tanks. The released helium expels the poison from the tanks, through the injection nozzles into the moderator.

Trip parameters that are similar to those used to activate SDS1 also initiate a trip condition on SDS2. The instrumentation for these trips, however, is physically and electrically separated.

Shutdown system number 2 is presented in Figure E-14.

E.3.12.4 Emergency Core Cooling System

E.3.12.4.1 System Operation

The emergency core cooling system provides ordinary water to the HTS to compensate for the heavy water coolant lost in a postulated loss-of-coolant accident, and recirculates (and cools) the heavy water/light water mixture that collects in the reactor building floor to the reactor headers, in order to maintain fuel cooling in the long term.

The CANDU 6 ECCS has three stages of operation: high, medium and low pressure. During a LOCA, ECCS operation is triggered when the HTS pressure drops to 5.5 MPa (800 psia) and a loop isolation system (independent of ECCS logic) closes the applicable valves to isolate the two HTS loops.

E.3.12.4.2 High Pressure Operation

The initial LOCA signal isolates the two HTS loops, opens the gas inlet, high-pressure injection (HPI) and the applicable HTS H_2O/D_2O isolation valves simultaneously, and also initiates the rapid cooling of the SGs. The latter is accomplished by opening the main steam safety valves on the SG secondary side, which discharges steam. Emergency coolant (ordinary water) is forced from the ECCS water tanks into the ruptured HTS loop, when pressure in that loop falls below the injection pressure - 4.14 MPa (600 psia). The elapsed time to ECC injection can be about 10 seconds for a maximum pipe-size break. Coolant escaping from the ruptured circuit collects in the reactor building sump. The minimum time to empty the water (maximum break) is 2.5 minutes. The entire high-pressure phase is initiated automatically.

When the ECCS water tanks reach a predetermined low level, the HPI valves close automatically.

E.3.12.4.3 Medium Pressure Operation

The medium pressure stage consists of water supplied from the dousing tank, which is delivered to the HTS headers via the ECC pumps. The valves connecting the dousing tank to the ECC pumps are opened on the LOCA signal, while the medium pressure injection (MPI) valves open on a delayed signal.

There are two ECC pumps, each capable of providing 100 per cent of the water requirements at a pressure of 150 psia. Class IV electrical supply to the ECCS pumps is backed up by Class III power and the EPS.

E.3.12.4.4 Low Pressure Operation

As the dousing tank nears depletion, the valves between the reactor building sump and the ECC pumps open (for recent CANDU 6 design). Water collected in the reactor basement is returned to the HTS via heat exchangers to provide long term fuel cooling.

The heat exchanger maintains the temperature of the coolant flow at about 49°C. The temperature of the water (D_2O and H_2O) from the sump would be about 66°C at the ECC pumps.

For small breaks, decay heat is transferred to the SGs and is rejected via the main steam safety valves, which have a total steam flow capacity greater than that of the SGs. For large breaks, the break itself acts as the heat sink, in combination with ECC injection.

E.3.12.4.5 Backup Decay Heat Removal (Moderator Heat Sink)

In the very unlikely event that the ECCS fails during or following a LOCA, decay heat is transferred from the fuel to the moderator by radiation and conduction. The centre element of the CANDU fuel bundle is only 50 mm from the cool heavy water moderator; hence, decay heat removal from the fuel following shutdown is assured without melting the uranium dioxide, even if no coolant is present in the fuel channel.

E.3.13 Containment

Containment comprises a number of systems that operate to provide a sealed envelope around the reactor systems, if an accidental radioactivity release occurs from these systems. The following structures and systems form the containment system:

- a lined, post-tensioned concrete containment structure,
- an automatic dousing system,
- air coolers,
- access airlocks,
- an automatically initiated containment isolation system, and
- hydrogen igniters and/or recombination units (for recent CANDU 6 design).

If a large break in the HTS occurs, then the building pressure will rise, and at a pressure of 3.5 kPa (0.5 psig), containment closure will be initiated (if closure has not already been initiated by an activity release signal). Other sensors associated with the reactor will have caused a reactor trip and ECCS operation. The dousing system will start to operate automatically at a pressure of 14 kPa (2 psig), and will stop when the overpressure drops to 7 kPa (1 psig). The operation can be continuous or cyclic, depending on the size of the break.

Condensation on the building walls, as well as operation of the building air coolers subsequently reduces the pressure from an excess of 7 kPa (1 psig) to about atmospheric conditions.

For a small break in the HTS, the building coolers will condense the discharging HTS coolant, and will maintain the building pressure at the atmospheric level.

Gamma activity, if sensed in the ventilation discharge ducts and/or vapour recovery system, will initiate signals that close the containment dampers and valves to prevent activity releases.

A fission product release in a fuelling machine room, caused by damage to one or more fuel elements, would be sensed in the ventilation discharge ducts, and would initiate containment isolation.

