AECL EACL

Analysis Basis

PROBABILISTIC SAFETY ASSESSMENT METHODOLOGY

ACR

108-03660-AB-001

Revision 1

Prepared by
Rédigé par

Menon Usha

Reviewed by
Vérifié par

Shapiro Hymie

Approved by
Approuvé par

Bonechi Massimo

Jaitly Raj

2003/07/23
Controlled
Licensing

2003/07/23
Contrôlé
Licensing

2251 Speakman Drive
Mississauga, Ontario
Canada L5K 1B2

2251 rue Speakman
Mississauga (Ontario)
Canada L5K 1B2

AECL EACL

Analysis Basis

Probabilistic Safety Assessment Methodology

ACR

108-03660-AB-001

Revision 1

2003 July

CONTROLLED - Licensing

2251 Speakman Drive
Mississauga, Ontario
Canada L5K 1B2

Juillet 2003

CONTRÔLÉ - Permis

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

AECL EACL

Release and Revision History / Liste des documents et des révisions

0939B Rev. 13

Document Details / Détails sur le document

Title / Titre	Total no. of pages / Nbre total de pages
Probabilistic Safety Assessment Methodology	179

CONTROLLED – Licensing / CONTRÔLÉ - Permis

Release and Revision History / Liste des documents et des révisions

Release Document No./N°	Release Document Date	Revision Révision No./N°	Revision Révision Date	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
1	02/02/20	D1	02/02/20	Released for Review and Comment.	P. Iliescu	H. Shapiro	M. Bonechi
2		0	02/03/26	Issued as “Approved for Use”.	P. Iliescu	H. Shapiro	M. Bonechi
3		1D1	03/03/06	Issued for Review and Comment. Revision Summary: Changed the document title “PSA Methodology ACR” and revised the document to refer to “ACR” instead of “NG CANDU”. Section 4.8 modified. Section 4.9 was modified to include revised PDS states for ACR. Section 7 was modified to include methodology for “Seismic Margin Assessment”. In Section 9.6.1 a para on “CAFTA for Windows” was included. In Section 11 References 2, 4, 10, 72 and 81 revised . New References 50, 52 and 86 added.	U. Menon	H. Shapiro P.Santamaura Beomsu Lee Mani Mathew Victor Snell Owen Hines Bin Ly Ed Choy Zoran Bilanovic	
4		1	03/07/23	Issued as “Approved for Use”.	U. Menon	H. Shapiro	R. Jaitly M. Bonechi

SCS/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°
	108	03660	AB	001	1	1	

TABLE OF CONTENTS

SECTION **PAGE**

TABLE OF CONTENTS

SECTION **PAGE**

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

SECTION **PAGE**

APPENDICES

1. INTRODUCTION

1.1 General

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

In addition, if performed during the initial plant design, a PSA can be used to improve the designer's understanding of the safety significance of plant design features and to identify design weaknesses.

Assessment of the adequacy of plant design and operation is achieved by identifying potential accident sequences that dominate risk and establishing which features of the plant 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.

Probabilistic Safety Assessments vary widely in scope depending on the available time and resources as well as the purpose of the study. Depending on the objectives, they 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 NUREG/CR-2300 (Reference 3, 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 inside containment. It includes an analysis of plant design and operation with emphasis on the accident sequences that could lead to core damage, their basic causes, and their frequencies. It does not investigate the probability or mode of containment failure or the consequences of radio-nuclide releases. Both internal events, and external events such as fires and earthquakes, are included.

b) Level II – System and Containment Analysis:

   A Level II PSA consists of 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. It predicts containment failure modes, and the frequency and inventory of radio-nuclide 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 - System, Containment and Consequence Analysis:

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

Figure 1-1, which is based on Figure 2-1 of NUREG /CR-2300 [3], gives an overview of the probabilistic safety assessment process.

Note: Probabilistic Risk Assessment (PRA) and Probabilistic Safety Assessment (PSA) are equivalent terms. In Canada and most European countries the term Probabilistic Safety Assessment (PSA) is used, while in the United States the term Probabilistic Risk Assessment (PRA) is common.

The PRA Standard for Level I and limited Level II internal events (excluding seismic and internal fires) analysis while power operation has been issued by ASME [26]. The PRA standards for external events and fire events and for low power and shutdown operation are now under development by other organizations and expected to be issued in near future. The intention of the standard is to provide standardized technical requirements for the use of the PRA, especially for risk-informed application. The ASME standard divides the PRA capability into three categories, Category I, II, and III. The capability category I is generally understood as corresponding to the PRA for the risk ranking, category II as corresponding to the PRA for risk-informed decision making, and category III as corresponding to the risk-based decision-making.

The ASME standard is in general form endorsed in the USNRC SRP Chapter 19-1 [6] and draft Regulatory Guide DG-1122 [53] with some comments. The Standard and the SRP specifies the application of PRA based on Capability Categories on a case-by-case basis.

The ACR™* design is intended to satisfy current licensing basis of the USNRC. The major objectives of the ACR PSA are:

- to have a reasonable estimation and understanding of the core damage frequency and large release frequency,
- to identify relative importance of accident sequences and the accident sequence progression,
- to rank Structures Systems and Components in terms of significance to the CDF and LRF, and thus provide risk insights on the ACR design for feedback to the design and for use in the operation and maintenance when the plant is constructed and operated.

Considering these, the appropriate capability category for satisfying the purpose of the ACR PSA is judged to be the Category I.

For satisfying these objectives, the PSA will be integrated into the ACR design process and the results will be used as one of the major inputs for the design. Designers will review any design

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

vulnerabilities and significant accident sequences identified from the PSA and will consider modification of the design if practicable against these objectives.

1.2 Definitions of Terms

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 Initiating Event (IE), or a system failure subsequent to an IE.

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" 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, mitigating 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.

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.

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 of two or more components during a short period of time as a result of a single shared cause.

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.

Core Damage State (CDS) – Accidents grouped into categories of similar potential for airborne radioactivity content within the plant and similar containment integrity challenges.

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.

Event Tree Analysis - a method of modelling plant-level sequences that may lead to a plant damage state (PDS) and that represents the response of the plant to the initiating event (IE).

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.

Front-Line System - those systems that directly perform a function to maintain normal reactor operation (e.g., feedwater) or emergency operation (e.g., ECI).

Fuel Channel Failure - the failure of the pressure tube (PT) and the calandria tube (CT).

Human Error Probability (HEP) – a measure of the likelihood that plant personnel will fail to initiate the correct, required, or specified action or response in a given situation, or by commission performs the wrong action. The HEP is the probability of the human failure event.

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 (IE) – any event either internal or external to the plant that perturbs the steady state operation of the plant, if operating, thereby initiating an abnormal event such as a transient or LOCA within the plant. Initiating events trigger sequences of events that challenge plant control and safety systems whose failure could lead to core damage or large early release.

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 Analysis - identification and quantification of the sequences of events leading to the onset of core damage.

Limited Core Damage – improbable events for which the channel core geometry is maintained.For example, a LOCA + LOECC is classed as a limited core damage in a CANDU®* reactor, but it does not lead to a severe core damage, 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.

Loss of Core Structural Integrity - a loss of heat sinks leading to core damage that involves multiple fuel channel failures and core disassembly.

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. The system assists in returning the unit to a safe state.

---

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

Parallel System - a system which contains more than one 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 core damage sequences, which have similar characteristics with respect to the limited core damage progression and containment performance.

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")

Recovery Analysis - the process of identifying, quantifying and applying recovery actions to 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.

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 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 failure of shutdown.

PDS1 involves accidents with late loss of core structural integrity with the PHTS at a high 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 support to a front-line system function (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.

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").

1.3 ACR PSA Program

The PSA will consist of a Level I and Level II PSA for the ACR design, for internal events, internal flood, internal fire and shutdown state. As well, a seismic margin assessment will also be conducted.

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

PSA items listed in the Licensing Basis for Advanced CANDU Reactor document (Reference 4) will be undertaken.

Throughout this document, the acronym of ACR PSA is used to describe the PSA Program dedicated to ensure the licensability of the ACR.

NUREG/CR-2300, *PRA Procedures Guide*, Volume 1, Section 2.2 [3], and NUREG/CR-4550, Volume 1, Revision 1 (Reference 5) have been used as guides in developing the PSA methodology for the ACR program

The PSA will analyse the ACR initiating events by conducting a systematic review of plant design for initiating events.

1.4 Purpose

1.4.1 Probabilistic Safety Assessment (PSA)

The purpose of the ACR PSA is to establish the spectrum of accident sequences which could lead to the specified design basis accidents, limited core damage or severe core damage accidents, determine their basic causes and calculate their frequencies. The PSA will also be used to provide safety design assistance through engineering feedback to the process designers, at an early stage so that changes can be made before construction.

In the Level II portion of the PSA, the objective is to perform containment analysis to establish the various failure modes of containment and the frequency and magnitude of radionuclides releases from containment.

1.4.2 PSA Methodology Document

The purpose of this document is to describe the methodology to be used in the performance of the ACR Probabilistic Safety Assessment (PSA).

1.5 Scope

1.5.1 PSA

The PSA will consist of a Level I and Level II PSA for the ACR design, for internal events. In addition to internal events, assessment of the internal flood, internal fire and seismic events will also be included in the PSA. The PSA will not include a Level III PSA.

As well, a shutdown state PSA will also be included in the ACR PSA. This addresses additional concerns to those that are addressed in the full power PSA and includes simultaneous system unavailability during different phases of an outage, the importance of operator actions to restore functions, and maintenance restrictions to various mitigating and safety systems while the plant is in a specified shutdown state. A shutdown state PSA can provide insight to outage planning, outage management practices (e.g., Maintenance restrictions), and design modifications to lower the risk of severe core damage

The PSA work is started early in the project in parallel with the design as it evolves. One of the primary objectives of the design PSA is to provide design assistance based on past PSA studies, engineering judgement and/or on simple fault tree analysis. This is seen as a valuable input to the early design process when most design changes can be implemented at a minimal cost.

For the ACR PSA high level fault trees will be developed.

Specifically, the scope of the PSA includes the following tasks:

a) Identification of all credible accident scenarios (that may challenge plant's safety functions and lead to the need for reactor shutdown and decay heat removal) as basic input for ACR design requirements and to ensure that safety goals for the plant will be met according to the provisions in Section 3.4 of the Licensing Basis Document, 108-00580-LBD-001, Rev. 0.

b) Identification of dominant accident sequences that may result in the design basis, limited core damage and severe core damage accidents and assign them frequencies based on CANDU units operational experience.

c) Demonstrate that the predicted sum of frequencies, for accident sequences which result in severe core damage-, is less than 1.0 x E-05 events /year (except for seismic) which is the safety goal based on design targets specified in the Licensing Basis Document (see Section 3.4, Reference 4).

d) Identify feasible design changes required to minimize the operator actions that may be needed to mitigate the accidents' consequences.

e) Prepare support information for subsequent use as PSA input to the preparation of the emergency operating procedures (EOPs).

f) Provide input to the environmental qualification program and control centre design.

g) Input to the test and maintenance programs such that they can be optimized in terms of cost and safety.

In summary, the PSA will include the following:

a) Level I and Level II PSA analysis for
   - internal events for full power,
   - internal events for shutdown state,
   - internal fires and internal floods for full power;
   - PSA based seismic margin assessment;

b) Identification of a comprehensive list of initiating events;

c) Confirmation of the system reliability targets via high level fault tree analysis of the ACR front-line and support systems;

d) Human reliability analysis;

e) Calculation of the severe core damage frequency for the ACR design.

External events like high winds and tornadoes are not expected to be safety significant contributors because the plant is designed for these hazards. Site-specific external events will be evaluated as per the recommended progressive screening approach specified in NUREG-1407 (Reference 32).

1.5.2 Summary of PSA Methodology Tasks

The methodology of the PSA process for the ACR is outlined in Figures 1-1 and 1-2. Figure 1-1 is for an integrated PSA, i.e., it covers Levels I, II and III of the PSA, whereas Figure 1-2 is for a Level I PSA only. Figure 1-2 is taken from NUREG /CR-4550 [5] and shows the Level I ACR PSA methodology.

The following is a list of the major tasks associated with the ACR PSA. These tasks are briefly described in the following sections of the document.

a)	Familiarization with ACR Design	Section 3
b)	Internal Events PSA	Section 4
c)	Event Tree Development	Section 4.3
d)	System Reliability Analysis	Section 4.4
e)	Database Development	Section 4.7
f)	Accident Sequence Quantification	Section 4.8
g)	Plant Damage State Analysis	Section 4.9
h)	Dependent Failure Analysis	Section 5
i)	Human Reliability Analysis	Section 6
j)	External Events Analyses (Seismic)	Section 7
k)	Fire PSA	Section 8
l)	Flood PSA	Section 9
m)	Uncertainty and Sensitivity Analysis	Section 10
n)	Level II PSA	Section 11
o)	Quality Assurance	Section 12
p)	Reporting of Results	Section 13

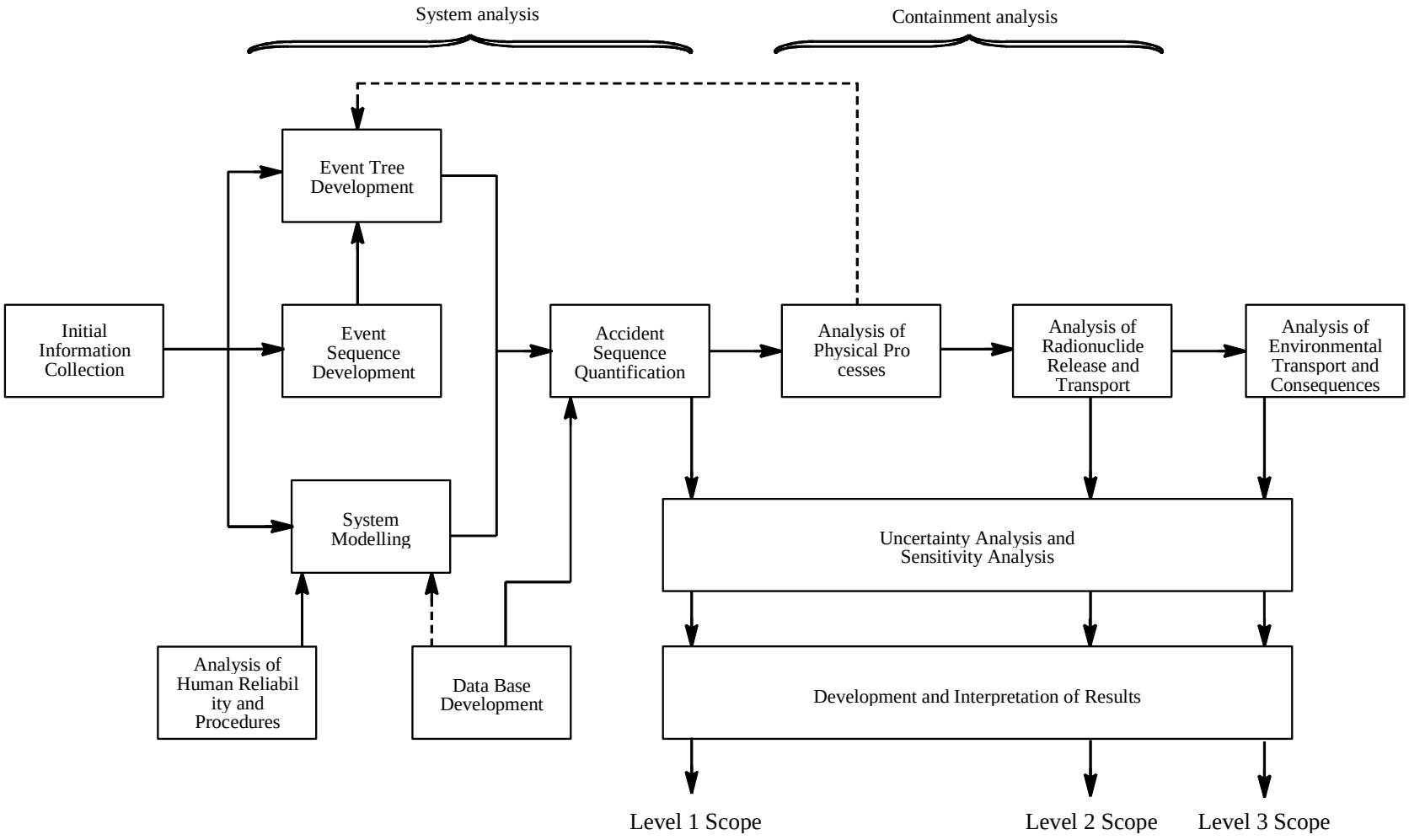


Figure 1-1 Overview of Probabilistic Safety Assessment Process

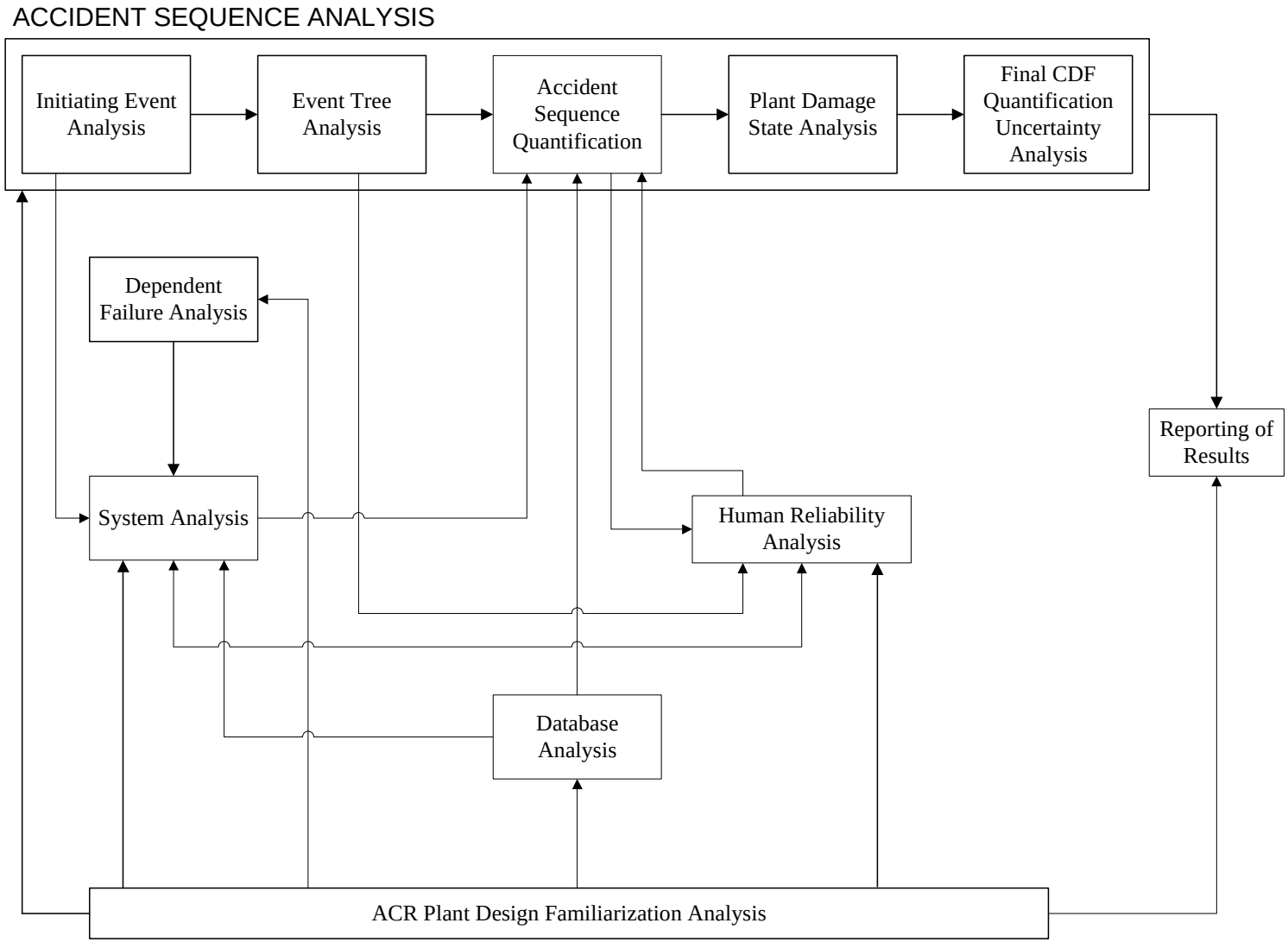


Figure 1-2 Task Flow Diagram for a Level I PSA

2. PSA OBJECTIVES

2.1 PSA Objectives for ACR

The PSA objectives for ACR are:

a) Summed mean frequency for the accident sequences (initiated by internal or external events when reactor is either shutdown and at full power) leading to severe core damage (plant damage states PDS0, PDS1, PDS2), should have a value of less than 1.0 x E-05 events per year (except for seismic) per Licensing Basis Document (Reference 4)[1].

b) Summed mean frequency for the accident sequences leading to large release of radioactivity, should have a value of less than 1.0 x E-06 events per year (except for seismic), as per Licensing Basis Document provisions (Reference 4).

c) The target frequency for the individual severe core damage sequences for internal events at power is going to be less than 1.0 x E-07 events/year.

d) To comply with the Canadian Nuclear Safety Commission's (CNSC's) Consultative document C-006 Rev. 1 (Reference 1).

e) Confirm safety system unavailability targets of CNSC's Regulatory Documents R7, R8 and R9 (References 7, 8 and 9 respectively).