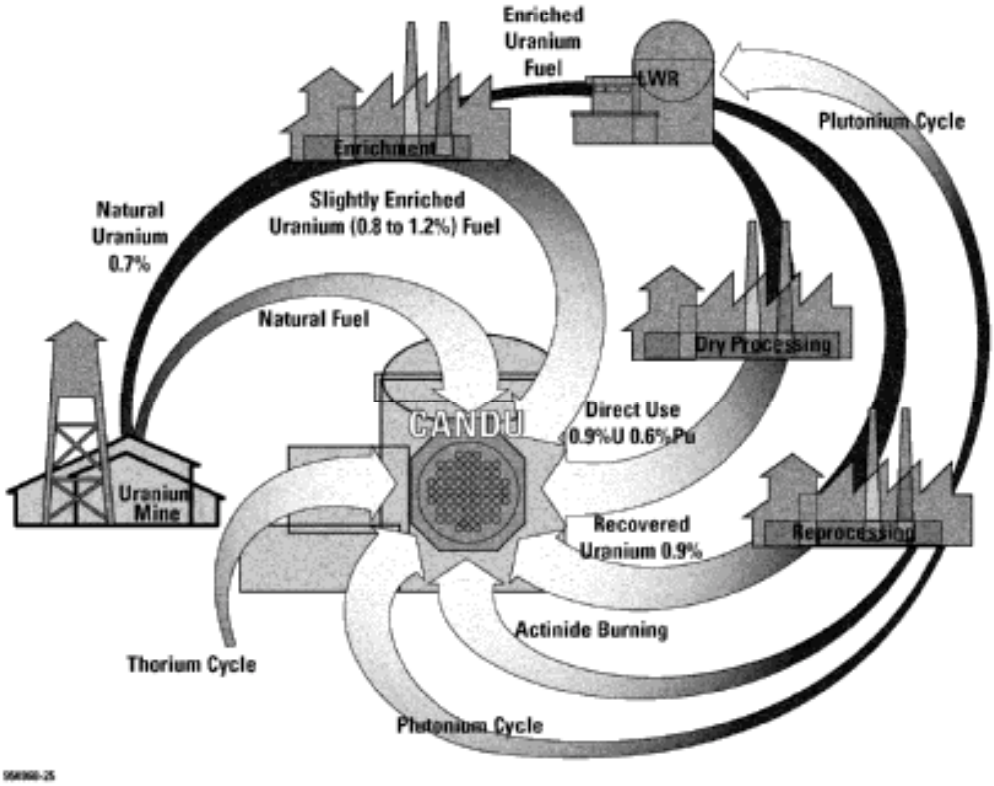


Figure E-1 CANDU 6 Fuel Cycle

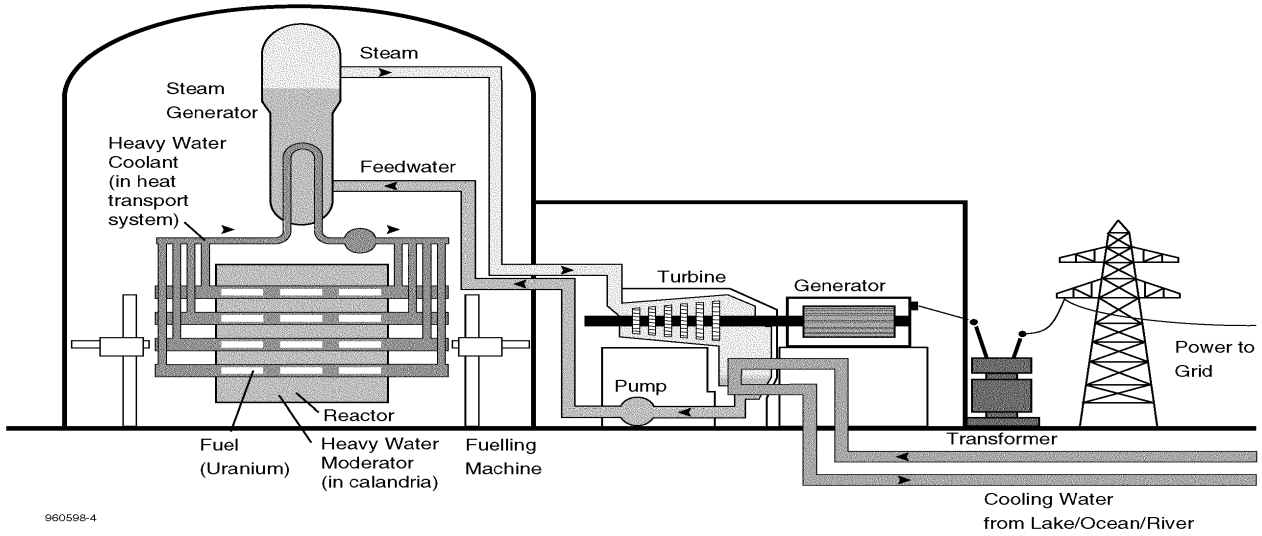


Figure E-2 CANDU 6 Station Flow Diagram

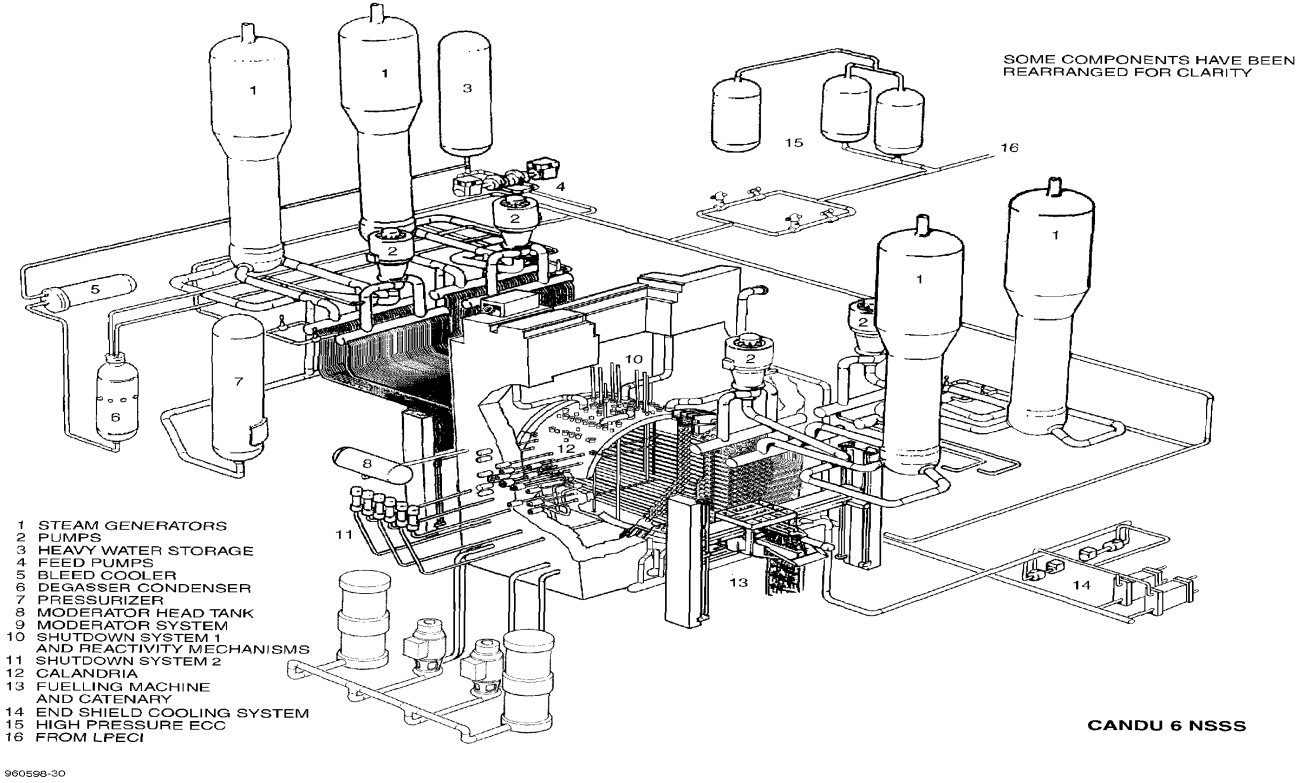


Figure E-3 Nuclear Steam Supply System

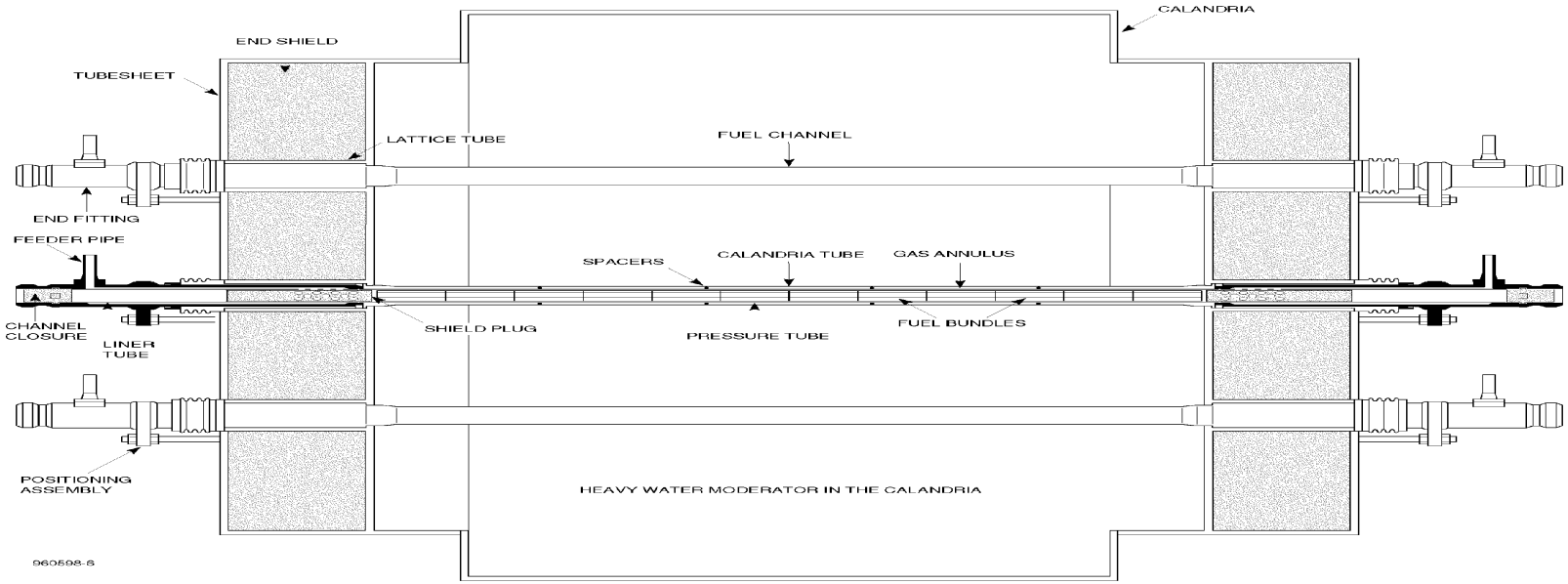


Figure E-4 Calandria Assembly Schematic