[1] See Reference 4, Section 3.4 on Safety and Environmental Goals.

3. FAMILIARIZATION WITH ACR DESIGN

Probabilistic Safety Assessments are broad, integrated studies requiring a considerable amount of information related to the plant design, analysis and operation. The first major task in the ACR PSA program is familiarization with the ACR plant design. Before technical analysis begins, the PSA team must become familiar with all aspects of the plant design.

This task is the foundation for all subsequent tasks and includes the collection of information from previous studies, from the ACR Technical Description (Reference 10), and from other documents. The quality of information collected in this task and the manner in which it is managed is critical to the success of the entire PSA analysis effort.

3.1 Information Management System

It is important that the PSA team leader establish a system for acquiring and distributing, to all PSA team members, all pertinent information collected during the study, beginning with the initial collection phase. The purpose is to ensure that all the analysts (PSA team members) consistently use the same information and the latest version of the information. A considerable amount of information is acquired from almost every department and discipline responsible for the design of the NSSS within AECL, and the Architect/Engineer (A/E), responsible for the balance of plant (BOP) design. This information must be organized and communicated to the PSA analysts in a fast, reliable and consistent manner.

3.2 Initial Information Collection

For the PSA Level I analysis, sufficient information must be assembled to allow performance of the following tasks:

a) Preliminary identification of the initiating events applicable to the ACR plant design (e.g., loss of coolant accidents, transients) to be included in the analysis.

b) Identification of the functions to be performed for each initiating event to successfully prevent severe core damage/design basis accidents or mitigate their consequences.

c) Identification of the plant systems, which perform these mitigating functions. These systems are referred to as “mitigating systems” or “front-line systems”.

d) Determination of success criteria and establishment of reliability targets for each mitigating system.

e) Development of an initial set of event trees based on an understanding of the plant response to the initiating events.

f) Identification of dependence between the front line systems and support services provided by the electrical power, air, and service water systems.

The following documents provide the necessary background for starting the PSA work.

a) CNSC Consultative Document C-006, Rev. 1 (Reference 1);

b) Licensing Basis for ACR, Rev. 0 (Reference 4);

c) ACR Technical Description 10810-01371-TED-001, containing preliminary flow sheet and design information (Reference 10);

d) ACR Safety Design Guides (SDGs) 108-03650-SDG-001 through to SDG-006 (References 71 to 76) and Safety Analysis Basis (SAB) documents (Trip Coverage methodology - 10810-03550-AB-001) (Reference 37).

e) CANDU 6 system design manuals, system flowsheets and safety reports;

f) CANDU 6 PSA studies;

g) CANDU 9 system design descriptions and system flowsheets;

h) CANDU 9 PSA studies.

i) Generic CANDU PSA (References 45 and 46).

3.3 Limitations on Design Changes

In addition to the collection of the above information, regular contact must be maintained between the PSA analysts, especially the team leader, and the system designers to ensure that the latest design changes are incorporated in the on-going PSA analysis. Design changes, if authorized, are communicated via the configuration change control process as described in Procedure 00-681.1 (Reference 67).

Before the final or detailed design PSA begins, a configuration freeze date will be set, i.e., the date after which design changes will not be included in the PSA analysis. This minimizes the potential for the analysis to be outdated before the configuration freeze date, and ensures that the analysts are not dealing with a moving target in terms of plant configuration.

4. INTERNAL EVENTS PSA

4.1 Introduction

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 3.

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 sub-criticality 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 (this includes internal floods and internal fires) 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 external fires, earthquakes and external floods, 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 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 1, C-006, Rev. 1 and from similar systematic design review studies of previous CANDU plants. The main process, shown in Figure 4-1, is the systematic review of the plant design for initiating events. Methodology for this systematic review of the plant design for identification of initiating events is documented in Reference 2.

4.2.3 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.

4.2.4 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.

4.2.5 Initiating Event Frequency Quantification

Various methods, such as 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. 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.

4.2.5.1 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.

4.2.5.2 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 4.2.5.4 supports the use of the chi-square approximation to derive the frequencies for rare events.

4.2.5.3 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 would require special quantification techniques, such as the chi-square approximation (see Section 4.2.5.4).

4.2.5.4 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.

4.2.5.5 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 based on previous CANDU experience and using chi-square distribution. See Section 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 external events is different and is discussed in Section 7.

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.

The second set of event trees are for Level II containment sequences. Dependencies between the Level I and Level II ETs will be assessed (See Section 11).

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 computer code CAFTA Event Tree Editor [41] is used to produce the event trees by AECL. 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 will be obtained from existing design and analysis reports. Where the analysis does not exist, plant response will be assumed based on engineering judgement and past experience. 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).

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 the 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. Recovery actions may be applied where applicable. 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 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.

Front-line or support systems that are credited to mitigate any initiating event that results in harsh environmental conditions must be environmentally qualified or immune from the harsh environment 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, Section A.2 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 mission 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. The PDSs will be explicitly categorized for these sequences based on the criteria in Section 4.9. Other, lesser damage states should be labelled according to the criteria in Section 4.9.2 (e.g., PDS3, PDS4, 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. This is based on previous CANDU experience. These sequences will be verified during ASQ to ensure that they are less than 1E-9/yr, if not they will be developed further.

A probability truncation limit of 10^{-10} per year is used in accident sequence quantification. Since the expected summed SCDF is of 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 containment 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 containment 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 mission 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 11.

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., PDS0, PDS1, 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 for the accident sequences includes the abbreviation of the initiating event and a sequence number so that each sequence is uniquely identified.

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 5, 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. Initially, fault trees are constructed for front-line systems, credited in the event trees. Fault tree analysis may also be used to derive the frequencies of some initiating events.

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).

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 NUREG-0492, Fault Tree Handbook [56]. Logic is developed using the principle of immediate cause. The top event failures are clearly defined, as are the system boundaries.

For ACR PSA, high level fault trees would be developed.

4.4.3 Computer Codes Used in System Analysis

For the ACR PSA program, a computer code CAFTA Fault Tree Editor is used for Fault Tree analysis [41] throughout to construct, evaluate and quantify the fault trees. CAFTA also maintains the primary event database and is used to draw the fault trees. CSRAM in CAFTA (cutset editor) is used to calculate the initiating event frequencies. Codes with equivalent capabilities may be substituted. From this point on, fault tree analysis related information is described based only on use of CAFTA.

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) technical specifications (TS),

c) Preliminary Safety Analysis Report (PSAR),

d) system flow sheets (FS),

e) instrument loop diagrams (ILDs),

f) elementary wiring diagrams.

For PSA, the design information is based on the description as given in the ACR Technical Description (Reference 10).

4.4.5 Fault Tree Event Nomenclature

An essential part of fault tree modelling and analysis is a fault tree event naming or *Fault Tree Event Labelling Scheme*. The labelling scheme 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. 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 25 characters grouped in five segments or fields. 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:

Unit Number Field: One character field for the Unit followed by a dash.

ASI Field: A five-character field, which identifies the system to which the component belongs, and which is based on the AECL Subject Index (ASI) for ACR.

CN Field: A twelve-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 or 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.

4.4.6 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.

4.4.6.1 Assigned Probability

The calculation type identifiers that can be used in the **C** field are designated by 0, 1, 2, 3, 4, 5, 6 and 9. When a probability is assigned, rather than calculated by the CAFTA program, the value **C** = 0 is entered by the analyst in the calculation type field of the BE database.

4.4.6.2 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.

4.4.6.3 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 < 4 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 + 12 hours, unless otherwise specified. The characteristic time τ = T/2 + MTTR + 12 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 $\tau = 2(T/2 + T_r) = T + 2T_r$.

4.4.6.4 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 > 4 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, 5 or 6 may be used –(CAFTA User's Manual [41]).

4.4.7 Modelling of Specific Events

4.4.7.1 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 assumed to be half the time taken between outages, since this represents the average time for which the component is unavailable. This duration is typically assumed to be 1 year.

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 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.

4.5 Labelling of Fault Tree Events

Dependent Failure Analysis

In risk analysis, the treatment of dependencies in the identification and assessment of interrelationship within systems or between systems 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 are affected as well. 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 improve the availability of some plant functions. Section 5 describes in detail the dependent failure analysis used in the ACR PSA.

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 are identified during the PSA process and are analysed. Section 6 describes the HRA used in the ACR PSA.

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). 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 component 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 PSA work is compiled primarily from operating CANDU plants (e.g: Pickering, Bruce and CANDU plants).

Component reliability data, which are based on operating experience from Ontario Power Generation's generating stations, are found in OPG's Darlington NGS A Risk Assessment (DARA) study. OPG was formerly 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 is from CANDU operating stations. These data were based, as much as possible, on operating experience at Pickering NGS A and Bruce NGS A. This experience was accessed through system and equipment reliability analysis (SERA) reports and station quarterly technical reports. Where required data were not available, data from other sources such as OPG fossil-fuel station operating experience, and external sources were used. Data based on fossil-fuel station experience were accessed through thermal outage and maintenance activity system (THOMAS) reports.

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 [60], and

b) Nuclear Plant Reliability Data System (NPRDS) 1983 Annual Report of Cumulative System and Component Reliability [61].

The IEEE Standard [60] 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 [61] 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.

Data from published external sources, such as NPRDS, SERA and IEEE Standard 500 - 1984, were used only when OPG data were not available.

It is noted that the collecting of data 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 α percentile of the chi square distribution, with (2n + 2) degrees of freedom.

b) Mean Time to Repair

The MTTR is calculated as follows:

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

where t_i = the observed repair time, in hours, of the ith 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 ACR 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 ACR component reliability database are 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 12-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, not extend beyond the component level for which sufficient data are available. For ACR PSA this will be based on the available design information.

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.

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 error factor associated with each failure event.

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 and success/failure of various mitigating systems. The fault tree linking approach is used to solve the accident sequence frequencies whereby the event tree and fault tree mitigating systems are merged together.

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 a 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 of ASQ is to merge and then evaluate the mitigating fault trees for all the decision branch points of a particular initiating event that lead to the accident sequence under study (fault tree linking approach as described above). 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, system fault

trees (front line, supporting and broken loop logic) and associated logic flags. Also, success criteria of the individual sequence must be evaluated and deleted from the sequence of interest. Furthermore, any mutually exclusive events and recovery actions must be accounted for in ASQ.

ASQ is performed on the individual sequences of the event trees which lead to an undesired state or PDS. 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. Frequencies of the cutsets resulting in SCD may be summed to obtain the overall or SCDF of the plant.

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 (accident sequence logic) and system fault trees.

ASQ will be performed using the CAFTA and PRAQUANT [41], [42] computer codes, developed by DS&S. Figure 4-3 shows the sequence of analysis and the DS&S computer codes used to perform the ASQ. The event tree is first constructed using the event tree computer code CAFTA Event Tree Editor. The PDS sequences of interest are identified in the event tree. The system fault tree logic is then developed using the CAFTA fault tree editor. Next, each PDS accident sequence in the event tree is converted into accident sequence logic of a fault tree format using the CAFTA Event Tree Editor or directly into PRAQUANT.

For each sequence, two top gates are created: 1) AND logic of the ‘failure’ part of the sequence and 2) OR logic of the ‘success’ part of the sequence. For each event tree, associated flags are determined such as trip parameters and availability of support systems e.g. Class IV electrical power, service water.

Once all the supporting system fault trees are prepared, they are merged into one larger fault tree using the fault tree editor. The circular logic between support systems is broken in this file. Then, the front line system fault trees are merged together with the supporting (broken circular logic) fault trees into one large master fault tree. This master merged fault tree is now ready as an input for each accident sequence for PRAQUANT.

Several support files are also required to evaluate the accident sequences. The sequence quantification file acts as the control file which lists all the information about the sequences, e.g. sequence names, flag files, success logic files, truncation limits etc. The flag file contains true/false information about flags and the accident sequence logic from the event tree.

Since the cutsets for some sequences may contain success logic, it may be necessary to condition these cutsets, by deleting the success logic. This is performed automatically by PRAQUANT via the sequence quantification file. 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. One master mutually exclusive file is developed from each individual fault tree system.

The last step before ASQ can be performed is to develop a recovery file. The recovery file contains operator actions and other credits which can be assigned to particular cutsets if certain conditions exist (i.e. basic events). This is an iterative step, as the cutsets have to be reviewed first to determine what can be credited.

Once the merged fault trees and supporting files are prepared, ASQ can be performed. The cutsets for each accident sequence are generated using the most efficient cutset generator available from 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 Prepare Accident Sequence Logic Files

Accident sequences to be evaluated are converted from the event tree into fault tree logic, as described in Section 4.8.2. The failure branches and initiating events are logically "ANDed", and the success branches are "Ored". In order to "AND" the failure branches, any logic loops between supporting systems must first be resolved see Section 4.8.2.3. This is not a necessary step as the event tree logic can be imported to PRAQUANT directly.

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, "ANDed" together. The trip parameters and other flags for the particular event tree must be established and included in the flag file.

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 success branch mitigating systems are included in the sequence quantification file for evaluation. 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.

4.8.2.2 Generate, Review and Merge Front-Line Systems

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, the system analyst and the PSA team leader review them. 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.

When all the fault trees are completed and the circular logic is broken see Section 4.8.2.3, 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.

4.8.2.3 Remove Circular Logic Loops

The circular logic loops may become apparent after merging the support systems. An example of such a loop would be the Class III AC electrical power on loss of off site power in CANDU 6, which results in the need to start and run the Class III diesel generator (DG) support systems. If the recirculated cooling water system is not available (to supply cooling to the DGs) due to the loss of Class III AC, then the DGs are functionally unavailable, and cannot in turn supply Class III AC electrical power. Any such loops that are found should be broken at some point, because the code will not be able to solve fault trees with these loops. This action should be done carefully to ensure that no cutsets are lost in the process.

Once the circular logic loops are removed the support systems can be merged with the front line systems.

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. Also, the trip parameters have to be identified.

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 all the 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 and adds many more cutsets to the solution. 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.

All the mutually exclusive events from the fault tree analyses are combined into one mutually exclusive file. This file must be reviewed carefully for consistency.

4.8.2.6 Modularization

The functional modularization technique serves to reduce the time that is required to evaluate large fault tree models. 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. In ACR PSA, modularization may be used.

Furthermore, modularization leads to a conservative solution as individual basic events which would have been deleted by the truncation limit remain in the module.

4.8.2.7 Frequency Truncation

It is expected that the frequency of individual sequences that cause SCD, will be 10^{-7} 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

Recovery analysis is conducted as part of ASQ during the last step of PRAQUANT. Recovery factors are incorporated into the cutsets to achieve a more realistic result. This step produces 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, a recovery set of ‘rules’ have to be developed. Pre-selected basic events determined by rule-based functions are added to certain cutset combinations in a sequence. Each generated cutset is checked to see whether or not some conditional cutset is included (the ‘rule’). If the generated cutset contains the conditional cutset, then the recovery action is added to those cutsets. For example, if the both diesel generators fail during mission, a credit for restoration of

off-site power can be taken whereas if both diesel fail to start no credit can be taken. This process may be iterative until all the recovery events are established for the sequences of all the event trees in the PSA study. The recovery rules and basic events to credit are maintained in the recovery file.

PRAQUANT automatically adds recovery actions to cutsets, which are determined by rules established in the recovery file.

4.9 Plant Damage State Analysis

The event tree analysis yields a large number of events accident sequences that can result in significant fission product releases to the containment. The events may be from internal or external events. The objective of grouping (binning) these numerous event sequences is to collapse the spectrum of 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 11). 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 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 ECC on the timing of the fission product release from the primary HTS and the implications of the initiating event on the HTS 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) Failure to shutdown - 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 Large LOCA plus loss of ECI).

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

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

g) Power cooling mismatch with late ECC injection due to multiple channel failure - PDS6.

h) Power cooling mismatch in a single channel with containment over-pressure - PDS7.

i) Power cooling mismatch in a single channel with no containment over-pressure - PDS8.

j) Tritium Release - PDS9.

k) Fuelling machine failures. The analysis of this PDS will be done in the PSA when details of fuelling machine design and operation are known - 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 for internal and external events 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 –Failure to shutdown.
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 Failure to Shutdown - PDS0

This event comprises end states resulting after a failure of shutdown functions. This 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. 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.

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.

Should the cooling water supply to the moderator and shield tank water also fail, eventual fuel melting will occur, when the moderator and shield tank water boil off. This core melt scenario is called the late loss of core structural integrity/late core disassembly caused by a complete loss of heat sinks, with the HTS at high pressure, and a failure of ECC to remove decay heat.

A description of a core melt progression for this plant damage state (PDS1) is given in Reference 11. The event sequence that leads to late core disassembly is a loss of Division 1 & 2 service water that results in a loss of cooling to the moderator, shield tank, LTC, ECC heat exchanger, etc., combined with a consequential loss of Class IV power, and a loss of other sources of feedwater (e.g., main and auxiliary feedwater and Reserve Water Tank Makeup) to the steam generators.

This event can lead to fuel channel failures, followed by calandria vessel failure, with the release of molten core material into the shield tank.

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

This category involves accidents with loss of heat sinks when the HTS is at low pressure. A typical event is a LOCA +LOECC + loss of moderator as a heat sink.

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

Any LOCA beyond the capability of the H_2O feed system requires the initiation of the ECI. Failure of ECC results in a loss of fuel cooling 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, pressure tubes may strain and contact their associated calandria tubes, in which case the moderator provides a heat sink.

PDS3 represents significant fuel damage. This is a rapid core voiding and prolonged period with moderator as a heat sink (eg: Large LOCA plus loss of ECI).

The magnitude of fuel damage associated with PDS4 is quite small, and largely represents an economic rather than a public health risk. This is a slow core voiding and prolonged period with moderator as heat sink. It is typically the result of a small LOCA with the failure of ECI or any size LOCA and failure of LTC in ECC mode.

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 LOCA with Successful Initiation of ECC - PDS5

This category includes events when there is a certain size LOCA and ECC is successful. There could be fuel failures with pressure tube intact.

4.9.2.4 Power Cooling Mismatch with Late ECC Injection Due to Multiple Channel Failure – PDS6

This category includes events when there is a delayed LOCA consequential to loss of heat sinks. Multiple channel failure occurs with delayed ECC as a result of power cooling mismatch.

4.9.2.5 Loss of Cooling in a Single Channel – PDS7 and PDS8

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 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 PDS7.
- 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 PDS8.

4.9.2.6 Tritium Release – PDS9

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 – PDS9-1,
2. Fast release of moderator into containment (fuel cooling is maintained) – PDS9-2, and
3. Slow release of moderator into containment (fuel cooling is maintained) – PDS9-3.

4.9.2.7 Loss of cooling to Fuelling Machine – PDS10

A separate PDS has been defined for this event, as there is a potential fuel damage which is comparable to single channel events. This will be included in the PSA when details of fuelling machine design and operation are known.