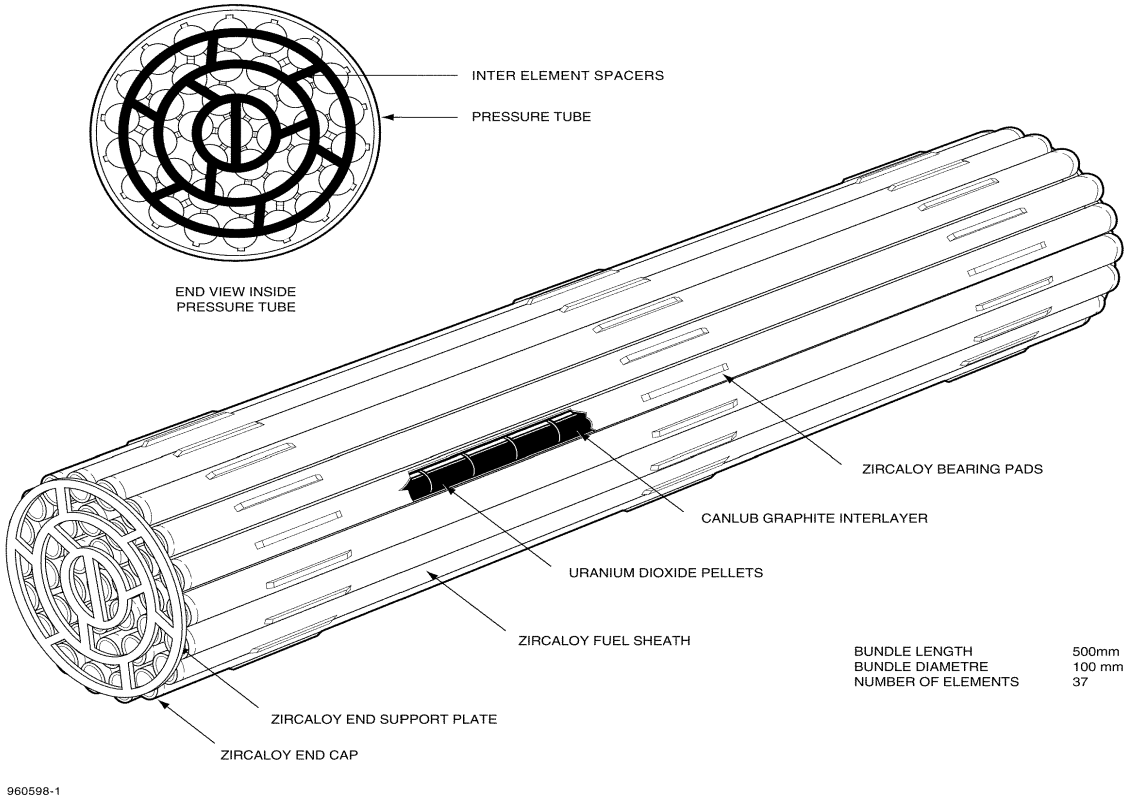


Figure E-5 CANDU 6 Fuel Bundle

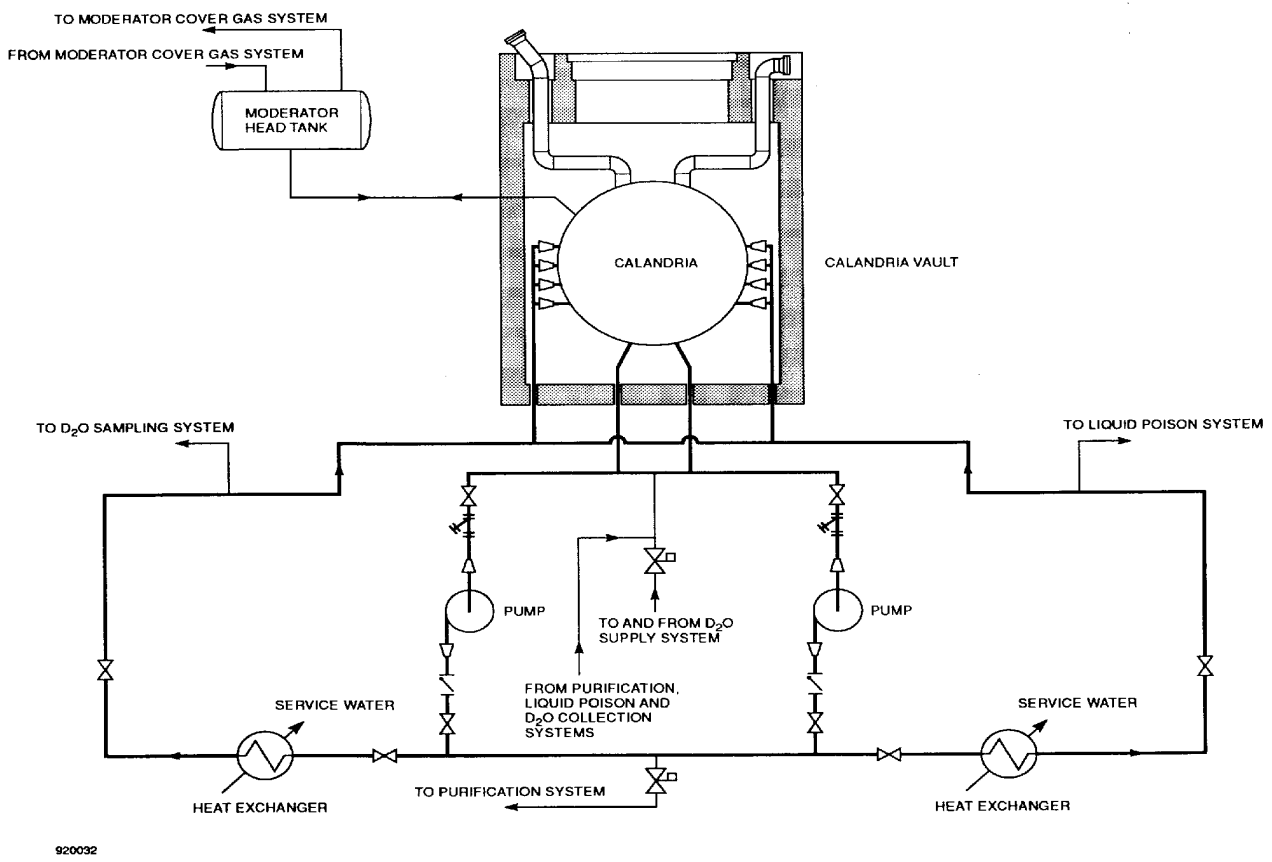


Figure E-6 Moderator System