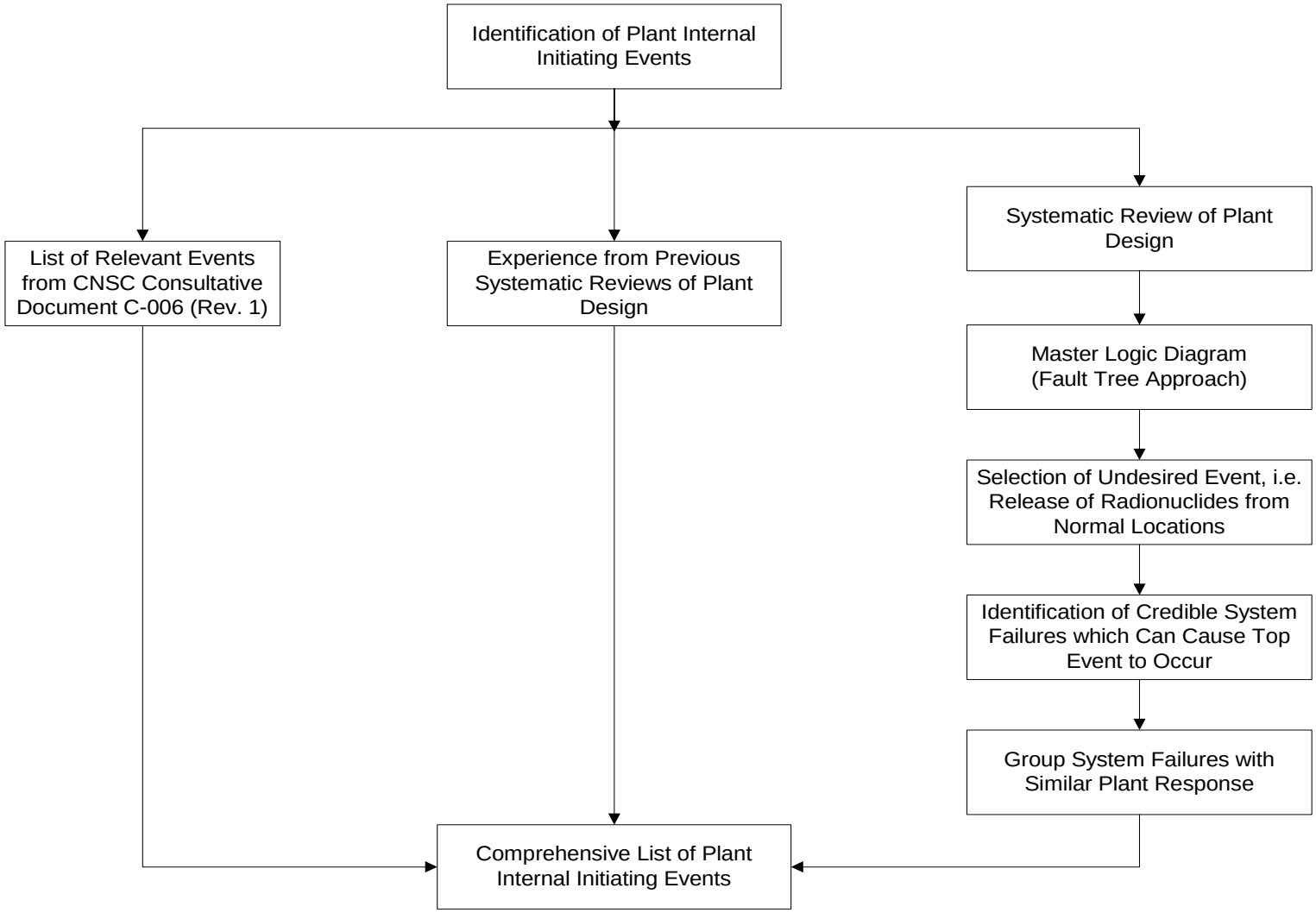


Figure 4-1 Plant Internal Event Identification

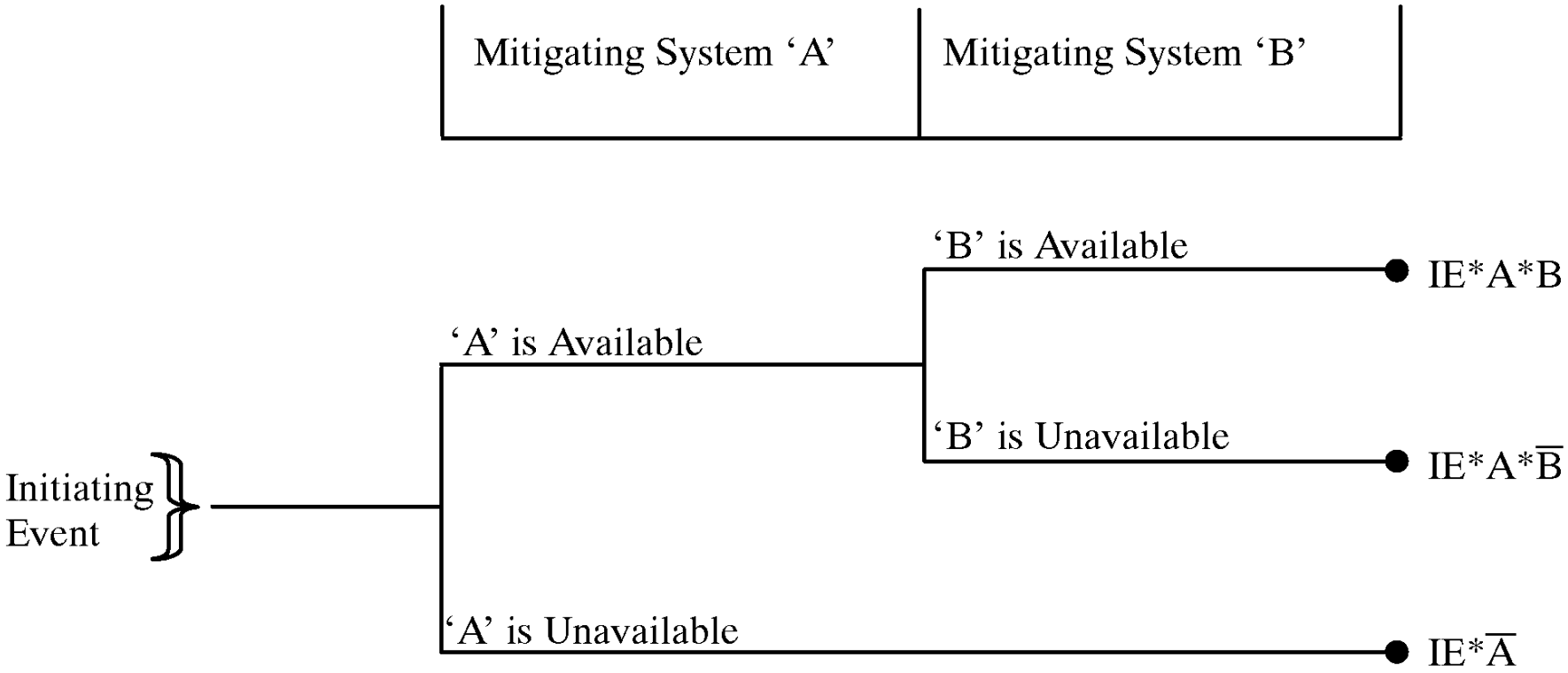


Figure 4-2 Simplified Example of an Event Tree

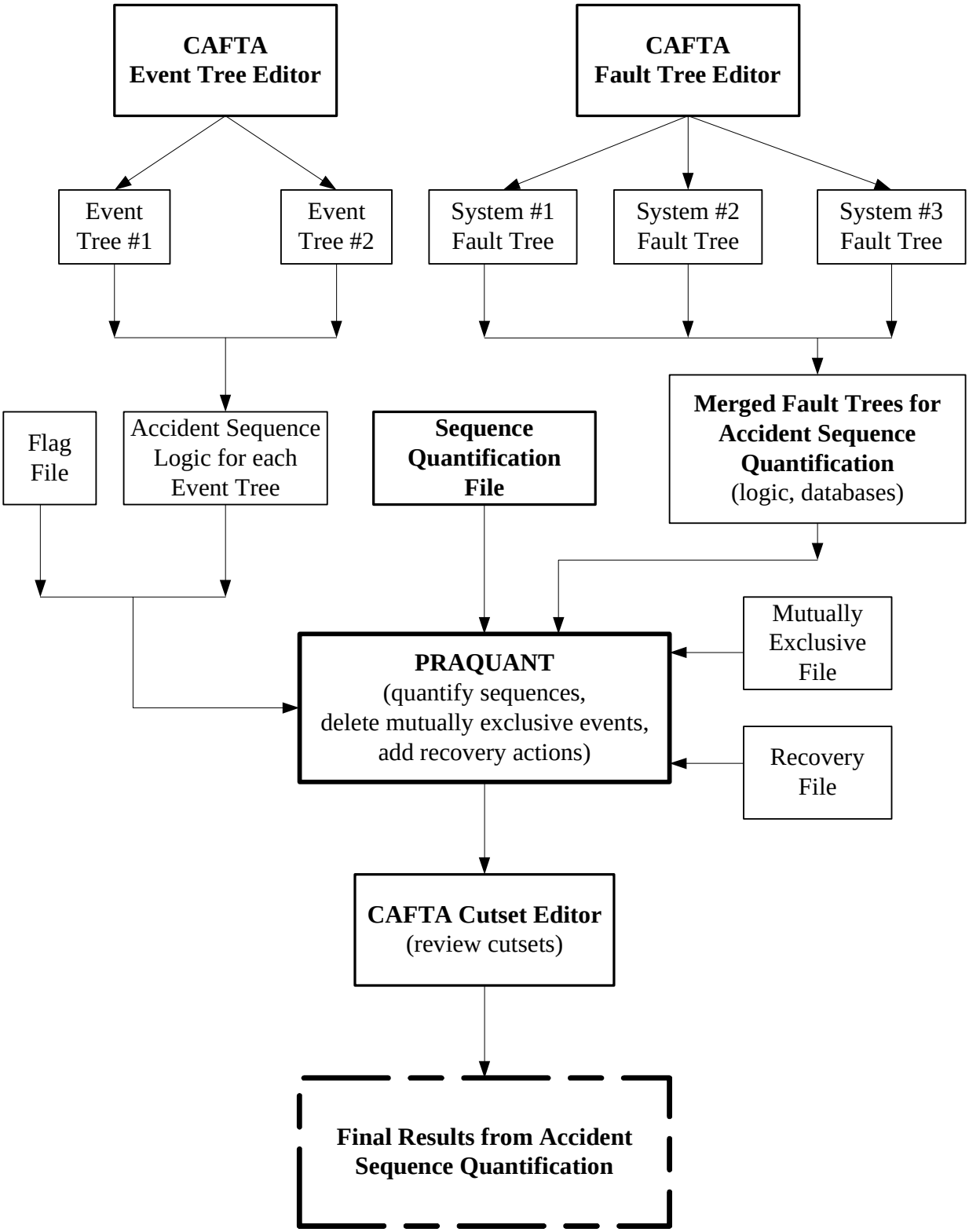


Figure 4-3 Analysis Procedure Using DS&S Codes

5. DEPENDENT FAILURE ANALYSIS

5.1 Introduction

The reliability requirements of many ACR systems are such that the design of these systems incorporates redundancy. When a system design includes two or more redundant trains of equipment, each of which is capable of performing the system function, the possibility of dependent failure exists. Dependent failure is an overall term applied to events which can cause multiple components to be unavailable because they are coupled in some fashion. In particular, dependent failures can affect the redundant trains in a system simultaneously and cause overall system failure. It is essential to carry out dependent failure analysis for systems incorporating redundancy since dependent failure is often a significant contributor to the overall system failure probability.

Dependent failures can be classified into two main types: explicit and implicit. Explicit dependencies are clearly identified as to the specific cause of dependent failure and quantified in the systems analysis. These include three main areas:

a) functional dependencies - redundant trains of equipment relying on common support services (e.g., cooling water, electrical systems)

b) physical interactions - physical phenomena which can impact multiple components such as the external events (fire, flood, seismic)

c) human interactions - pre-accident human errors in the testing or maintenance of redundant components are addressed in human reliability analysis.

The implicit dependencies are the “residual” causes of multiple component failures. These are known as Common Cause Failures (CCFs). Generally the root causes of such failures are related to environmental conditions that locally affect redundant components, common design faults, or additional human interactions which are not identified in the human reliability analysis. The modelling is implicit in the sense that the CCF events incorporated in the fault tree encompass a variety of potential causes which are not explicitly stated. In some cases, causes such as environmental factors can be modelled explicitly if sufficient data are available to do so. Where such information is not readily available, these causes are included in the domain of CCFs.

One purpose of the ACR PSA program is to perform an assessment of the plant design and determine which components and systems contribute most to the overall severe core damage frequency (SCDF). Due to the expected importance of common cause failures, a methodology is required to assess their probability of occurrence for specific sets of redundant components. This information can then be used to recommend specific design changes to minimize susceptibility to CCFs and thereby reduce the SCDF.

The Unified Partial Method (UPM) [13] is a method which enables CCF 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 report 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 incorporating both qualitative and quantitative analyses are thus realised. One of the main conclusions from the Common Cause Failure Reliability Benchmark Exercise (CCF-RBE) was that it is essential to combine qualitative and quantitative methods when performing CCF analysis.

Numerous alternative approaches to quantifying common cause failure probabilities exist. Each 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 incorporate CANDU-specific CCF data into the calculation of CCF basic event probabilities. 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 such generic CCF data and allows the analyst to take credits or penalties for design features and maintenance/operating practices which 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 common cause failure 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 [15], 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 ACR PSA.

5.2 Scope and Objective

This section is intended to provide a methodology for ACR PSA CCF analysis using the UPM, and should be used in concert with the UPM workbook [13], which contains a detailed explanation of aspects of the development and use of the method. The following sections explain the main features of the UPM and the tasks involved in its application. In addition, some guidance is presented on additional aspects of CCF analysis that are not addressed in detail by the workbook. This includes such topics as selection of CCF component groups, incorporation of CCF events into fault tree models, the CCF fault tree event labelling scheme and modifications to the basic UPM which can fine-tune the modelling results and/or reduce the effort required of the analyst.

5.3 Background

The importance of dependent failures in redundant systems has long been recognized and over the past 15 to 20 years many models for CCF assessments have been proposed. These models broadly fall into two main categories according to whether the analysis is applied at a system or at a component level. The system level models estimate a limit to system reliability based on analysis of the overall system vulnerability to CCFs. Component level models consider sets of

redundant components and estimate the probability of CCF within the set based on the features of the components under consideration.

All CCF models require an element of engineering judgment to be applied. It is important that the CCF analysis acknowledges this. The basis on which judgments are made is also an important part of a CCF analysis.

UPM is a development of the Partial Beta Factor method for assessing CCFs at the component level. The historical development of UPM is discussed fully in the workbook [13]. A brief description of the partial beta method and the main developments of this method which resulted in UPM are included in this section.

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 is required to assess a partial beta factor for each of these topics. The value selected has to be between a specified minimum and unity, based on the features of the set of components under review. An overall beta factor is then calculated by multiplying all 19 partial beta factors together. The minimum partial beta factors were adjusted so that there is a lower limit of beta = 0.02 for systems with identically redundant components and of beta = 0.001 for systems incorporating 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 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 which 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 uses the same model structure as for the partial beta factor approach but calculates a system cut-off, or limiting CCF probability, by modifying the factor definitions and the calibration appropriately.

5.4 Main Features of UPM

The main features of the UPM method are [13]:

- 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. It 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 which 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 [13].
- The method 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 common cause failures. The system reliability estimate is therefore based on a qualitative comparison of the features of the system being modelled and historical experience/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 for levels of redundancy beyond duplicity within the assessment. 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.

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 [13] specifically makes mention of 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 5.5.5.2.
- 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 which incorporate software is specifically placed outside the scope of UPM.

The UPM workbook [13] guides the analyst through the steps of the method and includes specific advice on the correct interpretation of the various subfactors which are considered. The structure of the UPM workbook has been designed to try and ensure 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 (& 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 common cause failure issues and receive feedback from reliability analysts at the time of design formulation, credit may be taken for reduced CCF probability.
5. M.M.I. (Man Machine Interface): This sub-factor is used to account for the possibility of human actions affecting multiple components. Better procedures, limitations on human interaction, and checking and testing of maintenance actions all serve to reduce the CCF probability. See Section 5.5.5.2 for a discussion of this category in the context of the larger PSA.
6. Safety Culture: The level of training of staff relates to the probability of human actions which result in failures of multiple components, especially those actions which 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, limiting the number of local sources of potential environment-related CCFs (e.g., temperature, moisture) reduces the probability of such failures.
8. Environmental Testing: Here emphasis is placed on the benefits of verifying manufacturers' claims for environmental qualification. Lower CCF probabilities are claimed when example units are subjected to a variety of tests.

5.5 Application of The Unified Partial Method for CCF Analysis

5.5.1 Selection of Common Cause Component Groups

The most important, and perhaps the most difficult task in a component-level CCF analysis is defining 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 it. 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 is adapted from NUREG-CR-4780 [15], 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 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 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.

Identifying potential members of a CCF group is facilitated by examining system flowsheets 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 and/or operating characteristics
- component testing procedures and characteristics; e.g., test interval, test configuration, etc.
- 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 flowsheets 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 which must be answered is: are they in fact redundant? If either component can by itself cause a system failure, 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 how many components 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. Including 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 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 below:

Figure 5-1 CCF Grouping Example #1

System failure is defined as 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, credit will be taken for the large separation between AB and CD. However, this is misleading because 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 which causes two nearby valves to fail open is more likely than one which 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 was taken for the enhanced separation. This is 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 associated with not including enough 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, pneumatically connected in series as shown in Figure 5-2:

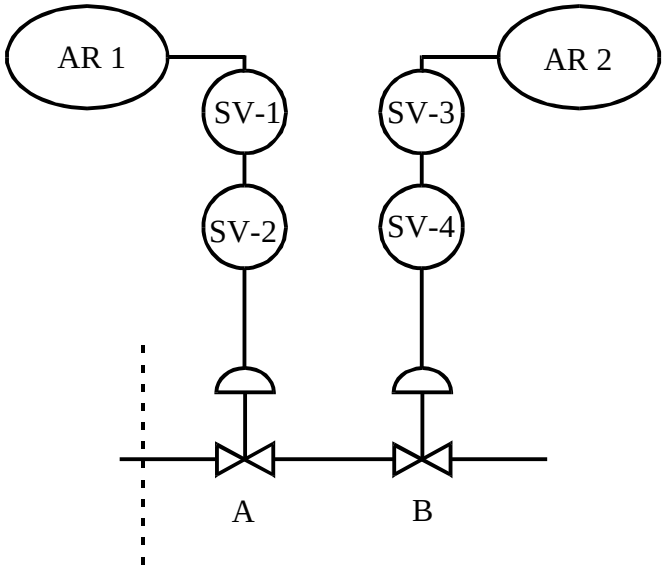


Figure 5-2 CCF Grouping Example #2

From the standpoint of a single pneumatic valve, there is dual redundancy. However, 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 (CCF of solenoid valves SV1, SV2, SV3 and SV4 together). This will also be conservative compared with the alternate groupings of SV-12 (CCF of SV1 and SV2 together) and SV-34 (CCF of SV3 and SV4). For it to be non-conservative, the sum of the probabilities of the second order cutsets SV-12*B (CCF of solenoid valves SV1 & SV2 "ANDed" with the failure of valve B), SV-34*A (CCF of solenoid valves SV3 & SV4 "ANDed" with the failure of valve 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 artifact 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.

5.5.2 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 adjacent to each basic event which 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 an additional failure mode of each component, as in Figure 5-3.

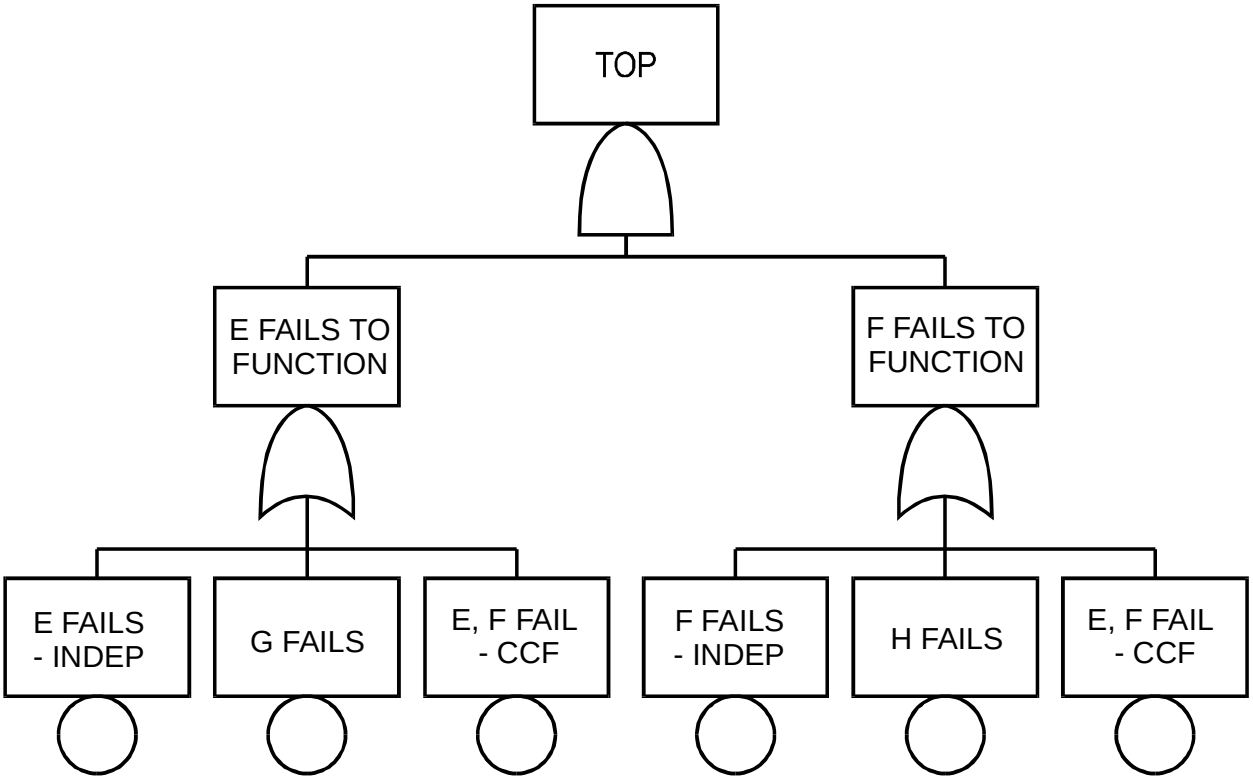


Figure 5-3 Addition of CCF Basic Events to Fault Tree

The output of the UPM is a beta factor which may be multiplied by the component total random failure probability to get the CCF failure probability, i.e.