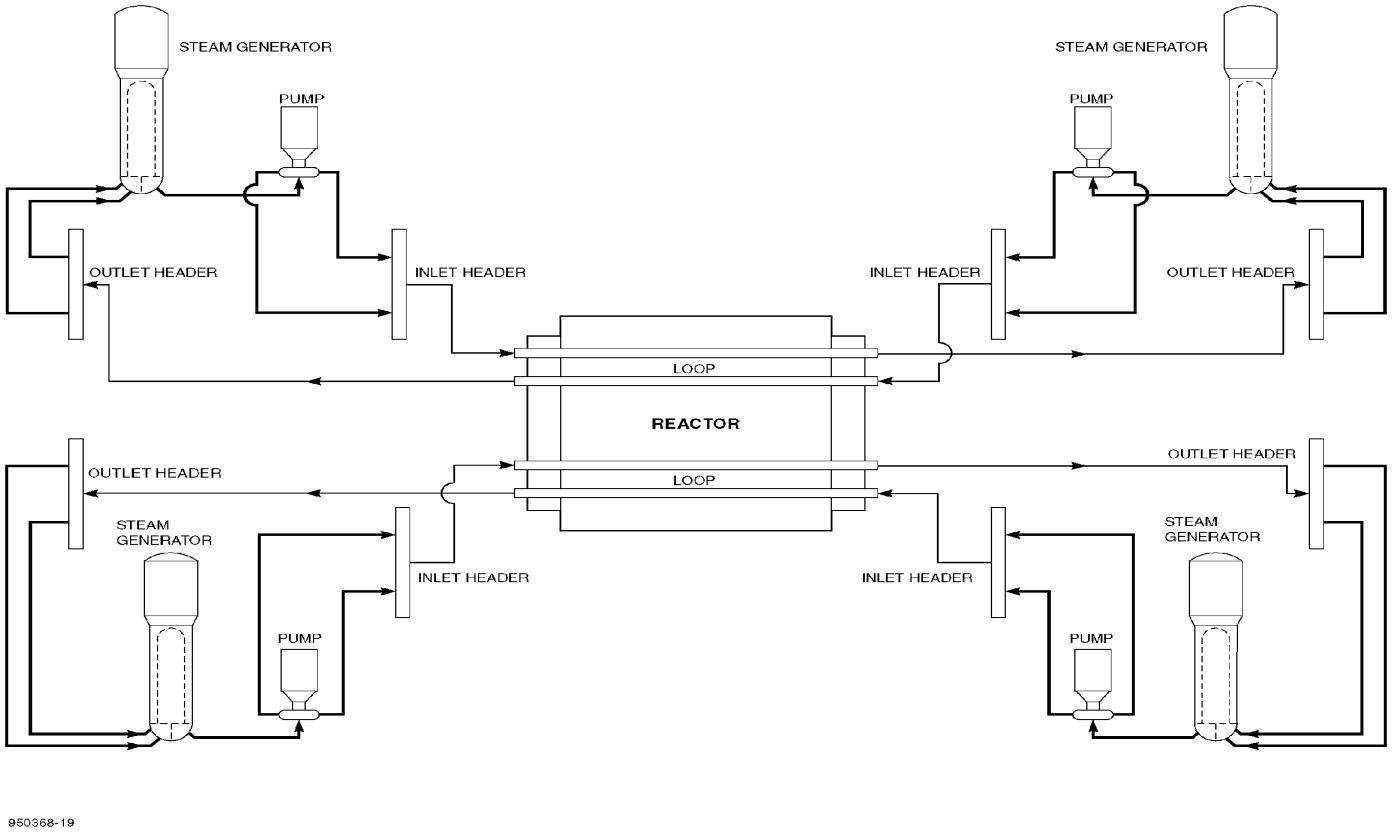


Figure E-7 Heat Transport System

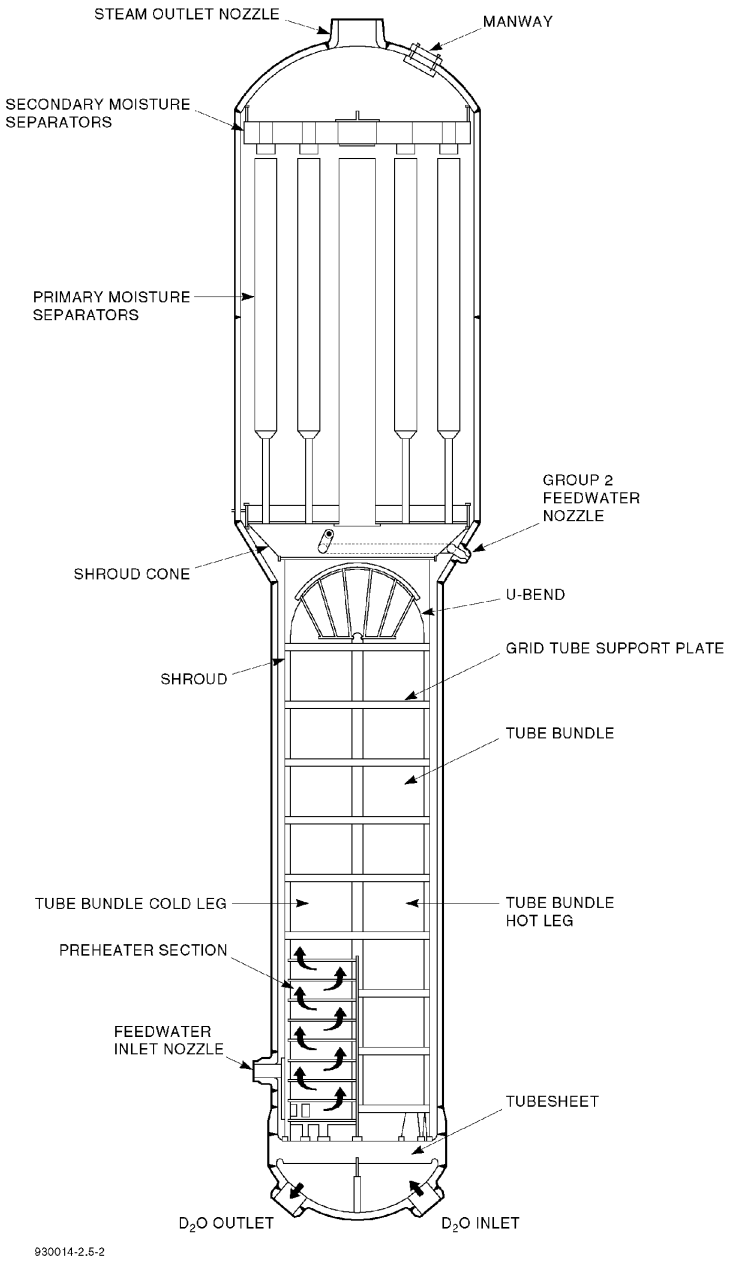


Figure E-8 Steam Generator

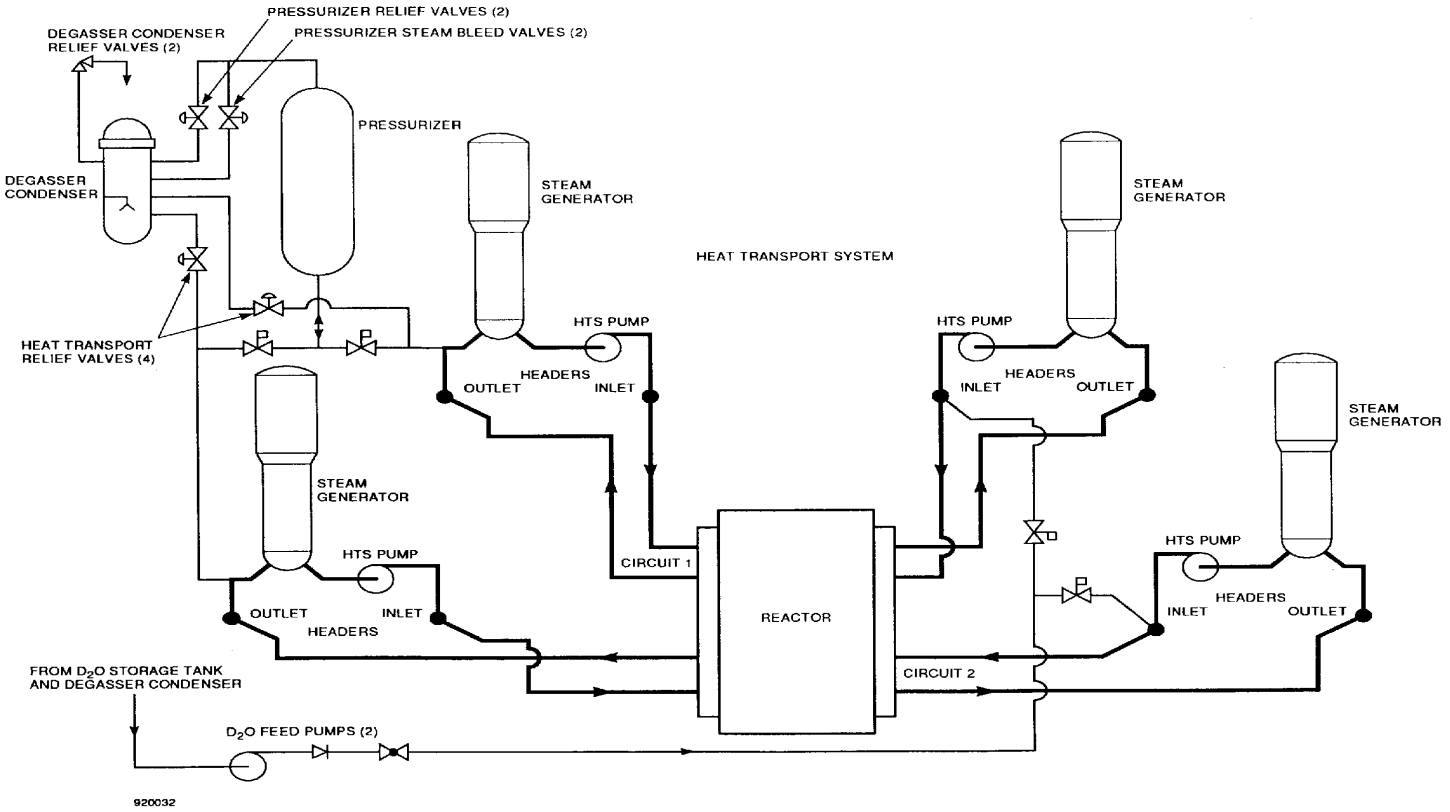