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

where

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

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

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 [13] suggests using one of two values. 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}, i.e.,

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

When the fault tree structure shows the failure of a component 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 different failure modes are tested for at different intervals, 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, it makes little sense to apply a separate beta factor to these events or 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 accounted for within the beta factor 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 using these failure rates to get the independent component failure probabilities represents double-counting where CCFs are modelled. In theory, the independent failure probability, P_{INDEP}, should be calculated as follows:

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

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}.

5.5.3 Calculation of Beta Factors

5.5.3.1 Screening Analysis

Having identified a common cause component group and created an appropriate fault tree basic event, the analyst must 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 of the analyst to document his or her assumptions and fill out the UPM "judgment tables" to arrive at a beta factor may be substantial. Therefore, a quantitative screening shall be done before applying the UPM directly.

NUREG-CR-4780 [15] 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 which contribute most to the top event unavailability of a given fault tree. This can be determined by examining the top 100 minimal cutsets or, alternatively, 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 re-evaluated.

Following CCF analysis by UPM, if the CCF events are still dominant risk contributors, then other CCF analysis techniques (e.g: MGL, alpha factors) may be used as necessary.

5.5.3.2 Detailed Analysis

The UPM must be applied to those component groups which survive the quantitative screening. The method is structured to provide a framework which allows the analyst to firstly, 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 [13]:

1) The system to be analyzed must be clearly defined. It is necessary to define the physical boundary of the system, i.e., which components and parts of the system are to be considered in the analysis. See Section 5.1 for further discussion of this step, which is not unique to the UPM.
2) For ACR PSA, a component level assessment seems appropriate, because system reliability calculations will be made using detailed fault trees. See Section 5.4 for further information.
3) The third step is to consult the judgement tables for each sub-factor. Each table relates to a different aspect of system design or operation and its effectiveness in defending against CCF. The analyst must choose the system description which most closely matches the system under consideration out of the five which are listed in the tables. Justification for the choices must be recorded in tables for each CCF component group, using the format shown in Table 5-1.
4) Step four is to fill in the estimation table, which summarizes the judgements made in the previous step. This step can be combined with step three by getting the numerical values for each sub factor from the UPM estimation table and entering the information in Table 5-1. This step is the bulk of the analysis.
5) Step five is to calculate the value of the system cut-off or component beta factor as appropriate.

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

Table 5-1
Judgment Table Format

Sub-Factor	Judgement Decision	Category/Numerical Value	Comment
Redundancy			
Separation			
Understanding			
Analysis			
Human Factors		N/A	see 5 5.5.2
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 =**	

5.5.4 Component Types and Boundaries

The types of components listed in Table 5-2 are to be modelled as part of ACR PSA CCF analysis. They have been selected based on the criteria listed in Section 5.1. That is, these components are active, and appear in non-diverse, redundant structures within CANDU plants. Passive components may be also considered in a few limited cases. This is not intended to be an exhaustive listing, but rather a minimum requirement based on the types of components for which generic beta factors have been collected [18-21].

Table 5-2
Component Types and Boundaries for CCF Analysis

Component	Present Boundary
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.
Pneumatic Valves (PV)	Includes contribution from actuator, but not air supply to the actuator. Includes contribution from failure of associated limit and torque switches.
Pumps	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.
Air Compressors	Includes contribution from motor failures. It does not include contribution from loss of power supply to the motor.
Air Coolers	Cooling coil, fan/motor set modelled separately.
Batteries	Battery cells, interconnecting links and supporting structures. Does not include outgoing cables with their connections.
Diesel Generators	Includes motor and generator.
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.

5.5.5 Additional Considerations

There are a number of additional aspects of common cause failure analysis using the UPM which 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.

5.5.5.1 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 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 common cause failure, a fairly simple methodology for running/standby CCF events is proposed here.

According to the UPM manual, a common cause failure is defined as "a dependent failure event where simultaneous or near simultaneous multiple failures result from a single shared cause…" Although 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, the fact that the running item is assumed 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 failure of both the 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 above 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 accounted for in special analyses and are therefore beyond the scope of the UPM or other CCF methods.

5.5.5.1.1 Summary

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

a) If two or more CCF components are running prior to the initiating event and required to run during mission, 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 components are dormant (standby) prior to the initiating event, both failure to start and 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.

5.5.5.2 Interface with Human Reliability Analysis (HRA)

The UPM attempts to quantify the human contribution to common cause failures through two of its sub-factors. These are the M.M.I. (Man Machine Interface) and Safety Culture sub-factors. As there is a potential overlap with HRA methodologies within the M.M.I sub-factor, the analyst must take care to avoid double-counting.

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

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 referring 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 components unavailable by using manual overrides or performing other errors of commission, presumably in a post-accident situation. In cases where components perform their function without any interaction 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 sub-factor. At least for these components, the presence or absence of written procedures for operating/monitoring the system has no relevance.

HRA is typically used to model obvious human errors which 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 temporarily cross-tying 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 sub-factor of the UPM.

5.5.5.2.1 Summary

Human actions that can cause unavailability of redundant components shall be modelled explicitly using HRA methods. Therefore, the M.M.I. sub-factor shall be assigned a value of zero and shown as not applicable.

5.5.5.3 Interface with External Events PSA

It is very important to distinguish root causes of multiple component failures which are included in the CCF analysis from those which are not. When a full-scope PSA includes external events and other hazards, component unavailability due to certain causes is modelled explicitly to arrive at plant damage frequency estimates. The “external” events and other hazards to be evaluated in

ACR PSA are seismic events, internal fires and internal flooding. 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 sub-factors are not generally based on cause, but instead on CCF defences, it is difficult to break down the beta-factor to eliminate these events as contributors. A solution might be to scale down the Separation and/or Environmental Test sub-factor values by some constant. The aim would be to reduce the CCF unavailability of a given set of components by an amount 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 underlying the UPM's beta factors includes failures due to these causes.

5.5.5.3.1 Summary

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

5.5.5.4 Staggered Testing

One effective means of defending against CCFs which 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, 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.

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

If component A is found failed at Month 3, *and there is a procedural requirement that the redundant item B should be checked after the first failure is found*, 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, 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 left unavailable until it is tested at Month 4. If there is no checking of the second component 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. Staggered testing will be applied where necessary to reduce impact of CCF.

5.5.5.5 High Levels of Redundancy

A contentious issue in CCF modelling is how to deal with high levels of redundancy. By its very nature, the UPM models only those CCF events in which all components in a group are assumed failed. The particular *m* out of *n* success criterion affects the beta factor calculation (under the Redundancy sub-factor), 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 be for all sixteen items 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. Further complicating matters is the fact that the sub-factor 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, presumably an optimistic number. However, if the redundancy is assumed to be equivalent 1 out of 2, it is tantamount to saying that the probability of two identical components failing in a setup 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 which 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 design related, the other due to harsh environment). The likelihood of this occurring would seem negligible 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 is environmental degradation, periodic replacement/refurbishment of some fraction of the components would be an effective defence. Then it might be argued that separate groups are acceptable, perhaps with an additional limited CCF probability attributed across the groups. Otherwise, the analyst has little recourse but to use the UPM in its present conservative form.

5.5.5.6 Re-Assignment of Sub-Factor Categories

For each sub-factor, the UPM requires the analyst to select the category description which most closely resembles the components being studied. There are five categories to choose from (A through E) in the manual [13], except for the *Redundancy sub-factor*, which has seven. However, there is no particular restriction limiting 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 sub-factor for separation

than the worst case category A value. The sub-factor 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*. Then the *y*-value for a new category (e.g., A+) can be calculated, by choosing an appropriate *x*-value and substituting into the above expression. An example of how this may be done is shown for Table 5-4 below, in which it is desired to interpolate an A+ category midway between the A and B categories.

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

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+}:

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

5.5.5.7 Plant Safety Culture

The safety culture of the plant is addressed in one of the UPM sub-factors. For a plant which has not yet gone into operation, the eventual, "steady-state" management conditions and the levels of staff training and experience must be assumed.

6. HUMAN RELIABILITY ANALYSIS

6.1 Introduction

An important aspect of any Probabilistic Safety Assessment 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 interaction with the systems are often significant contributors to system unavailability. The purpose of human reliability analysis is to identify potential human errors and to quantify the most significant of these. This covers the analysis of the human actions of potential concern identified during the PSA process.

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 human reliability analyses for quantifying the potential contribution of human error to accident sequence frequencies. All methods have merits and limitations under the particular circumstances in which they are applied. The human reliability analysis methodology described in this report is based on previous work in this area done in AECL and on industry accepted methods and guidelines.

For pre-accident, 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 and for other facilities as Irradiation Radiation Facility and National Research Universal (heavy-water moderated and cooled test reactor of AECL). A particular attention in the ACR PSA is given to modelling the post-accident execution errors in line with international practice, based on the ASEP procedure, Reference 25.

This report also covers post-accident execution actions modelling for external events - fire and earthquake. The HRA modelling for fire PSA considers the adverse effects of a fire in the main control room in a manner similar to that employed in other IPEEE (Individual Plant Examination for External Events) studies. The model for HRA quantification during seismic events accounts for the intensity of the earthquake, elapsed time after the earthquake, and location of the operator (MCR, SCA or field). Different performance shaping factors are used, according to different earthquake design and qualification for MCR, SCA and other structures and systems for the ACR.

This report also includes modelling Human Error Probabilities (HEPs) for recovery actions based on the methodology for quantification of post-accident operator errors. Operator actions 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

Review of several PSA studies have indicated that it is necessary to account for different types of human actions, some of which may mitigate the consequences of an accident while others may increase the severity. These reviews, the results of which are incorporated in EPRI documents, identified five basic types of generic human actions common to nuclear power plants. In general, these five basic types of human actions can be grouped in 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 which lead directly to initiating events (initiators);

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

These categories facilitate the incorporation of HRA results in the PSA structure and are determined by the way in which they are generally analysed 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, test, calibration and repair errors which 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 not be detected 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 which 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 initiated by an error in following testing procedures. Category B type actions are not modelled in the ACR PSA. They are presumed included in initiating events' 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 complement 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. They 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 thus 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 is the most difficult to identify and model and is not considered in the ACR PSA human reliability analysis as errors of commission. Also, this methodology does not address sabotage, bad 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 to terminate an accident. These interactions consist of recovery actions, which are generally included in accident sequences that dominate risk. These actions may include recovery of previously unavailable equipment or the use of non-standard procedures to mitigate the accident conditions. Recovery actions are considered in the ACR PSA.

6.2.2 Classification of Tasks

A task classification scheme is required for identifying different types of human action or behaviour, and associated error mechanisms, and is suitable for PSA purposes. A well known task classification scheme presented in chapter 2 of the ASEP HRA procedure, Reference 25, is adopted. This model distinguishes between three following 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 which 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 applies to those actions which must be taken quickly following an initiating event, and which are supposed to be committed to memory by the operating personnel.

b) Rule-based Behaviour

Human actions requiring the performance of less familiar tasks which require more conscious mental effort than skill-based tasks, are usually described as rule-based. 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 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 requiring 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 (for example, operator actions for accident situations not previously included in operating procedures and/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 in the execution stage. For a more detailed description of this task classification scheme, see Chapter 2 of the ASEP HRA Procedure, Reference 25.

6.3 Organization of Shift Operating Staff

This section comprises the assumption of how the shift operating staff would be organized in an ACR plant. The typical operating crew for a single unit station would have the following structure:

- Shift Supervisor (SS), licensed as Control Room Operator and as Field Operator
- Control Room Operator 1 (CRO1), licensed also as Field Operator
- Field Operator (FO), named also Control Room Operator 2 - CRO2, licensed also as Control Room Operator
- Principal Power Operator 1 (PPO1), named also Senior Secondary Operator
- 8 Principal Power Operators 2 (PPO2) which are field operators located in various areas in the plant

The SS, CRO1, FO and PPO1 are permanently in the Main Control Room (MCR) and are available to act in accident situations. There is generally no permanent operator in the Secondary Control Area (SCA).

In accident situations, the diagnosis in the MCR is performed by CRO1 and verified by SS. All execution actions which do not involve changes of reactor power are performed by PPO1 at request from CRO1. CRO1 and SS provide two levels of verification for execution actions. Operator actions in MCR involving changes of reactor power, including manual shutdown, are performed by CRO1 and verified by SS.

The field actions are requested by CRO1 and executed by the operators PPO2. The execution actions are verified in the field by the field operator FO. The effect of the action executed in the field is checked in MCR by CRO1, which thus provides the verification. Although SS may also verify the effect of field actions, we conservatively assume only verification by FO and CRO1.

6.4 Pre-Accident Human Reliability Analysis

6.4.1 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 opening or closing manual or motor operated valves, following repair or test, to restore these valves to their normal operating position or status. These tasks are usually performed by operations personnel, instrumentation and control personnel, and maintenance personnel under non-accident conditions. Pre-accident tasks can affect the availability of safety systems required to mitigate an accident sequence.

In the evaluation of pre-accident tasks for an existing plant design, 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 which 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 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 human reliability analysis considers the ability of people to understand and implement rules (usually written rules).

6.4.2 Basic Human Error Probability

The ASEP HRA Procedure (Reference 25) presents a simplified model of human behaviour for pre-accident tasks. The model includes a generic basic human error probability (BHEP) which can be used, Reference 3, for all pre-accident tasks, as well as rules to adjust this basic human error probability (BHEP) for the effects of dependence and recovery factors. The BHEP has a value of 3E-2 is for performance of pre-accident actions, exclusive of any recovery factors (RFs). Thus for each key action that must be accomplished, e.g., restore a valve to its normal operating position after maintenance, or perform a critical step in a calibration procedure, a total BHEP of 3E-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 1E-2 (Reference 27).

6.4.3 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 internal characteristics.

Performance shaping factors, 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 accounted for, to some degree, in the uncertainty bounds for the various HEPs. If it is considered necessary, the BHEP of 3E-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 but 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.

6.4.4 Recovery Factors

A recovery factor (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 apply to the effects on human performance of displays of component status in the control room (especially those which 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 Recovery Factors are not part of the post-accident Recovery Analysis discussed in Section 6.8.

In the ASEP HRA Procedure for pre-accident tasks (Reference 25), 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 ACR PSA human reliability analysis, RFs will be credited for written checklists on the assumption that these checklists are available and required to be checked off.

The procedure makes a distinction 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.E-02 is assumed. The following recovery factors are applied.

a) *Indication in MCR or SCA*: Unavailable component status is indicated in the Main Control Room (MCR) or Secondary Control Area (SCA) 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 1E-4 is assessed for failure to detect unavailable status of component due to a compelling signal, that is, one that demands the same kind of attention from an operator as an annunciator.

   An RF of 1E-2 is assessed for failures to detect the unavailable status of components due to all other forms of indication in the control room, such as a CRT alarm or panel indicating lights.

   This is based on past CANDU experience. This will be confirmed later by detailed analysis of MCR alarms.

b) PM or PC Test: Component status is verified by a Post Maintenance (PM) or Post Calibration (PC) test. If done correctly, full recovery of any related error is assumed. An RF of 1E-2 is assessed for failure to perform the test correctly (including failure to do the test), based on the ASEP HRA Procedure, Reference 25.

c) Written Verification: There is a requirement for an RF involving (1) a second person (checker) to verify directly the component status after 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 original task performance. No credit is given for either check unless a written checklist is used during the check.

   An RF of 1E-1 is assessed for 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 25.

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 1E-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 25.

Determination of the applicable recovery factors to the specific activity under review is based on the data given in Table 6-1, based on ASEP HRA Procedure (Table 5-3 in Reference 25).

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 25, for the cases applicable to critical activities

2) See Section 6.4.2 for comments on Basic Human Error Probability.

3) See Section 6.4.4, item a for comments on compelling signals and/or other types of MCR indication.

4) See Section 6.4.4, item b for comments on recovery factors applicable to post-maintenance and post-calibration tests.

5) See Section 6.4.4, item c for the requirements on recovery factors involving written verification of component status following maintenance or calibration

6) See Section 6.4.4, 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 per Section 6.4.4, item b.

** An HEP of 1.E-04 is assumed for a compelling signal and an HEP of 1.E-02 is assumed for all other types of MCR indication.

6.4.5 Dependence Effects

Dependence between two tasks, or activities, refers to the situation in which the probability of failure on one task is influenced by whether a success or failure occurred on 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 28.

The BHEP of 3E-2 must be modified for the effects of dependence. As noted in Section 6.4.4 between-person dependence is already included in the HEPs for the recovery factors. 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 that in 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.

6.4.5.1 Levels of Dependence

Dependence is a continuum, discretized for practical reasons in a number of levels, varying from two levels (zero dependence and complete dependence) in ASEP HRA Procedure, Reference 25, to five discrete levels in Handbook of Human Reliability, Reference 28.

In this report the dependence is discretized in four levels, from zero (no) dependence to complete dependence. This is a conservative simplification. These four levels will be used if the ASEP process (two levels) is shown to be unduly conservative.

The levels of dependence in this model are:

a) Zero dependence (ZD)

b) Moderate dependence (MD)

c) High dependence (HD)

d) Complete dependence (CD)

6.4.5.2 Assessment of Dependence

For pre-accident errors, the modelling of dependent errors in the fault trees is affected by the level of dependence assigned between the errors. Equations for the calculation of the conditional failure probabilities 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 28, and are based on the positive dependence model. Guidance for the assessment of dependences is given in Figure 6-1 derived from Table 5-1 and Figure 5-1 of the ASEP HRA Procedure. In the ACR PSA dependencies will be analyzed only at system level and not at sequence level.

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 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 common cause failure 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 $P_{[B|A]}$, i.e.,

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

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 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.

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 failure on previous Task "A" for five levels of dependence. This table is based on Table 10-2 of NUREG/CR-1278, Reference 28.
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

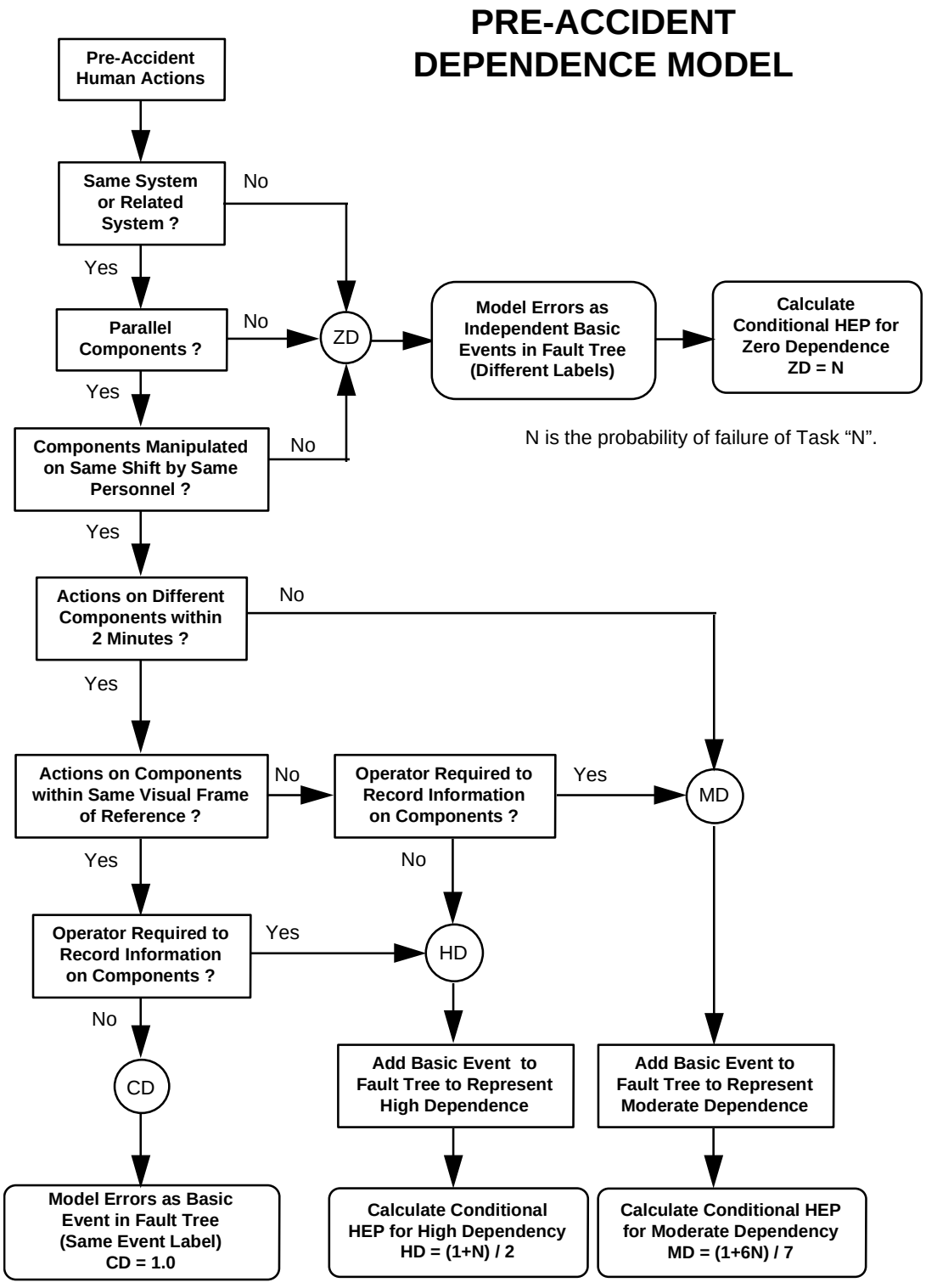


Figure 6-1 Model for Assessing Positive Dependence for Pre-Accident Task; In ACR PSA Dependencies are Evaluated at System Level Only

6.4.6 Quantification

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

a) Basic Human Error Probability

A total BHEP of 3E-02 is assigned for each critical action.

b) Performance Shaping Factors

The only explicit PSF, excluding recovery factors and dependence effects, considered in the calculation of the pre-accident nominal human error probability (NHEP) is radiation. If the critical action is performed in a radiation area, the BHEP is multiplied by a factor of 2, see Section 6.4.3.

c) Recovery Factors

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

d) Dependence Effects

1) Series System (ZD)

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

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

Where the BHEP has the value of 3E-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 nominal human error probability 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 nominal human error probability is approximated by the following equation:

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

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

6.4.7 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 6.4.4, the following equation can be used (Reference 28):

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

Where:

U = unavailability,

E = the basic HEP (3E-2),

R = the probability of failing to recover from the error that results in a component being in the failed condition,

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

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;

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 is available, otherwise conservative numbers will be used based on judgement.