Figure E-9 Pressure and Inventory Control System

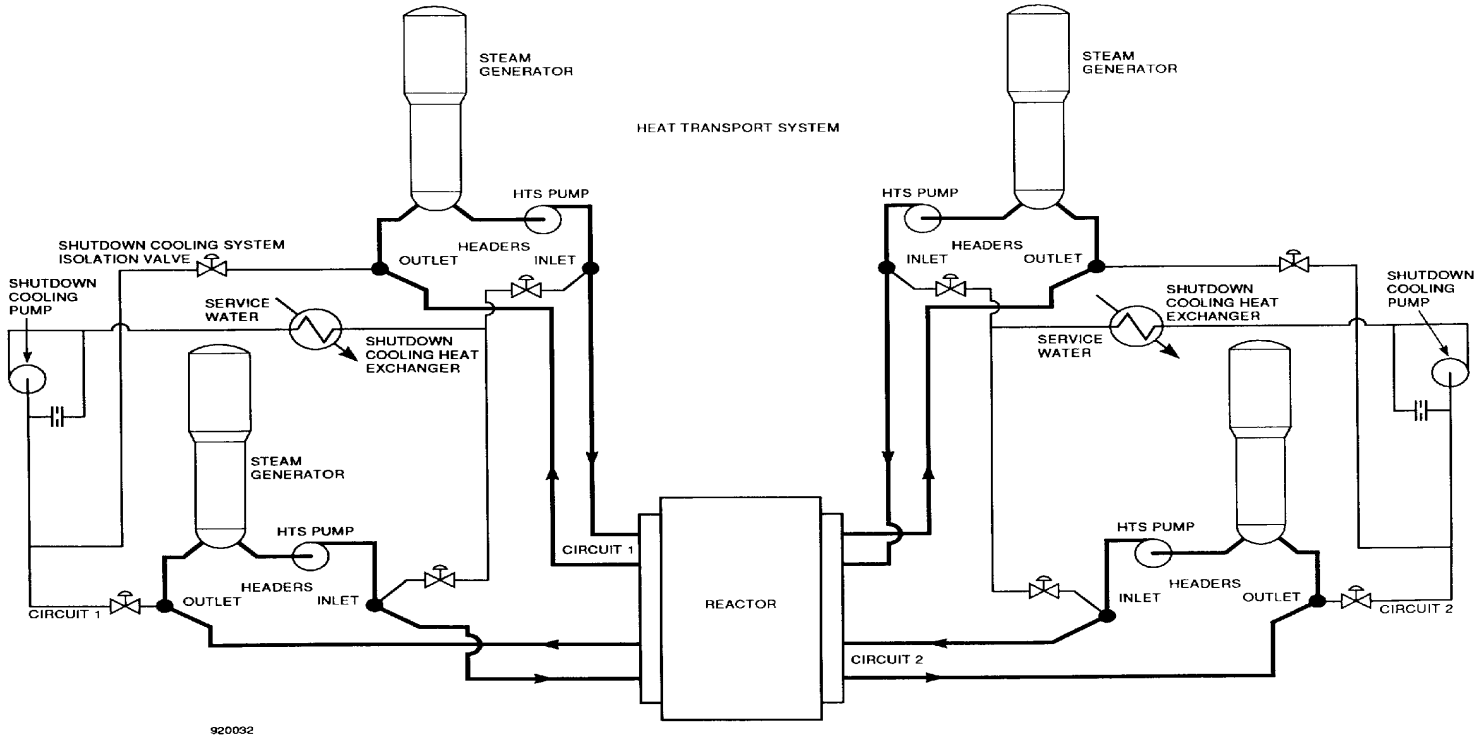


Figure E-10 Shutdown Cooling System