6.5 Post-Accident Human Reliability Analysis For Internal Events

6.5.1 Introduction

Post-accident human actions typically pertain to activities performed by reactor operators stationed in the main control room, and which 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.
- The automatic actuation of a mitigating system was successful, but its continuing operation requires operator action (ex. replenishing of water inventories for feedwater after 8 hours).
- There are no design features for automatic mitigating action.

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

Post-diagnosis actions are activities 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.

6.5.2 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 requiring 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/subsystem is affected by the operator action.

As a result, a pre-requisite for the systematic identification of post-accident human actions are the accident sequence event trees for each initiating event. In addition to the event trees, the analyst reviews emergency procedures 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 followed by the operator, clearly specifying the next required action.

6.5.3 Time Relationship between Diagnosis and Execution Tasks

One of the simplifications 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 analysts 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 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 analysts. The time left after this subtraction is the allowable diagnosis time. The diagnosis time is expressed as:

$$\mathbf{T}_d = \mathbf{T_m} - \mathbf{T_a}$$

where:

T_m = 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) so as to meet system success criteria established by the systems analysts.

T_d = 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 T_m

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

6.5.4 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 to the operator of the off-normal condition, and specifically excludes the time taken to execute the specific corrective action required, see Section 6.5.3. 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 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 expected to be in the control room following an abnormal event.

Table 6-3
Diagnosis Model for Estimated BHEPs and Error Factors

Item	Diagnosis Time (Td) (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 human error probabilities in this table represent the joint HEP for the performance of the entire control room crew. This is based on the ASEP procedure (Reference 25).

6.5.5 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 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 controlling 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 performance effectiveness of system-required behaviour for most people. The onset of an abnormal event 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 which causes the performance of most people to deteriorate drastically. The occasion of a large loss-of-coolant accident is assessed as resulting in extremely high stress to operating personnel. For example, in Reference 5, 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;

c) More than two safety-related systems fail.

The nominal HEPs for post-accident execution errors are quantified based on ASEP methodology, Reference 25. The common practice for determining nominal HEP is to use the median values for HEP, Reference 5, which include the effects of stress and complexity of the task. The human error probabilities assessed for the type of task and stress level are based on the values in Table 8-5, Reference 25 and in Table 7.3-14, Reference 5, and are given in the Table 6-4. The original performer (OP1) is the operator performing the task. In the case when recovery of OP1 errors is still possible at the point of error action, use the HEP for the related task and stress categories for the second person in the operating crew (OP2). Also, a third operator can be credited for verifying the emergency actions and taking recovery actions during an abnormal state of the plant. Verification may consist in checking and monitoring the adequacy of heat sink configuration.

If there are recovery factors (RFs) other than human redundancy (checkers), the influence of these RFs will be assessed separately. Credit to second and/or third operator (checker) can be given according to the structure of the operation crew described in Section 6.3. 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:

For the tasks performed in the Main Control Room:

a) If the allowed time is greater than 30 minutes, the credit for the second operator is given.

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

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

a) If the allowed time is shorter than 60 minutes, the credit for the second operator is not given.

b) If the allowed time is longer than 60 minutes, the 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 human error probability for the activity under investigation. For the tasks when there is insufficient time to execute the task the operator is not credited (HEP=1).

6.5.6 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 for high dependence (HD) the conditional failure probability equations given in Table 6-2 (see Section 6.4.5) are used.

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 making up the set can be judged to be completely dependent.

b) An 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 according to the structure of the operation crew described in Section 6.3. The HEP for the third operator (checker) is the same as that for the second operator (checker).

6.5.7 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 which must be taken within the total allowable time. Thus, the total failure probability for combined diagnosis and execution tasks is given by the following equation:

$$P_t = P_d + P_e - P_d \times P_e$$

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:

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

6.6 Human Reliability Analysis For Fire Events

We assume that fire events in various areas in the plant do not influence operator performance in the main control room. So HEPs for such fire events are considered to be the same as for the internal events PSA. For the case of fire in the main control room, the HEP for post-accident execution actions will be considered during the PSA, to account for the increased stress. This approach is consistent with HRA modelling in the IPEEE for Zion and for Byron plants, References 29 and 30.

6.7 Human Reliability Analysis For Seismic Events

During a seismic event the operator faces a complex situation due to the supplementary stress caused by the earthquake itself, random damage of systems and components, possible induced fires and floods, aftershocks, and likely impaired communications and control room indications. The time 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. For ACR, the main control room is habitable after an earthquake.

It is reasonable to assume that the impact on human actions will vary with the strength of the seismic event. Thus, we assume that operators will be unable to perform required actions at seismic levels high enough to fail the building structure because they 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 if compared with the Internal Events PSA case. Regardless of the earthquake “g” level however, most of the operators have not experienced a seismic event and this can adversely affect their performance.

Also, a seismic event is assumed to have 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 Performance Shaping Factors, (PSFs) Reference 31.

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 be commencing, producing some chaos 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/outside control room may not be mentally or physically available to perform a desired task.
- Location of action.
- Complexity of task.

6.8 Recovery Analysis

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

Based on the approach the steps involved in recovery analysis are the following:

a) Obtain information for post-accident analysis.

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

c) Develop accident sequence description.

d) Determine sequence and cutset timing.

e) Identify potential recovery actions.

f) Determine available operator time.

g) Determine operator performance time.

h) Select viable operator action.

i) Determine human error probability (HEP).

6.8.1 Obtain Information for Post-Accident Analysis

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

6.8.2 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/subsystem is affected by the operator action.

6.8.3 Develop Accident Sequence Description

The accident sequences 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.
- Accident Type and subsequent Plant Damage State.

6.8.4 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 cutsets for recovery analysis are chosen among those having a dominant contribution within the ASQ set of cutsets. For practical purposes, these accident sequences are to be of a frequency 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), b), c), d) in Section 6.8. 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.

6.8.5 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.

6.8.6 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).

6.8.7 Determine Operator Performance Time

The operator performance time is the time the operator needs to execute the recovery action. If the action is simple and performed in the main control room, it may require only a few minutes. If the action is performed in the SCA, add another 15 minutes to the operator action time.

6.8.8 Select Viable Operator Action

A recovery action is considered viable if the time required to perform the action is smaller than the amount of time available to perform the action. If more than one operator action is capable of restoring core cooling, the recommended order in which these actions are to be initiated, is:

- Restore Auxiliary Feedwater,
- Restore Long Term (Shutdown) Cooling,
- Start Reserve Water Makeup to Steam Generators.

6.8.9 Determine Human Error Probability (HEP)

Human error probabilities for recovery actions include the contribution of diagnosis errors and of execution errors, calculated according to the methodology for quantification of post-accident operator errors, described in the Section 5. Human error probabilities for recovery actions during fire or seismic events will also consider the factors defined in the Section 6.6 and Section 6.7 respectively.

At cutset level, the maximum credit for human error composite should not be greater than 10^{-5} when the time available is between 4 to 8 hours, and than 10^{-4} when the operator has between 2 to 4 hours to act.

7. EXTERNAL EVENTS ANALYSES

7.1 Introduction

External events in the ACR are defined to be initiating events originating outside a nuclear power plant systems that cause safety system failures, operator errors, or both, that in turn may lead to core damage or large radiation release. These external events are of particular concern because they are "common cause" initiators. In other words, the event itself can cause initiating events as well as failures of redundant components and systems, and thereby reduce the number of mitigating systems available to bring the plant to a safe and stable state.

There are many potential external events. NUREG-1407 [32] recommends to use the progressive screening approach for determining external events that require detailed analysis. One of the screening criteria that the reference suggested is based on whether the plant design satisfies the 1975 Standard Review Plan (SRP). The ACR design is expected to satisfy all current criteria of the SRP through site selection criteria and/or designing the plant against the potential external events. Thus the external events except the seismic, which the reference requires to address, can be screened out.

The methodology for analysis of the other common cause events such as internal fires and internal floods is covered in Sections 8 and 9 respectively. The plant damage states are defined in Section 4.9.

7.2 PSA-BASED SEISMIC MARGIN ASSESSMENT

7.2.1 Introduction

Seismic events are one group of external events requiring further analyses. 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 [12] provides a general procedural guide for conducting a seismic PSA. NUREG-1407 [32] contains specific procedures and submittal guidance for conducting external event analyses, including seismic events. The report [32] was written by the US Nuclear Regulatory Commission (USNRC) for the Individual Plant Examination of External Events (IPEEE) for the Light Water Reactors in the United States. 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 [33]. CNSC's Consultative Document C-006 Rev. 1 [1] provides the requirements for the safety analysis of CANDU nuclear power plants, which includes provisions for analysis of common cause events under Section 3. The document includes seismic events in the Table 2.5 – "*Specified Common Cause Events*" under the generic term *earthquake*.

A PSA based seismic margin assessment is adopted for seismic analysis of ACR design. It was considered appropriate to follow SECY-93-087 recommendations (Reference 70). A PSA-based seismic margin assessment consists of similar steps to a seismic PSA but does not include the step of development of seismic hazard and integration of the hazard curve with the rest of the analysis. This method eliminates the need to deal with the uncertainty in the seismic hazard curve.

The PSA based SMA is based on an event/fault tree approach to delineate the accident sequence. In this method a seismic hazard curve is not used, instead HCLPF value obtained at the end of each end state of the Seismic Event Tree (SET) is used.

The following sub-sections present a description of PSA-Based Seismic Margin Assessment methodology.

7.2.2 Scope

There are many steps to be followed in performing a PSA based Seismic Margin Assessment. Figure 7-1 shows the typical steps involved in a PSA based Seismic Margin Assessment. The major steps in the PSA based Seismic Margin Assessment are listed below:

a) Select the 'Safety Objective HCLPF' (the design basis earthquake (DBE) for the ACR is 0.3 g and it is expected that a plant HCLPF value of 0.5 g will be adopted as a Safety Objective for the assessment, as recommended by the USNRC (Reference 70)).

b) Review Internal Events PSA and sequences related to PDS 0, 1, 2 (Section 4.0)

c) Collect and review seismic design guide, design criteria, seismic analysis reports, flow sheets, arrangement drawings, and other design documents and drawings.

d) Identify structures/components for seismic capacity analysis – Safe Shutdown Equipment List (SSEL).

e) Perform seismic capacity analysis for the structures/components selected in part (d) above.

f) Develop seismic initiating hierarch event trees and seismic event trees.

g) Develop seismic fault trees by modifying internal event fault trees.

h) Generate minimal cutsets by quantifying the seismic event trees in part (f)

i) Calculate HCLPF value and random failure probabilities for each minimal cutsets.

j) Derive the HCLPF value for each seismic core damage sequences in seismic event trees (h).

The plant HCLPF for PDS 0, 1, 2 is the minimum HCLPF value for those event sequences leading to PDS 0, 1,2. These steps are shown in Figure 7-1 and are discussed in the following sections.

7.3 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 events PSA or external events analyses. The PSA-based SMA requires additional work that involves the seismic capacity analysis of structures and components, relay chatter analysis, etc.

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 [34-36].

There are two seismic levels of earthquakes defined in accordance with CAN3-N289.1 [34] 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 less than 0.01 per year.

Non-safety related systems and structures are designed to an earthquake similar to what is adopted for normal industrial plants and public buildings. This earthquake is used as a minimum level for designing all structures and equipment in the ACR plant and its peak ground acceleration is selected 0.1 g. This level represents one third of the DBE level and forms the basis for operator action following an earthquake such as plant shutdown and inspection. (Reference 69).

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 available to the PSA team in a 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 documents,
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.

7.4 Systems Analysis

7.4.1 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.

7.4.2 Safe Shutdown Equipment List

The first step in the analysis is to identify the Safe Shutdown Equipment List (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 SMA.

The internal events PSA fault trees do not provide a complete list of equipment for the SMA; structural items must be added to the list, e.g., electrical panels and cabinets, instrument racks, walls, buildings, etc. For each safety function, the safety system(s) and its components must be identified (see example in Table 7-1).

Generally speaking, manual valves, check valves, small relief valves and other passive equipment are not included in 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 in the SSEL.

Various sources of information for the SSEL include the seismic qualification equipment list, 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 in 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 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 emergency operating procedures for the loss of offsite power, etc., to ensure that 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.

7.4.3 Damage Correlation Issue

Earthquakes may cause multiple equipment failures at the same time. The likelihood of this occurrence 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 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.

7.4.4 Screening of Equipment and Structures

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 seismic plant modeling. 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^{-7}/yr to core damage, then its contribution is considered minimal, and it can be screened out. Since the ACR does not have the seismic hazard, the severe core damage frequency cannot be postulated. Since the safety objective HCLPF is 0.5g for the ACR, a HCLPF capacity of 1.0g is considered to be sufficiently high to screen out the SSCs.

7.4.5 Seismic Event Tree Development

A PSA based SMA 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 HCLPF 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., long term 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.

Two sets of event trees need to be developed. The first set of event trees (seismic initiating event tree) will be used strictly to define the seismic-induced initiating events. As such, the sequences in the seismic initiating event trees will terminate in either a success state, a damage state in which the reactor core has disassembled (SCD), or some seismic-induced initiating events. The essential purpose of the first set of event trees is to determine seismic-induced initiating events. The event order in the seismic initiating 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 second set of event trees is to delineate the plant behaviour on the seismic initiators. The second set of event trees is developed by modifying the internal event trees to reflect the seismic-induced conditions. The headings in the second set of event tree symbolically represent a failure of a system due to the seismic induced failures, random failures or combinations of both.

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 seismic-induced loss of offsite power, it is assumed to be not 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.

7.4.6 Development of Seismic Fault Trees

For the mitigating systems identified from the 2^{nd} set of seismic event trees, seismic fault trees are developed by modifying the internal event fault trees. The seismic-induced failures, which are not considered in the seismic initiating event tree, are added in the respective system fault trees as seismic-induced failures. The failure probability for the seismic events is temporarily set to 0.1 to ensure that the cutsets containing the seismic failures were not filtered out.When the seismic-induced failures are recoverable, the operator actions to recover the failures are also added in the fault trees. If some seismic-induced component failures of interfacing systems affect the functionality of the mitigating systems, the failures should also be included in the system fault trees.

When initial set of fault trees are developed, the pruning of the fault trees can be done. The purpose of the pruning is to reduce the minimal cutsets. The CCF events are in general retained in the system fault trees.

The final seismic fault trees are used for deriving the minimal cutsets of seismic induced core damage sequences by fault tree linking.

7.4.7 Plant HCLPF and Seismic Vulnerabilities

ASQ is undertaken to derive the minimal cutsets for each seismic induced event trees. The minimal cutsets are then reviewed to remove any illogical and duplicated cutsets. From the review of each sequence cutsets, the HCLPF capacity for each seismic-induced accident sequence is determined. This is done using the MIN-MAX method [55]. In this method, the HCLPF value for a cutset is the maximum of the HCLPF values of the seismic failures in the cutset. Cutsets, which contain both seismic failures and non-seismic failures, are called "Mixed Cutsets" in this analysis and are treated separately. "Mixed Cutsets" have both a HCLPF value and an independent probability. The HCLPF for a seismic core damage sequence is the lowest cutset HCLPF among the cutsets comprising the sequence. The plant HCLPF is the lowest sequence HCLPF.

After determining the plant HCLPF, each seismic-induced core damage sequence cutsets are reviewed to identify the plant seismic vulnerabilities. The "Mixed Cutsets" are also reviewed to identify accident scenarios that might have had a lower HCLPF in the presence of a failed component or failure of an operator to take appropriate action. The identified vulnerabilities can be used as an input for design improvements or for development of plant procedures for the seismic events.

7.5 Calculation of HCLPF Values

7.5.1 Overview

The HCLPF values reflect the seismic ground motion corresponding to a 95% confidence of not exceeding a 5% failure probability and is defined by the lognormal distribution using following equation:

$$\text{HCLPF capacity} = A_m \exp [-1.65(\beta_r + \beta_u)].$$

The three parameters in the equation represent: 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. The parameters can be estimated in different ways depending on the methods adopted.

The HCLPF capacity of the SSCs are calculated using one of the followings:

- Fragility Analysis Methods
- CDFM (Conservative Deterministic Failure Margin) Method
- Generic Fragilities

These methods are described in the sections below.

7.5.2 Fragility Analysis Methods

The fragility of a SSC is defined as the conditional probability of failure for a given seismic input motion or response parameter, e.g., peak ground acceleration. The SSC response to the seismic force exerted upon it is normally represented as a curve showing the dependency of the failure probability function on the *peak ground acceleration*. This curve is defined as a *fragility curve*. Figure 7-2 shows a typical fragility curve.

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 SSC, and (*b*) the determination of the seismic capacity. Components may have more than one failure mode, and each mode should be considered in the analysis. Therefore, there may be more than one fragility curve for a particular component, wherever different failure modes are possible.

For equipment, failure denotes the inability of the equipment to perform its safety function. The consequences of failure are also important. By reviewing the equipment design, the failure mode that is most likely to occur as a result of a seismic event is identified. Three types of the SSC failure modes are usually analyzed:

a) anchorage

b) structural

c) functional

For structures, failure usually means the case when it loses its function to support the equipment attached to the structures due to buckling or fracturing. 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.

The fragility method 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-designed dimensions and actual material properties.

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.

7.5.3 CDFM Method

The CDFM method estimates the seismic capacities in terms of HCLPF values based on the following equations:

HCLPF (CDFM) = Seismic Capacities/Seismic Demand at Review Level Earthquake (RLE) * RLE

Seismic capacities are defined as 95% exceedance probability including the non-linear behaviour of the equipment and the seismic demand is based on the 84% exceedance probability estimated for RLE. The general criteria used in the CDFM calculation are as follows:

- Load combination: Normal operating loads + RLE loads.
- Ground Response Spectrum: 84% non-exceedance probability response spectrum.
- Damping: Conservatively estimated median damping value.
- Structural model: Model of Median value + uncertainty variation.
- Soil-structure interaction: Model of Median value + uncertainty variation.
- Material strength: Code specified minimum strength or 95% exceedance actual strength if test data is available.
- Static capacity equation: Code ultimate strength (American Concrete Institiute (ACI)), maximum strength (American Institute of Steel Construction (AISC)), service level D (ASME) or functional limits. If test data are available to demonstrate excessive conservatism of code equations, then use 84% exceedance of test data.
- Inelastic energy absorption: For the case done with the linear analysis, use 80% of computed seismic stress in capacity evaluation to account for ductility benefits for non-brittle failure modes. When non-linear analysis is done, use 95% exceedance ductility levels.
- In-structure spectra generation: Use median damping and use frequency shifting (rather than peak broadening to account for uncertainty).

7.5.4 Generic Fragilities

The ACR is now at a design stage and may not have detailed information for evaluating the HCLPF capacities using the fragility method. As such, generic HCLPF values or CDFM method will be used for the equipment whenever applicable. When generic HCLPF values are not available such as in case of the large equipment in the primary circuit, it will be assumed that the seismically designed equipment has 0.5g HCLPF. The seismic capacities of the equipment will be confirmed when the detailed design is available.

There are several sources for generic HCLPF values. EPRI, in the development of their seismic curves, collected seismic qualification test data from nuclear power plant utilities, test laboratories and vendors. The data included 15 classes of electrical and mechanical equipment. The data was analyzed to develop lower bound spectra called “generic seismic ruggedness

spectra (GERS)". The qualification test data were collected for equipment in US nuclear power plants, and the test response spectra were collected for plants with safe shutdown earthquakes (SSE) ranging from 0.10 to 0.25g PGA (peak ground acceleration). Another source of generic fragilities for components was developed in the Seismic Safety Margin Research Program (SSMRP), NUREG/CR-3558 [38]. 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 [39]. Further information regarding the screening of equipment is available in 'A Methodology for Assessment of Nuclear Power Plant Seismic Margin' EPRI-NP-6041 [40]. The limitations of any databases or sources will be reviewed for applicability to CANDU equipment, when deriving HCLPF values.

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.

7.5.5 Relay Chatter Analysis

It is expected that the ACR will use solid state switching devices and electro-mechanical relays in all safety related electrical and control systems. Solid-state switching devices are known to be inherently immune to the contact chatter. In the ACR, electro-mechanical relays of robust seismic capacity will be selected to preclude the concern for seismic-induced relay chatter. These assumptions about the type of relays will be confirmed during the detailed design stage.

7.6 Reporting Results

The following information should be fully documented for PSA-Based SMA, as discussed in NUREG-1407 [32]:

a) 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.

b) A description of dominant functional and systemic sequences that lead to SCD, including any recovery actions.

c) Any seismically-induced containment failures, and other containment performance insights.

d) A table of component HCLPF values that are used for deriving the HCLPF capacities quantification.

e) A discussion of non-seismic failures and human actions that can be significant contributors, or that have an impact on results.

Table 7-1
Equipment Information

Equipment ID	Equipment Description	Location	Normal Operating Position	Fail Safe Position	Class of Component	Power Supply and Control Power	PSA Basic Event
3432-PV33	Emergency Core Cooling Injection Valves	RB	NC	FO	Pneumatic valve	48V DC to solenoid valve	3432PV33-$VBDDFC

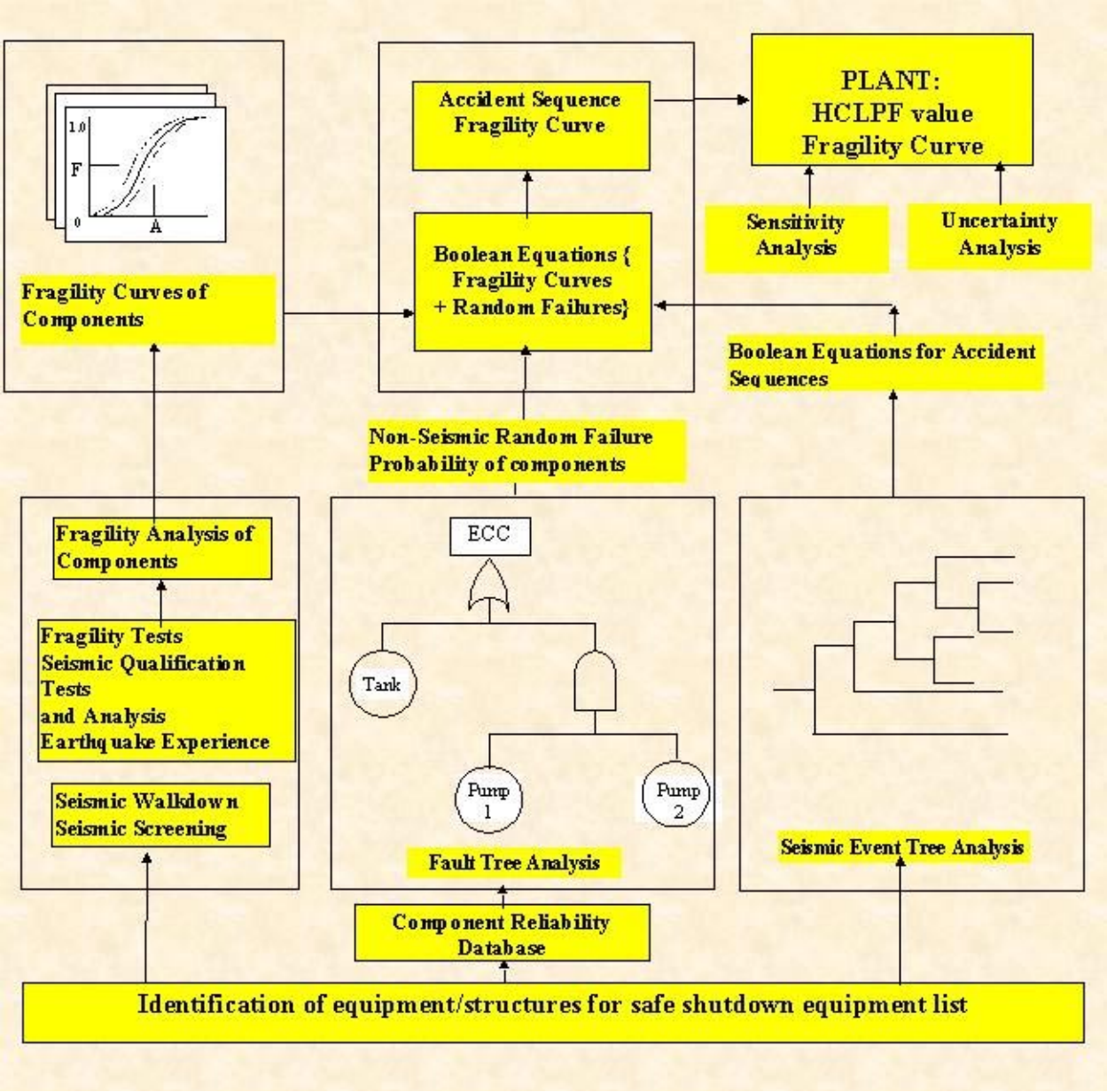
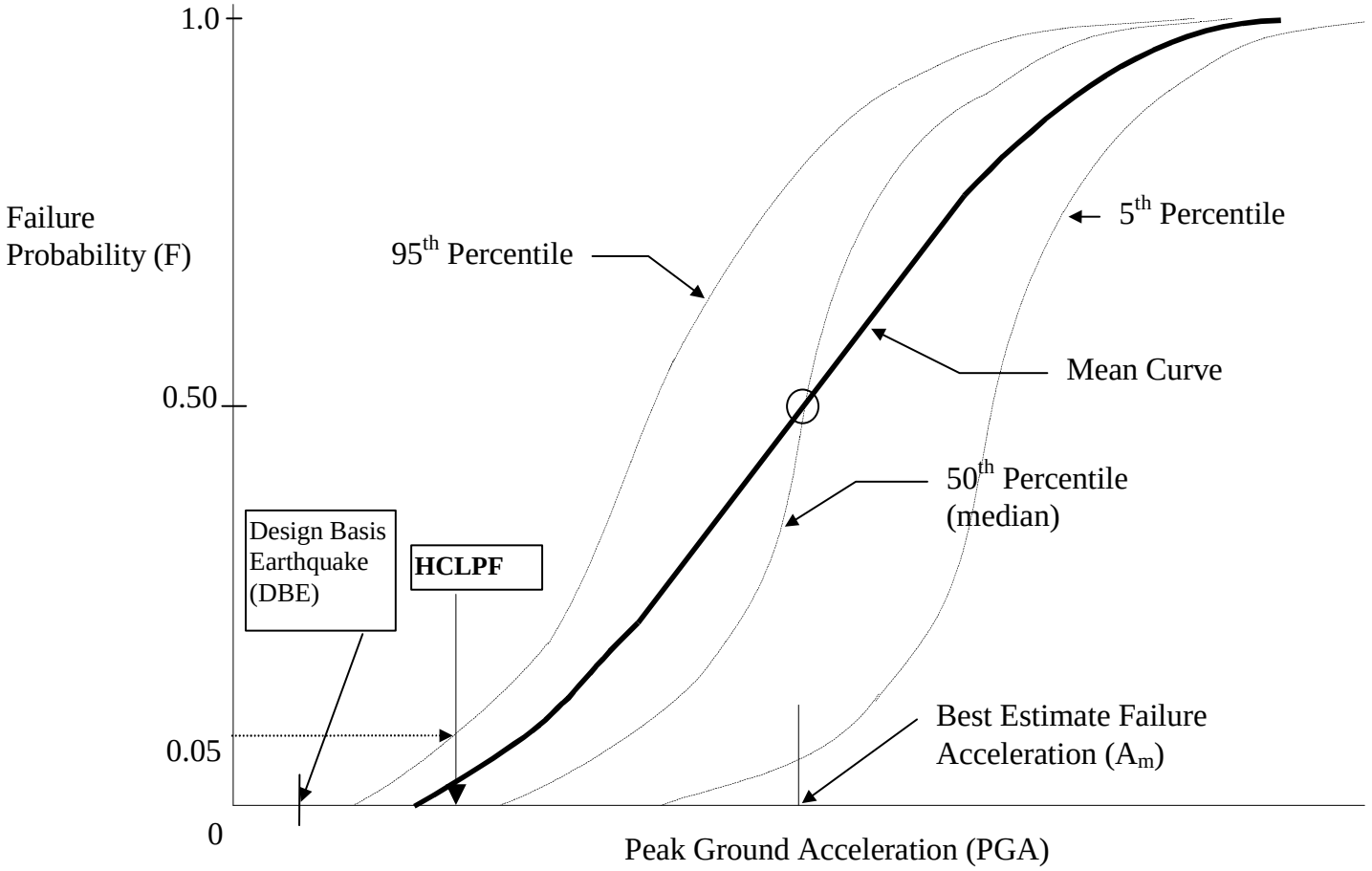


Figure 7-1 Steps of a PSA-Based SMA



HCLPF is the abbreviation for a High Confidence (95%) of a Low Probability of Failure 5%)

Figure 7-2 Typical Fragility Curve

8. FIRE PSA

8.1 Introduction

This analysis describes the PSA methodology for internal fire events in an ACR NPP. Internal fires have been shown to be a significant contributor to risk. Fires may propagate and damage surrounding equipment. The result may impact safety related systems 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 for internal fire events starts with the identification of the basic cause of the event, and then examines historical or physical data to establish the sources and frequency of the 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 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 43).

Wherever detailed information is not available assumptions will be made. The assumptions such as cables and control procedures will be documented for each fire zone, and will be traced during the design, and confirmed as one of the Combined License (COL) action items.

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 the 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.

This methodology is applicable for full fire PSA when all the information is available. For Fire PSA done for the Design Certification stage, the fire walk down cannot be performed and assumptions will be made with respect to layout, wiring and other details to derive fire-induced SCDF. The assumptions will be confirmed during the detailed design for the ACR.

8.1.2 Procedures for Fire PSA

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 initiation of a fire in an area and progression 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 consequences depend on a number of parameters, such as:

- the number and location of fire ignition 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.

The fire PSA for the ACR will use the successive screening approach to identify potential safety significant fire areas. For the areas remaining after the screening process, detailed analyses for the areas will be performed. The major steps included in the ACR fire PSA are as follows:

1. Divide plant into fire areas and fire zones
2. Perform qualitative screening analysis
3. Perform quantitative screening analysis
4. Perform detailed analysis.

The following sections describe the approach of ACR fire PSA in general terms, and identify the basic assumptions that are incorporated in the methodology and its application to a plant assessment.

8.2 Definition of Fire Area and Fire Zone

A fire area is defined as that portion of a building or plant that is separated from other areas by fire barriers with a fire resisting rate of 3 hours or more, including components of construction such as beams, joists, columns, penetration seals or closures, fire doors, and fire dampers. Fire barriers would withstand the fire hazards inside the fire barriers and protect equipment in a fire area from the fire outside of the fire area.

Fire zones are subdivisions of a fire area and are typically based on fire hazards analyses that demonstrate that the fire protection systems and features within the fire zone provide an appropriate level of protection for the associated hazards. Fire zones are well-defined areas where heat and combustion product such as smoke can be reasonably confined. The fire zone need not be enclosed by fire barriers.

The fire PSA for ACR would in general adopt the division of fire areas and fire zones defined in the fire hazard analysis. For the purpose of analysis, several fire areas may be integrated into a fire area. For example, a certain building which includes several fire areas or fire zones but does not have any safety related equipment, can be integrated into a single fire area. This would make the screening process easier. Also the fire zones consisting of several compartments may be divided into several fire compartments for detailed analysis.

8.3 Qualitative Screening Analysis

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. To perform the qualitative screening analysis, it is required to determine the equipment that should be included in the fire PSA. The equipment list will be developed based on the internal events PSA models including the containment systems. In principle, all the equipment included in the internal events PSA models will be included in the list. The equipment list will also include the equipment that can affect the PSA-credited function if actuated spuriously due to the hot-short mode of failure due to fires.

Once the equipment list is determined, the equipment of the list located in each fire zone will be identified. As necessary the locations of cables will be determined from the design details or assigned using judgement and assumptions based on the following:

- Safety Design Guide for Separation
- Design guide for cable routing
- Major plan for cable tray routing
- Fire hazard analysis reports
- Location of equipment

- Discussions with design engineers

The next step of the qualitative screening analysis is to identify the potential fire propagation pathways. During the qualitative screening analysis, fire propagation across adjacent fire area/fire zones will be assumed to occur except for the following cases:

- There are automatic fire suppression systems both in the exposing and the exposed fire areas/fire zones.
- The fire areas are enclosed with at least 3-hr fire barriers with combustible loading less than 20,000 Btu/ft^2.
- The fire propagation across the containment penetrations.

When all PSA-credited equipment and related cables are located and the potential fire propagation pathways are identified, the qualitative screening analysis will be performed. The screening will be performed at a fire area level first and then at a fire zone level. The criteria for qualitative screening of fire areas and/or fire zones are as follows:

- A fire in the fire area/fire zone does not cause initiating events other than a plant trip, and
- The fire area/fire zone does not have any PSA-credited equipment, and
- The fire in a fire area/fire zone does not propagate to other fire areas/fire zones that have any PSA-credited equipment.

The fire area/fire zone that can cause plant trip due to the fire will be screened out since the Conditional Core Damage Probability (CCDP) without any damage of PSA-credited equipment with the plant trip is quite low (of the order of 1.0E-7 or lower).

8.4 Quantitative Screening Analysis

For the fire zones remaining after qualitative screening analysis, quantitative screening analysis will be performed as described in the following subsections.

8.4.1 Calculation of Fire Initiating Events Frequencies

The first step of the quantitative screening analysis is to estimate the fire initiating event frequency for each fire zone. To estimate the fire frequency, the ignition sources in each fire zone should be identified. For the fixed ignition sources, it is expected that the fire hazard analysis would include all required information. For the transient ignition sources, it will be assumed that the plant procedure for the existing CANDU 6 plants would be applicable to the ACR. The major assumptions that will be applied in the ACR fire PSA are as follows:

- The hot work such as welding and cutting job will not be performed in the area of safety. If the work is necessary for the plant operation, the work will be done only when a qualified firewatcher is also present.
- The unattended transient materials will not be stored in the area of safety.

- When the transient materials are stored in a non-safety area, it will be stored in non-combustible cabinets with the limitations of the quantity.

The fire ignition frequency will be estimated using the CANDU fire database. The CANDU fire database has been developed in the Reference 54. The fire database is developed based on the fire experiences in the CANDU and US LWR power plants. The total fire experiences collected are 303 fire events during the 1481 combined operating years. The resulting fire frequency for each ignition category are presented in the Table 8-1. As shown in the table, the fire frequency per CANDU plant-year is estimated as 2.43E-1/year.

The composite fire frequency for the fire zone i, λ_i, is given by the following expression:

$$\lambda_i = \Sigma\, w_{i,j}\, \lambda_j + \lambda_h\, w_h$$

where $w_{i,j}$ = weighting (apportionment) factor for source-based categories of fire event source j (Categories 1-3, 5-22) 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), 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. The values for $N_{i,j}$, NT_j and the amount of cable insulation are determined from the information of the fire hazard analysis.

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 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 the ACR fire PSA, the first method for calculating w_h will be used.

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, regardless of their cause (equipment failure, human error, etc.).

For the ACR plants, it is expected that the cables installed would be fire retardant cables, which satisfies the IEEE-383 criteria. So it will be assumed that self-ignited cable fires do not occur in the ACR.

When the composite fire frequency for a fire zone is estimated to be less than 1.0E-7/yr, the fire zone can be screened out from further analysis.

The assumptions about the cables and other control procedures will be documented for each fire zone, will be traced during the design, and will be confirmed as one of the COL action items.

8.4.2 Identification of Fire Induced Initiating Events

Using the information existing in the fire zone, the potential fire-induced initiating events are determined assuming that all equipment and cables are damaged due to the fires. Where the spurious operation due to a fire is a concern, the potential initiating events due to the spurious operations such as the loss of inventory of primary systems will be considered. If the damage of all the equipment/cables would cause loss of supporting systems, the loss of supporting systems will be selected as one of the potential fire-induced initiating events. Among the potential initiating events, the worst initiating event will be determined as a fire-induced initiating event. If there will be no specific initiating events directly caused by the fire, the general transient will be considered as the fire-induced initiating event for the fire zone.

8.4.3 Quantification of Fire-Induced SCDF

By modifying the internal event PSA models to reflect the fire-induced conditions, the fire-induced SCDF due to the fires in a fire zone will be estimated. The quantification will be performed based on following:

a) The frequency of fire initiation is the composite frequency for all categories of fire event sources that are present in the room. The fire-induced initiating event is the worst one among all potential initiating events as determined above.

b) 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.

c) 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 loading of the zone. When the fire loading is higher than the ratings, the fire propagation is assumed to occur as a

probability 1.0. Otherwise, following generic barrier failure probability based on Reference [50] is used.

Barrier Type	Barrier Failure Probability/Demand
Fire Door	7.40E-3
Fire and Ventilation Dampers	2.70E-3
Penetration Seals	1.20E-3

Multiplying the number of barrier types by the corresponding failure probability and summing the contributions from the different types provides the barrier failure probability. When the specific number of barrier type is not available for the ACR design, the barrier failure probability will be assumed to be 0.1.

d) The automatic fire suppression system is assumed to operate, with the following generic failure probabilities. The probability is widely used in the US IPEEE such as Calvert Cliffs Nuclear Power Plant [47].

System Type	Unavailability of System
Wet Pipe Sprinkler	2.0E-2
Preaction Sprinkler	5.0E-2
Deluge Sprinkler	5.0E-2
CO_2	4.0E-2
Halon	5.0E-2

e) Manual fire suppression is not credited.

f) 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.

g) When spurious actuation of the equipment is a concern, the probability of hot short due to the fires is assumed to be 0.1.

h) When modifying the internal events model, the human error probability for post-accident actions is considered to be 5 times higher than that used in the internal events model, considering the potential stress due to the fire-induced environment.

i) The recovery actions included in the internal events models are considered not to be feasible in this screening analysis.

8.4.4 Quantitative Screening Criteria

The SCDF estimated for each fire zone is compared with the screening value. The fire zone resulting in the SCDF lower than the screening value will be screened out for further analysis. The screening SCDF applied for the ACR fire PSA will be 1.0E-7/yr.

8.5 Detailed Analysis

For the fire zones remaining after quantitative screening analysis, detailed analysis will be performed as described in the following subsections. The following constitute the steps in a detailed analysis:

- Develop fire scenarios taking into account various refinements, such as
    - Assign fire frequency for each ignition source in the fire zone
    - More realistic modelling of fire growth and propagation,
    - Credit for manual fire detection and suppression, and
- Calculate SCDFs for fire scenarios that require detailed analysis taking into account following:
    - Realistic treatment of fire-induced initiating events
    - Realistic estimation of HEP
    - Consideration of recovery actions
- Calculate the summed SCDF for fire, by adding the fire risk contribution for all zones from detailed analysis.