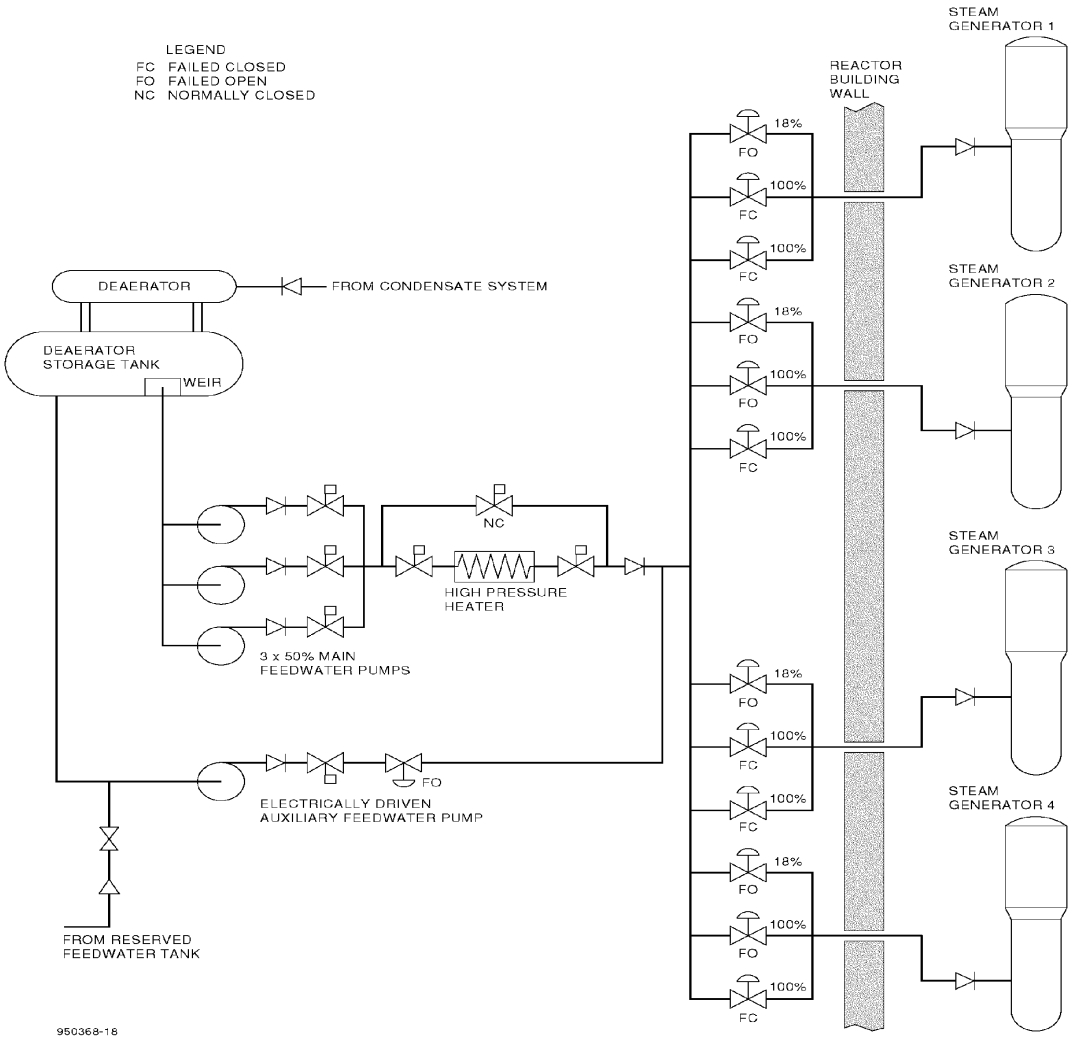


Figure E-11 Feedwater System

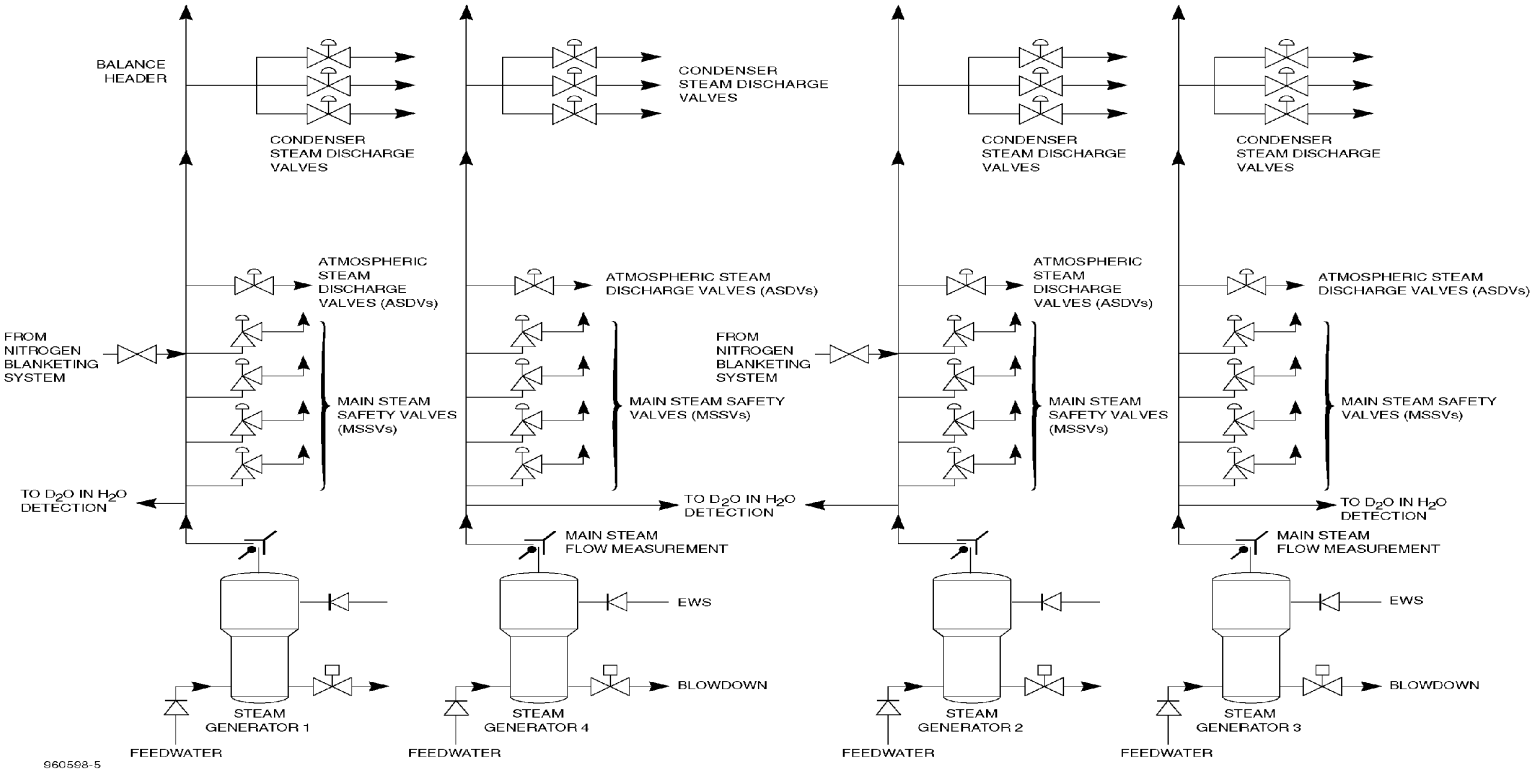


Figure E-12 Steam System

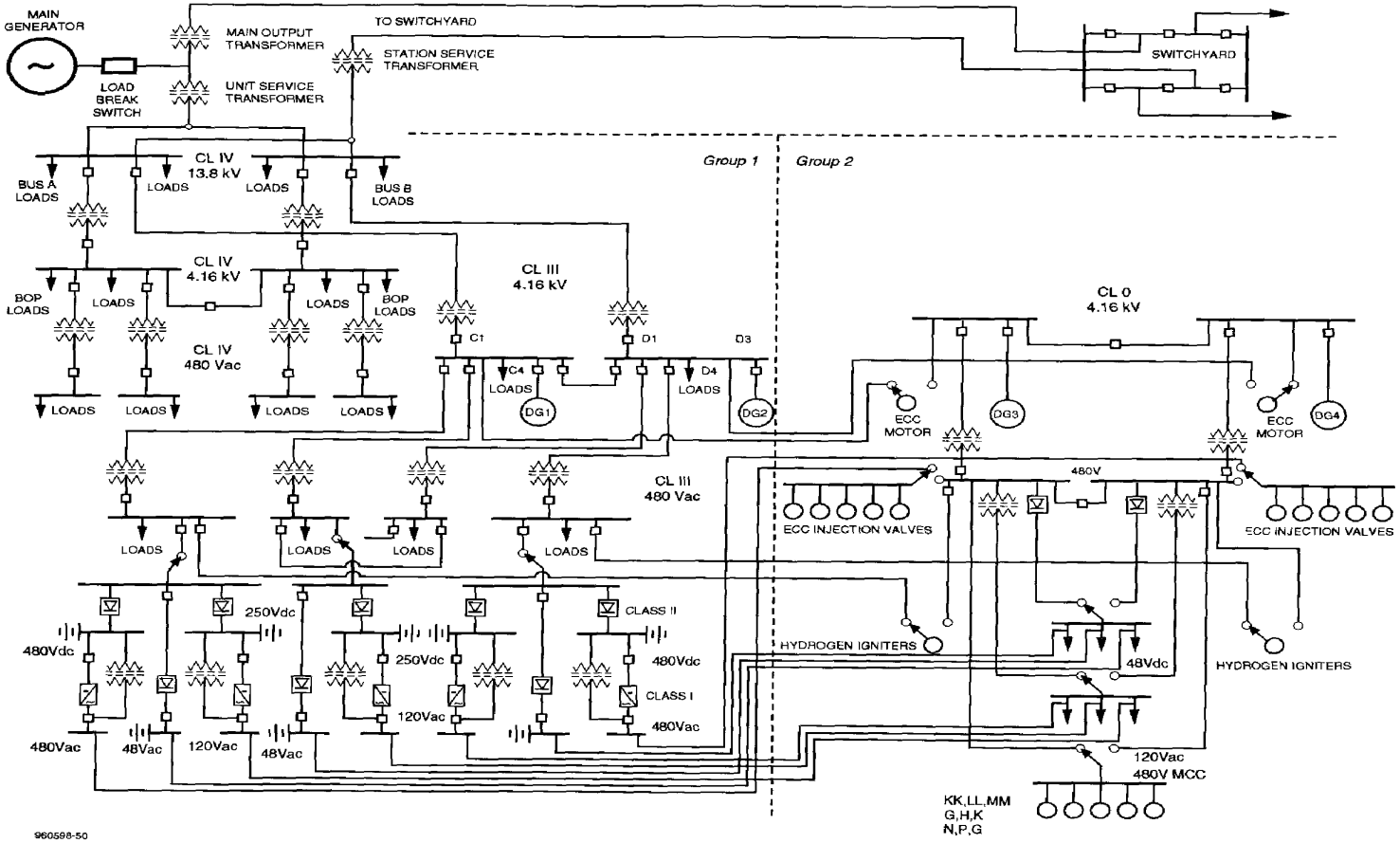