8.5.1 Detailed Fire Scenario Development

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 characterizes these sources is also considered.

b) The fire experience shows that a significant fraction of fires are extinguished without intervention of manual or automatic fire suppression activities. Thus the severity factor, which is fraction of fires that can be fully developed if not suppressed, will be assigned for each ignition fire sources. The generic severity factor, if applicable, will be used with the consideration of layout of the ignition sources and around combustibles. If generic severity factor is not available or cannot be applicable to the ACR, the severity factor will be determined through review of the fire database used for deriving the fire frequency.

c) Fire growth modeling is performed using the COMPBRN IIIe. COMPBRN IIIe requires inputs for the specific layout of the fire zones, characterization of ignition fuel source and other combustibles, damage criteria for the target equipment. Those will be determined during the analysis through the discussions with design engineers, review of other CANDU plants layout similar to the fire zone considered, review of generic information sources such as US LWR fire IPEEE reports and NUREG reports, etc.

d) 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 presented above is used.

e) Both 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 presented above 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. For the hot-work induced fire in the safety related areas, the fire suppression by a firewatcher is credited. The failure probability of fire suppression by a firewatcher is assumed to be 0.05 (same as automatic sprinkler system). The dependencies between the fire detection and fire suppression, between the automatic fire suppression system and manual fire suppression, between the fire suppression systems and other supporting systems will be considered explicitly.

f) Some equipment is vulnerable to the fire suppressants. The effects of fire suppression on the equipment in the fire zone are considered explicitly.

g) The direct effects of smoke and toxic gases generated by fires on the equipment are not considered. It will be assumed that those fire-generated products do not impact the function of the equipment directly during the time considered in the fire PSA. However, the impacts of smokes and toxic gases on manual fire suppression activities and the operator actions will be considered.

8.5.2 Fire Growth Modelling

The fire growth modelling will be performed to calculate 1) whether or not fire spread occurs, 2) whether or not damage is possible, 3) which targets (cables and equipment) may sustain damage, and 4) the length of time between fire ignition and damage using COMPBRN IIIe [52]. COMPBRN IIIe was developed at UCLA, and is currently maintained by EPRI and the USNRC.

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, if the fire is not suppressed within the time.

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.

8.5.3 Plant Response on the Fire Induced Events

For each fire scenario developed, the response of the plant is analyzed using PSA methodology. This involves:

- the identification of the PSA IE and the corresponding appropriate event tree,
- the modification of event trees to reflect the fire induced conditions, and
- the modification of fault trees to reflect the fire induced conditions

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) Modification of the internal events event trees: For the PSA IE determined in the previous step, the event trees that are built for internal events PSA are reviewed for applicability to the particular fire scenario and if needed are modified accordingly. For example, fire-induced loss of Class IV cannot be recovered in the same way as that considered in the internal events analysis and the recovery actions considered in the accident sequences should be modified accordingly.

   When there are no appropriate event trees that reflect the fire-induced conditions, new event trees may need to be developed. For example, complete loss of a supporting system may not be included in the internal event trees due to the low probability or other causes. But the fires in a certain area may cause complete loss of supporting systems and the response of the plant to the event can be quite different from that of plant trip. Also the MCR evacuation due to the fires may not be handled using the internal event trees.

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 included as a house event and set to true. Although some components may be damaged by fire, their fail-safe characteristic may still be credited.

d) Modeling of spurious actuation due to the fire: For the equipment that the spurious actuation is a concern, the probability of spurious actuation due to fires is estimated and the failure mode is included in the fault tree models. The probability of hot-short given fire-induced damage of cables are not clearly identified. In the ACR fire PSA, the generic probability of

0.068 presented in the Reference 16 will be used regardless of cable types. A recent study [17] showed that the likelihood of conductor-to-conductor hot short failure mode is quite dependent on the cable type and that the probability in case of multi-conductor armoured cables is 0.05. But the study also indicated that the probability could be as high as 0.8 in case of general multi-conduct cables without armour, shields, or drain wires. The multi-conduct cables of the ACR are expected to have ground shields, and thus the probability used here is judged to be reasonable. But for the significant fire scenarios that involve hot-short failure modes, some sensitivity study will be performed using different hot-short probability.

e) Estimation of Human Error Reliability. There can be three types of operator actions that need to be considered in the fire PSA as follows:

- The fire-induced conditions may prohibit or delay operator 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.
- The fire-induced conditions may require unique operator actions that are not considered in the internal event trees. The HEP for those actions will be estimated using the methodology described in the Section 6.
- The same operator actions considered in the internal events are applicable to fire-induced accident scenarios. The HEP 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.

8.6 Sensitivity Analysis

The sensitivity analysis will be performed for the major factors that are judged to be important to the resulting SCDF. The sensitivity analysis will includes followings:

- Fire ignition frequencies.
- Severity factors.
- Probability of hot-short failure mode given damage of cables.
- Fire Propagation Probability.
- Manual fire suppression probability.
- Human error probability: To identify the effects of operator actions on the fire-induced SCDF, the sensitivity analysis will be performed assuming that the HEP under fire-induced conditions are the same as those considered in the internal events. Also a sensitivity analysis is performed assuming that the recovery actions under fire-induced conditions are not feasible.

Table 8-1
Fire Frequencies for Ignition Source Categories

No	Category Name	Mean Freq. (/Op-year)	Components
1	Battery	1.30E-03	
2	Battery charger	2.32E-03	
3	Inverters	1.00E-03	
4	MCR	3.03E-03	Panels and cabinets in the control room
5	DCC computer	4.01E-03	
6	Diesel generator sets	2.19E-02	
7	HVAC equipment	3.24E-03	Heaters, fans, chillers, filters, air compressors
8	Dryers	5.70E-03	D_2O recovery dryers
9	Hydrogen fires	7.46E-03	Hydrogen vessels (excluding turbine -generator hydrogen fires)
10	Logic and protection cabinets	1.85E-02	Relays, fuses, panels, switches
11	HTS pumps	3.88E-03	
12	Pumps	1.17E-02	Motor pumps and diesel driven pumps
13	Motor control center	6.41E-03	
14	Motors	1.07E-02	MOV, strainer motor, starter motors
15	Motor generator sets	1.34E-03	
16	Power and control cables	1.22E-02	Cables, junction boxes
17	Low voltage switchgear	7.23E-03	Low voltage equipment (480 V or less)
18	High voltage switchgear	1.19E-02	High voltage equipment (above 480 V)
19	Gas Turbine Generators	1.11E-02	
20	Turbine-generator	2.52E-02	T/G exciter, oil, hydrogen
21	Main unit transformer	1.13E-02	
22	Transformers	1.21E-02	Transformers of all voltages
23	Transient fires	1.88E-02	Human error, transient fuel location
24	Cable fires caused by welding and cutting	1.66E-03	
25	Transient fires caused by welding and cutting	2.92E-02	

9. Flood PSA

9.1 Introduction

This analysis describes the PSA methodology for flood in an ACR NPP. The analysis describes the method for assessing the consequences of reactor accidents involving internal floods only.

This section provides the specific methodology for internal flood, and is used in conjunction with the generic methodology for the Level I PSA described in Section 4. The results of the Level I PSA, including internal and external events, are provided as input to the Level II PSA.

9.2 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 potentially 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.

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 subsequent 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 excluded as described in Section 7.1.

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) The detailed analysis of the potentially significant flooding sources and scenarios that are identified in the screening analysis. Local operator recovery actions are also credited.

9.3 General Approach for Flooding Event Analysis

Internal flooding requires consideration as a potentially significant risk contributor because it 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 successive 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 already treats some flooding events and their effects such as LOCAs from the primary circuit and feedwater line breaks. Therefore, these events are not part of the flood analysis.

c) Temporary hose/piping connections can be excluded from the analysis as flood sources, since they are used temporarily and relatively infrequently. Most of the activities using those are accompanied with the plant personnel so that when a leak or break develops, it can be isolated immediately.

d) Floods are treated as IEs and not as events that are subsequent to another initiator.

e) Spurious activation of sprinkler systems is considered.

f) Areas surrounded by walls without penetrations 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.

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.

9.4 Qualitative Screening Analysis

9.4.1 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 reactor auxiliary building, the turbine building, the reactor building, main control building, secondary control 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.).

A smaller flooding area can be defined by using 1) the presence of physical barriers (e.g., walls, floors, dikes), 2) mitigation features (e.g., sumps, drains), and 3) propagation pathways (e.g., open hatches or doors).

In ACR 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.

9.4.2 Identification of Flooding Sources

In this step, the major flooding sources in each flooding area, 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. The major flooding sources in each flooding area are the pipes connected to the tanks and the systems.

The flooding sources in each flooding area are the pipes connected to those systems and thus the piping routing is required. The location of pipes will be assigned using judgement and assumptions based on the followings if no piping information is available:

- Safety Design Guide for Separation
- Design guide for piping routing
- Plan for major piping
- Design flooding analysis
- Location of equipment

- Pipe routing information from other CANDU plants
- Discussions with design engineers

The assumptions about piping routing will be documented for input to the piping design and traced during the detailed design process.

9.4.3 Identification of Equipment in Each Flooding Area

For the determination of 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.

The system/equipment used for the accident mitigation can be identified from the review of internal events models and systematic review of plant design. However, the electrical and control cabinets, instrument racks and junction boxes are not explicitly included in the internal events models. These will be modelled as necessary in the flood models.

The assumptions made will be documented and confirmed during the detailed design phase.

9.4.4 Initial Qualitative Screening of Flooding 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.

The flood areas are screened out if:

- The flood area does not contain any susceptible equipment for safe shutdown and they do not contain any equipment that, if damaged, would lead to an IE except the plant trip.
- Flooding sources that do not have enough capacity to damage the equipment that is required for safe shutdown and/or to lead to an IE.

The flood-induced reactor trip without damage of PSA-credited equipment can be screened out since the CCDP is judged to be quite low (1.0E-7 or lower).

9.4.5 Refined Qualitative Screening of Flooding Areas

For the flooding areas that are not screened out above, more detailed screening analysis will be performed as described below:

- Determine the critical height of the equipment which if damaged can affect the function of safety systems or lead to the IE. It may be assumed that the critical height is less than 6 inches if the equipment is installed without any elevation.
- Determine the maximum flood height that the flood can cause in the flooding area assuming a conservative maximum flood flow rate and consideration of flood mitigation system (drains and sump pumps) and other flow paths out of the flood area. During the evaluation the potential maximum flow rates and volumes are assumed for all flood sources. For example, a double-ended guillotine break for the pipes and catastrophic failures for the tanks, pumps, and valves will be assumed When the conservative maximum flood flow rate is less than the capacity of flood mitigation systems and out flow path, a maximum flood height of 6 inches will be assumed.
- Determine other effects of flooding than the submergence on the equipment of concern. The equipment can be damaged due to the spraying, splashing, or dripping from pipe above. It will be assumed that the electrical equipment excluding cable insulations would be damaged if water contacts with it. When motors of pumps or valves are designed to protect from the water intrusion such as sealing or covering, the equipment will not be considered to be susceptible to those effects. The requirements on the equipment qualification may provide inputs for the determination.
- Determine the potential flood propagation pathways surrounding the flooding zone. The louvers, gap under the doors, and stairwells will be considered as potential propagation pathways.
- Screen out the flood areas if
    - the maximum flood height is less than the critical height for all equipment of concern,
    - the equipment is not affected by spraying, splashing or dripping, and
    - the propagation of flooding does not affect the equipment of concern in propagated flooding area.

The screening is expected to efficiently screen out open flood areas that do not have flood barriers and do not have equipment adjacent to the flood sources.

9.5 Quantitative Screening Analysis

9.5.1 Evaluation of Flood Frequencies

For the flood area remaining after qualitative screening analysis, the flood frequency for all flooding sources are estimated. The potential flood sources are the pipes.

For the screening analysis, the flooding frequency of each flooding zone will be assumed to be 0.01 except for the turbine building. The flooding frequency of turbine building is assumed to be 0.1. From comparison with the flooding frequency estimated for other CANDU plants and LWR plants, this frequency is judged to be sufficiently high enough and is considered to be bounding.

9.5.2 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.

9.5.3 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 $P_{bf} = 1.3\times10^{-4}$
- 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). However, there is a potential of significant loading due to the flooding, and the bounding calculation may need to be done to show that the walls are rugged enough to withstand the flooding induced loads.

9.5.4 Initial Quantitative Screening

The screening analysis is based on the conservative assumption that the equipment in the flooding area that the flooding originates from and the flooding area where the flooding is propagated to, is damaged due to flooding. By modifying the relevant fault tree/event tree models, a CCDP for the case is calculated. The SCDF is calculated by multiplying the flood frequency by the CCDP.

If the sum of the SCDF due to the flooding in a specific flooding area is less than 10^{-7} events/year (the SCDF is negligible, compared with the internal IE caused by the flood), then the flood areas will 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 conservative enough to retain significant flooding scenarios. It is expected that in the detailed analysis, the order of magnitude of these specific sequences will be further reduced, due to the use of more realistic value and therefore they will not be dominant contributors to the SCDF.

9.5.5 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 9.5.3).
- 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.

The results of the screening analysis are compared with the screening criterion (severe core damage frequency less than 10^{-7}/yr) to identify a final list of flood areas that require further detailed analysis.

9.6 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 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.

9.6.1 Flood Frequency Estimation

The major sources of flooding are pipes and its accessories. The pipe failure frequency presented in the WASH-1400 [24] will be used for the ACR flooding PSA.

The WASH-1400 [24] presented the pipe failure 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 discontinuities, such as valves, pumps, elbows, tees, etc., up to 10 ft in length. WASH-1400 frequency is a composite frequency that accounts for large, medium and small break sizes.

One of the major causes of flooding is the rupture of expansion joints in high flow-rate piping. The failure frequency is 2.5×10^{-4} events/yr, based on the frequencies presented in the Oconee PRA [22], will be used in the ACR flooding PSA.

The frequency of ruptures of tanks is 2.3×10^{-4} events/year and is equivalent to those presented in the Reference [23]. The reference 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.

The assumptions made will be documented and confirmed during the detailed design stage.

9.6.2 Flood Flow Rate

In the case of a flooding event, the operators can isolate the flooding before it can affect the equipment of safety functions. The estimation of available time for operators to isolate the flood 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.

9.6.3 Categorization of Flood

The flood frequency and flood flow rate are estimated as per the above sections. 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 Oconee PRA [22] proposed to categorize 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 will be used in the ACR flooding PSA.

9.6.4 Development 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 growth and propagation, and the time that is available for the operator to isolate the flood.

The growth of the flood level is determined by taking into account the flooding flow rate, the free cross-sectional area available for flooding times flooding height that can damage the equipment of concern (floodable volume), 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 is 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. 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 floodable volume by the flow rate. The human error probability for those actions will be estimated as per Section 6 of this document.

To get the floodable volume, the critical height for each component of concern should be determined. The critical height of the component would be determined by the designers based on the design flooding calculation. Then the floodable volume would be obtained by multiplying the floor area by critical height. Each safety equipment may have different floodable volume.

The safety equipment can be also damaged by spray or splash. Thus when developing the flood scenarios, the equipment damage due to the spray or splash due to high or medium energy line breaks and spurious actuation of fire suppression system should be considered. The equipment susceptible to the spray or splash adjacent to the pipe would be considered to be damaged first before submergence occurs.

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.

9.6.5 Quantification of Severe Core Damage Frequency

This step evaluates the severe core damage frequency for different flooding sequences. For each flood scenario, the flood frequency, the probabilities of operator error in terminating the flood, the flood propagation probability (flood barrier failure probability) are evaluated. Each flood scenario would define the resulting damage states, e.g., flooding-induced IE and the safety equipment damaged due to flooding and the frequency of the scenario. Modifying the internal event trees and fault trees reflecting the damage states the CCDP will be estimated. Then the severe core damage frequency would be obtained by multiplying the flood scenario frequency by the CCDP.

9.7 Sensitivity Analysis

The sensitivity analysis will be performed for the major factors that are judged to be important to the resulting SCDF. The sensitivity analysis will includes the following:

- The number of piping segments and the resulting flooding frequencies.
- Categorization of the flooding.
- Flooding propagation probability.
- Manual flooding isolation or suppression probability.
- Operator error probability to mitigate flood induced events.

10. UNCERTAINTY AND SENSITIVITY ANALYSIS

10.1 Uncertainty Analysis

10.1.1 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.

10.1.2 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.

10.1.3 Treatment of Uncertainty

10.1.3.1 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. However,

wherever possible best estimate information will be used. Sensitivity cases of key assumptions will also be performed.

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.

10.1.3.2 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.

10.1.3.3 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.

10.1.3.4 Approach to Uncertainty Quantification

The performance of uncertainty analysis is based on DS&S's UNCERT program [41]. 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 result 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.

10.1.4 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 provides for a 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).

10.2 Sensitivity Analysis

10.2.1 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 improvement of operations, if practical, on those systems that are especially large contributors to risk for Level I and Level II PSA.

10.2.2 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.

10.2.2.1 Items Covered in the Sensitivity Analysis

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. When ASQ is completed, importance analysis is performed. Based on the result of the importance analysis, items that are considered important will be selected for the sensitivity analysis. Sensitivity on key assumptions are based on importance measures.

11. LEVEL II PSA

11.1 Overview

The objective of Level II PSA is to confirm that the summed Severed Core Damage Frequency (SCDF) is ≤ 1E-5 per year and the Large Release Frequency (LRF) is ≤ 1E-6 [4]. A secondary objective is to enumerate the effect of certain design options on the SCDF and the LRF. Both probabilistic and deterministic analyses are required as illustrated in Figure 11-1.

The following tasks are involved:

1. "Large Release" (LR) will be defined. The source terms outside the containment will be compared against this criterion task 7 (see Section 11.2).
2. Accidents will be grouped into categories of similar potential for airborne radioactivity content within the plant and similar containment integrity challenges. These groups are called the Core Damage States (CDS's; see Section 11.3). They are guided by Plant Damage States (PDS's) evaluated for Level I PSA (Section 4.9).
3. CDS frequencies will be enumerated and summed (Section 11.4).
4. Characteristics and probabilities of open paths between the airborne radioactivity in the plant and the outside environment will be enumerated. Open paths are caused by Containment Events (CE's), which will be categorized and documented in the Containment Event Tree (CET) (Section 11.5).
5. Deterministic analyses will enumerate the radioactivity source terms outside the containment for all combinations of CDSs and CE's (Section 11.6).
6. A profile of source terms as a function of accident frequency will be derived. The source terms from task 5 and frequencies from tasks 3 and 4 will be used to develop this profile.
7. The source terms will be screened out against the LR criterion from task 1 and the LRF will be enumerated.

11.2 Large Release

The "Large Release" (LR) is used as a surrogate for public fatalities.

This criterion is to be developed which should be consistent with the current Canadian practice and EPRI guidelines, for example: the limits on Cesium.

All nuclear power plants and surrounding governments have emergency plans, which alter the population distribution around the plant (e.g., an evacuation of the population) as well as the public exposure conditions (e.g., a sheltering, thyroid blocking, etc.).

The LR is equivalent to Large Early Release (LER) defined by US NRC as "significant, unmitigated releases from containment in a time frame prior to effective evacuation of the close-in population such that there is a potential for early health effects" [44].

A rationale will be required as to what constitutes the LR, which needs to be available by the time the source terms are quantified by the deterministic analyses. This is a generic definition (i.e., the consequences of radioactivity release into the environment are not reactor specific). Therefore, the literature review supplemented by expert advice from health physics experts will be adequate for this task.

As per the Licensing Basis Document [4] the seismic events are excluded for large release frequencies.

11.3 Core Damage States

The core damage states are initially chosen by expert judgement to represent reactor and containment conditions with broadly similar radioactivity release from the fuel, fuel coolability conditions and containment integrity challenges. The initial choices are listed in Figure 11-1.

Core Damage State 1 is intended to cover "Design Basis" and most "Limited Core Damage" accidents. All these accidents have limited releases from the fuel, all are directly cooled by HTS or ECC coolant (which is in turn cooled by reliable heat sinks) and there are no strong containment integrity challenges. All of them are expected to produce source terms to environment well below the LR criterion from Section 11.2. Few (if any) longer-term interventions would be required to maintain the quasi-steady CDS1 state.

Core Damage State 2 covers the remaining "Limited Core Damage" accidents. These do not have the direct fuel cooling, so the release from the fuel is considerable and some flammable gases are produced to pose a potential containment integrity challenge. These accidents could potentially reach the LR criterion if the containment function is unavailable (e.g., a bypass, or some containment opening). Again, few (if any) longer-term interventions would be required to maintain the quasi-steady CDS2 state.

Core Damage State 3 covers the "Severe Core Damage" accidents that are arrested in process-systems vessels. These accidents involve significant core geometry changes (corium debris is formed), significant radioactivity releases from the fuel and moderate containment integrity challenges (hydrogen production and steam surges due to debris relocation). These accidents have a potential of reaching the LR criterion if the containment function is unavailable and could challenge the containment integrity in the longer term (depending on the timing of core disassembly). Some long-term interventions may be required to maintain the quasi-steady CDS3 state.

Core Damage State 4 covers the "Severe Core Damage" accidents that are not arrested in process-systems vessels. These accidents have all characteristics of CDS3 accidents plus a potential for corium-concrete interactions with its attendant additional radioactivity releases and containment integrity challenges due to non-condensable gas generation. These accidents would likely reach the LR criterion if the ex-vessel interactions commence and the containment is not sealed (i.e., a path to the environment exists).

For CDS1 and CDS2 categories, deterministic analyses of reactor response will be available for individual sequences from conventional design-assist and safety analyses. For CDS3 and CDS4, few accident sequences will be selected that bring the reactor into the CDS at the earliest time while producing the largest fission product release and/or the largest containment integrity challenge. Scoping analyses will be required to select the representative accident sequences for source term analyses.