Figure E-13 CANDU 6 Single Line Diagram

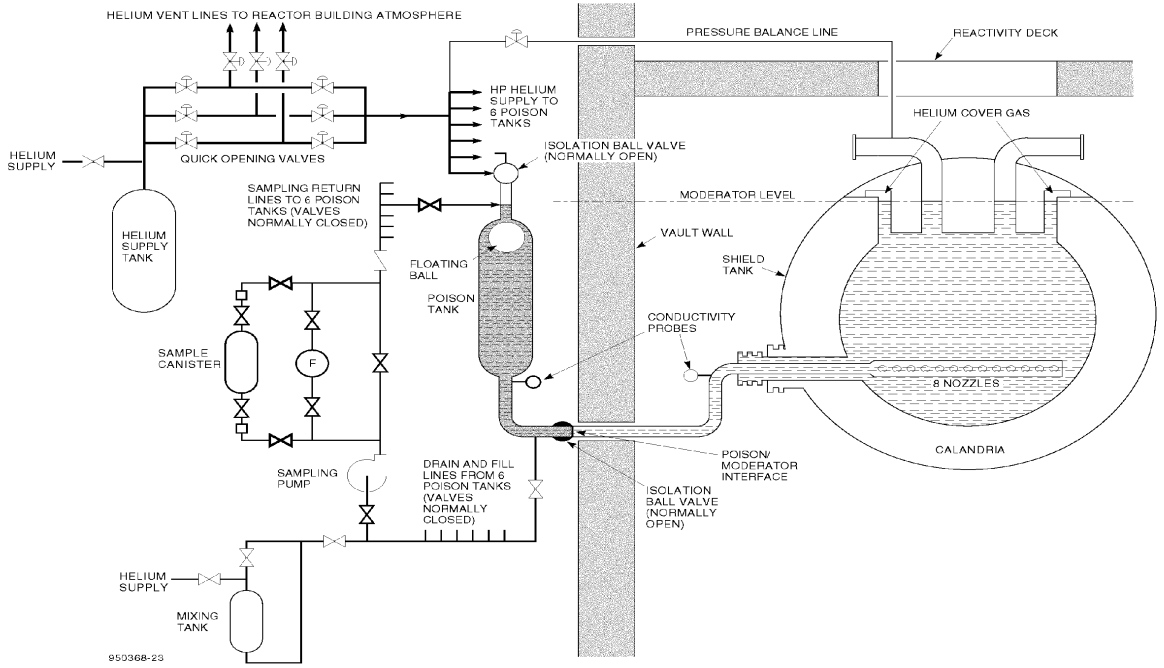


Figure E-14 Shutdown System No. 2 - Liquid Poison Injection System