Because only the worst sequences are selected to represent each severe accident category, a further subdivision may be needed for CDS3 and CDS4 to separate the severe accidents with "early" source terms from those with "late" source terms. This subdivision would only involve the combinations of CDS's and CE's that produce the LR. A decision on the subdivision can only be made when the source terms are available.

Typically, a CDS is not overly sensitive to the state of the containment boundary (This means that there is little or no feedback of the containment conditions on the conditions in the damaged reactor). Therefore, the CDS can be defined independently of the CE's discussed in Section 11.5.

11.4 Frequencies of Core Damage States

Probabilistic analyses define the frequencies of various automatic plant responses to internal and external initiators. These responses are grouped into broader accident sequence categories called the Plant Damage States (PDS's), which essentially define the starting conditions for the long-term accident progression (Section 4.9 defines the PDS categories for the internal and external accident initiators) (i.e., for the CDS's).

PDS0's are screened out based on low frequency. PDS5 to PDS10 are addressed under the scope of normal deterministic analysis.

In all accidents (i.e., for each PDS), manual interventions are eventually required to maintain and/or establish a steady state of the plant. Combinations of the PDS's and the long-term interventions define which PDS ends up in which CDS's. Probabilistic analyses of the longer-term interventions, based on the accident-mitigation design features of the ACR, are required in addition to enumerating the PDS frequencies.

11.5 Containment Events

The containment events impact significantly on the source terms into the environment. The Containment Event Tree (CET) defines these events. The CET top events are generally containment performance- (success/failure) oriented, reflecting performance issues that affect the source term to the environment.

The CET will include the analysis of the following ACR containment systems:

a) Local air coolers

b) Airlocks

c) Containment isolation system

d) Passive Autocatalytic hydrogen recombiners.

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.

Critical events with respect to source terms are the containment boundary failures. A special case is a containment bypass, which is a containment boundary failure brought about by the accident-initiating events. The containment bypass events are embedded within the PDS definitions and the resulting source terms are typically insensitive to the other containment events (A major release path to environment exists from the onset of the accident and any subsequent release path(s) due to other CE's have a second-order impact on the source term). Therefore, the bypass events are treated separately from the events defined by the CET (Figure 11-1).

The bypass events include:

- steam generator tube rupture,
- rupture of bleed cooler into the RCW system, and,
- interfacing LOCA ("V" scenario).

A complete list of the bypass events that are relevant to the ACR will be developed and the characteristics of the bypass flow paths will be enumerated.

A problematic containment event is a consequential containment boundary failure, which is phenomenological in nature. This containment event will be handled by the failure criteria employed in the deterministic analyses of SCD accident progression. The intent is to use the simplest criterion (i.e., a failure pressure).

11.6 Source Term Estimates

As illustrated in Figure 11-1, no analyses specifically performed for the Level II PSA are anticipated for CDS1 category. Existing analyses (perhaps supplemented by few calculations using GOTHIC [59] and SMART [14] computer codes for the release via the impaired containment, or SOPHAEROS computer code [51] for transport within the HTS will be sufficient to demonstrate that the LR is avoided for all Design Basis Events and Limited Core Damage Accidents in this group. The reference analysis tool for CDS2 through CDS4 accident groups is MAAP 4 CANDU computer code [63]. This code has all models required to enumerate the source terms into the environment as well as models to assess component and containment integrity challenges (If warranted, supplementary analyses can be performed for particular phenomenology aspects (e.g., fission product retention in a bypass flow path, detailed hydrogen distribution and burn in a volume, etc.) using specialized models). Once the

ACR-relevant failure criteria are developed (Failure criteria need to be developed for all process system boundaries (i.e., fuel channel, calandria and shield tank) as well as the containment (see Section 11.5). This is a major effort, which requires design details that may not be readily available. In terms of elapsed time when the deterministic analyses can commence, the development of failure criteria may well be the dominant constraint) and a given CDS sequence is simulated (as well as thoroughly checked) for the reference containment state, sequence variations reflecting different containment states (or bypass paths) are readily computed. Hence, the source terms for the release into the environment will be explicitly enumerated for all combinations of CDS's and CE's.

11.7 ACR Source Term Profile

The source term profile is a surrogate for the risk profile of the plant. Some binning of the source terms according to magnitude and timing will need to be developed, that relates to public radiological consequences. Literature will be reviewed for accepted international binning practice, or original rationale would have to be developed.

The Source Term Profile is the reference baseline against which design options/modifications can be compared.

11.8 Large Release Frequency

The large release frequency will be derived by screening the source terms bins against criteria of Section 11.2 and identifying the accident with the highest frequency of relevant bins.

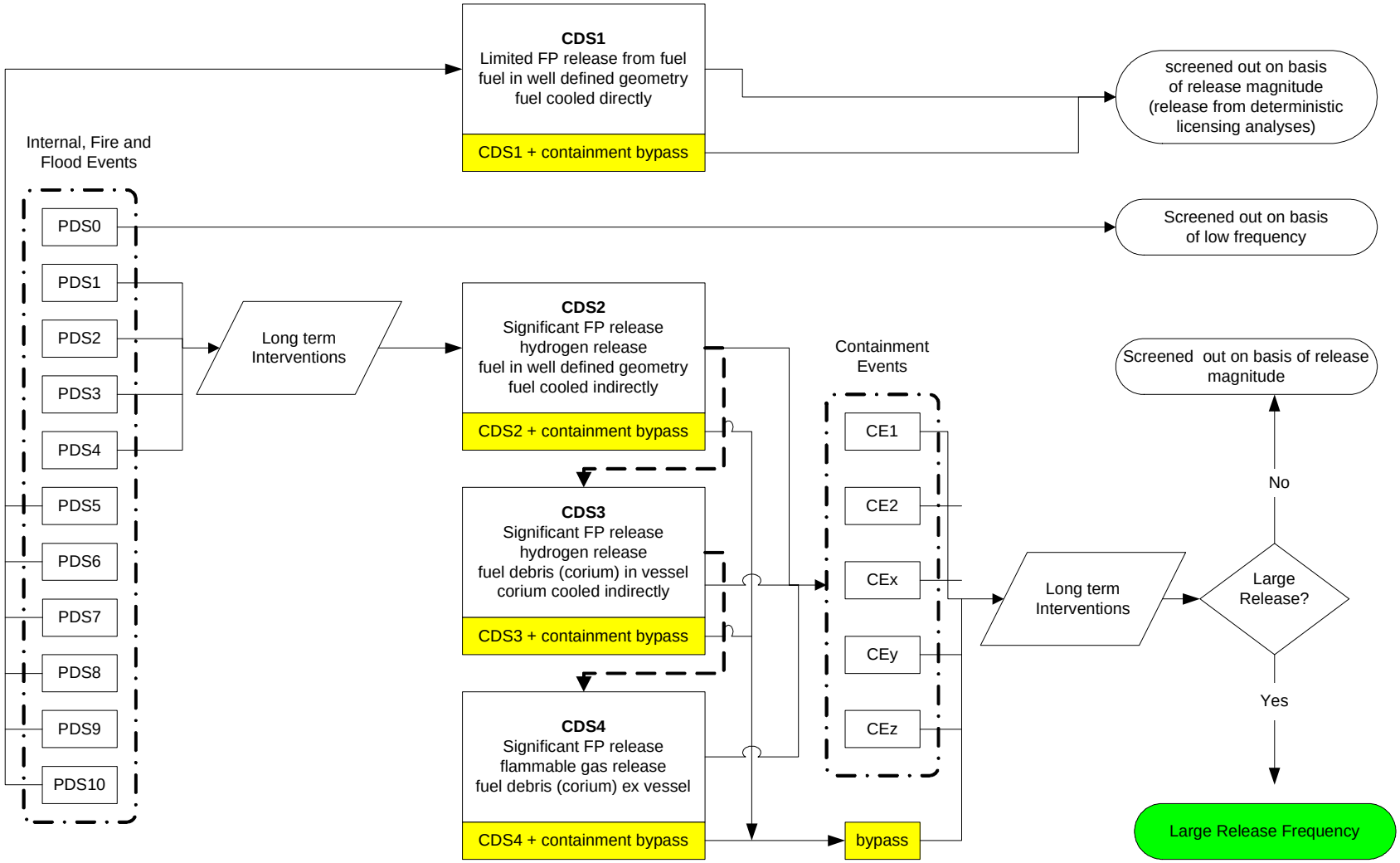


Figure 11-1 Elements of Level II PSA

12. QUALITY ASSURANCE

The quality assurance function is important to the efficiency and credibility of the PSA analysis as a whole (Reference 57).

Assurance of the quality of the ACR PSA work is provided by implementing the quality program described in the ACR Quality Assurance (QA) Manual (Reference 58), by meeting the applicable sections of the codes and standards of this QA manual, and by adhering to the PSA methodology outlined in this document.

The QA manual provides a description of the overall scope and objectives of the ACR quality program: the organization structure; roles, responsibilities, qualification and training of personnel; design control, verification, audit and program reviews.

The ACR PSA Methodology Report describes the methodology to be used in the preparation of the overall ACR PSA. The major PSA activities or tasks are shown in Figures 1-1 and 1-2.

Specific methods/procedures used in the PSA work to provide quality assurance are listed and discussed below:

a) Formal Design Documents Manual 00-03000-MAN-001;

b) Design Verification - Procedure 00-531.1;

   1) Project Operating Instructions,

   2) Review of Documentation,

c) Codes and Standards;

d) PSA Methodology;

e) Analyst’s Informal Daily Record Keeping;

f) Analysis and Software Control;

g) Review of PSA Work.

12.1 PSA Report

The Appendix S of the Formal Design Documents Manual 00-03000-MAN-001 [68] describes the following:

a) the purpose of the PSA report,

b) the preparation of the PSA report,

c) a suggested table of contents.

The procedure 00-414.3 is to be followed for the review, approval, issue and distribution of the PSA report.

12.2 Design Verification

Verification of design and analysis is achieved by using the approved procedures and operating instructions, and qualified personnel. Design and analysis verification activities are identified and summarized in the ACR Design Verification Plan (Reference 62).

12.2.1 Project Operating Instructions

Specific operating instructions will be prepared for the ACR project to ensure consistent application of methods by analysts.

12.2.2 Review Process

The review and comment process complies with procedures 00-531.4 (Reference [64]), 00-414.3 and 108-414.3.1 (References [65], [66]).

12.3 Codes and Standards

The following is a partial list of codes and standards which apply to the PSA analysis. Except as noted otherwise, the latest version of these documents will apply up to the design freeze date established for the project.

12.3.1 CNSC Documents

a) Consultative Document C-006, Rev. 1 - Requirements for the Safety Analysis of CANDU Nuclear Power Plants.

12.3.2 AECL Documents

a) Licensing Basis Document 108-00580-LBD-001, Rev. 0;

b) Quality Assurance Manual 108-01913-QAM-002;

c) Design Verification Plan 108-01920-DVP-001;

d) Technical Description 10810-01371-TED-001;

e) Formal Design Documents Manual 00-03000-001;

f) Procedure 00-681.1 - Change Control;

g) Procedure 108-681.1.1- ACR Change Control;

h) Procedure 00-414.3 - Documentation Management - Production and Release of Final Project Documents;

i) Procedure 108-414.3.1 - Production and Release of Documents using AIM and TRAK;

j) Procedure 00-531.4 - Document Review and Comment;

k) Operating Instruction - Rules for Fault Tree Event Labelling (to be issued);

l) Operating Instruction - Management of Component Reliability Database (to be issued);

m) Operating Instruction - Rules for Screening Human Reliability Analysis (to be issued).

12.4 PSA Methodology

As mentioned previously, one of the ways in which the PSA quality is assured is by adhering to the methodology outlined in this document. The major PSA tasks or activities are shown in Figures 1-1 and 1-2.

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

Each analyst will maintain an informal record of his/her analysis containing pertinent information such as descriptive material, correspondence, and notations regarding assumptions and supporting rationale. Each task in the PSA analysis (e.g., system reliability analysis) will have associated with it a readily retrievable set of information consisting 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.

f) Comments.

While this record will not be part of the formal PSA documentation itself, it will be used in report preparation. This record must be submitted to the Records Management Centre (RMS) for filing under the appropriate project and GSI number.

12.6 Analysis and Software Control

Analysis and software control will be performed in accordance with the QA Manual and the procedures referenced therein.

The major computer programs used in the PSA analysis are listed and described below. The description includes the version used, the user's manual and the verification / validation status. A complete list of all computer programs used in the PSA, will be included in the ACR PSA report.

12.6.1 CAFTA

CAFTA for Windows (Reference 41) is a micro-computer based software system for the modelling and evaluation of complex systems using fault tree analysis. It consists of a set of interactive editors (Event tree editor, Fault tree editor and Cutset editor), data bases, and model

evaluation tools. It was developed by Data Systems & Solutions of Los Altos, California. Version 5.0a of CAFTA is currently in use at AECL.

The CAFTA User's Manual provides details on the usage of this code, with supporting examples, however, it assumes some knowledge of basic fault tree methodologies and evaluation techniques as described in the Fault Tree Handbook (NUREG/CR-0492 - Reference 56) and the PRA Procedures Guide (NUREG/CR-2300 - [3]).

12.7 Review of PSA Work

An on-going review of the work, rather than at the completion of the study, is the most effective approach to quality assurance. This approach will be adopted for the ACR PSA work. It is also important that each major task of the PSA analysis be reviewed by people from different disciplines or with different perspectives 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 made in the analysis and to consistency among different analysts in addition to ensuring the accuracy of the analysis.

12.7.1 Familiarization with ACR Design

Review of the plant design will focus on how well the design information has been integrated, the selection and grouping of initiating events, and the identification of and success criteria for front-line systems. Adequate documentation to support the choice of success criteria will be provided.

Design personnel, both NSSS and Balance Of Plant, will review the analyses to ensure that the modelling is consistent with the current ACR design.

12.7.2 Event Tree Analysis

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

A standard procedure is used to initiate thermalhydraulics or other deterministic analyses required to confirm key assumptions made in the event sequence and/or event tree analysis. In this document, this analysis is referred to as PSA Support Analysis. The required PSA support analysis will be identified by the PSA team and documented in an analysis basis (AB) document for disposition by the safety analysis group. For each event requiring 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.

12.7.3 Fault Tree Analysis

Fault trees are generally reviewed in their entirety; however, particular attention is given to top logic of the fault tree. It is in this portion of the tree that major logic errors may arise. 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 consistent with the available data.

12.7.4 Human Reliability Analysis

The human reliability task will be reviewed for potential sources of human error. Each component placed in an inoperable position during testing, or removed from service during maintenance, should have human errors associated with failure to restore the component to an operable state modelled in the appropriate fault tree, unless the probability of such errors is so low as to be considered insignificant.

12.7.5 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.

c) Recovery factors reflect an understanding of the actions to be taken and of their plausibility under accident conditions.

12.7.6 Uncertainty and Sensitivity Analysis

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

12.7.7 Final PSA Report

The final PSA report is reviewed to ensure that:

a) Findings of the study are clearly stated (and supported by the analysis).

b) Assumptions inherent to the analysis in general and related to systems/sequences in particular are clearly stated.

c) Information 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.

13. REPORTING OF RESULTS

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. This, however, is time well spent. A well-prepared documentation of this thorough analysis will serve as a reference for future analyses and enhance decisions on the part of the designer (AECL) and the utilities.

This integration will include the tabulation of frequencies for accident sequences important to safety and the development of distributions reflecting the uncertainties associated with accident-sequence frequencies.

To provide focus for the assessment, the results are analysed to determine which plant features 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.

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 12), and has been modified where necessary to meet CANDU practice and needs.

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 NUREG/CR-2815.

There are several needs to be met by the documentation of a PSA study. The study 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;

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

The report should contain the following three major divisions:

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

b) The main report comprising an integration of the entire study, detailed descriptions of the tasks and associated methodology, and conclusions presented in sufficient detail to support (together with its appendices) a detailed technical review.

c) A collection of appendices containing detailed computations and data to support the models and analyses presented in the main report.

13.2.1 Executive 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. An executive summary will be included in the PSA report.

13.2.1.1 Purpose

This section should identify the purpose or objectives of the PSA.

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 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;

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

13.2.1.3 Report Organization

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

13.2.1.4 Tasks

This section should pertain to the major tasks of the PSA with a brief description of their associated methodologies, relationships to each other, and interfaces with each other.

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/dose requirements of *CNSC Consultative Document C-006, Rev. 1*;

b) Confirmation that all special safety systems meet the AECB reliability requirements as stated in Regulatory Documents R-7, R-8, and R-9;

c) Confirmation that the special safety systems as well as the key safety related systems meet both the target reliability requirements as revealed by the PSA Analysis;

d) A list of the dominant accident sequences;

e) Engineering insights into the relative importance of various system components and their overall effect on safety;

f) A list of design changes identified by the PSA and requiring implementation to improve overall plant safety;

g) Summed severe core damage frequency and large release for the ACR design.

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.

13.2.2.1 Integration

The main report should include a section, which 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 of each task;

d) A cross reference between the chapters of the main report and the appendices.

This PSA methodology document contains most of the above information and will provide the integration function.

13.2.2.2 Task Description

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

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., which inputs come directly from other tasks in the study, which are generated through iterative loops with other tasks, and which originate outside the study).

Inputs generated outside the study should be given either in the main report with specific sources cited, or in the appendices. Inputs generated within the study 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.

13.2.2.2.2 Methods for Each Task

Methods for various tasks to be performed for the ACR PSA are described in the PSA report. In some cases reference is made to other documents for more detail regarding the methodology of particular tasks. The methodology section should discuss the methods used to perform each task and subtask, as defined in this document, along with whatever additional tasks are defined by the report.

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

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

13.2.2.2.3 Outputs of Each Task

The products or outputs of each task can be viewed as “results” of the PSA 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 listing the products or outputs of the various tasks and subtasks, similar to Table 7.2 in the *Probabilistic Safety Analysis Procedures Guide* (Reference 12), be provided in the ACR PSA.

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 success and 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 undertaken to assure completeness of the models, with special attention to the initiating events, the identification of failure modes associated with each event tree heading, and the identification of dependencies, should be addressed.

13.2.3 Appendices of a Probabilistic Safety Assessment (PSA)

The appendices contain material of such sheer mass and level of detail that its inclusion in the main report is unwarranted. Examples of such material include - the system detailed fault trees, plant technical specifications, system descriptions, flow sheets, electrical elementary wiring diagrams, PSA support analysis, component reliability data bases and tables listing accident sequence quantification cut sets and importance measures.

14. REFERENCES

[1] CNSC - Safety Analysis of CANDU Nuclear Power Plants - Draft Regulatory Guide C-006, Rev. 1, September, 1999.

[2] Systematic Review of Plant Design –Methodology for identification of Initiating Events, 108-03660-AB-002, Rev. 0, June 2003.

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

[4] AECL - Licensing Basis for ACR - Licensing Basis Document 108-00580-LBD-001, Rev. 0, July 2002.

[5] USNRC - Analysis of Core Damage Frequency: Internal Events Methodology - NUREG/CR-4550, SAND86-2084, Volume 1, Rev. 1, January 1990.

[6] US NRC SRP Chapter 19.1, "Determining Technical Adequacy of PRA Results for Risk Informed Activities." Draft, 2002.

[7] AECB - Requirements for Containment Systems for CANDU Nuclear Power Plants - AECB Regulatory Document R-7, February 1991 .

[8] AECB - Requirements for Shutdown Systems for CANDU Nuclear Power Plants - AECB Regulatory Document R-8, February 1991.

[9] AECB - Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants - AECB Regulatory Document R-9, February 1991.

[10] ACR-700 Technical Description 10810-01371-TED-001, Rev. 0, June 2003.

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

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

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

[14] Computer code SMART– IST-VER-0.300, by AECL, 2002.

[15] *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*, NUREG/CR-4780, prepared by Pickard, Lowe and Garrick, Inc., USNRC, Washington, D.C., 1989.

[16] NUREG/CR-2258, "Fire Risk Analysis for Nuclear Power Plants," September 1981

[17] J. LaChance, S. P. Nowlen, F. Wyant, V. Dandini, "Circuit Analysis – Failure Modes and Likelihood Analysis," May 2000

[18] C*ommon 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, NUREG/CR-2098, prepared by EG&G Idaho, Inc., USNRC, Washington, D.C., February 1983.

[19] *Common Cause Fault Rates for Valves: Estimated Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants*, 1976-1980, NUREG/CR-2770, prepared by EG&G Idaho, Inc., USNRC, Washington, D.C., 1 February 1983.

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

[21] USNRC - A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants, NUREG-0666, April 1981.

[22] EPRI, "A Probabilistic Risk Assessment for Oconee Unit 3," NSAC-60, 1984.

[23] IAEA, Component Reliability Data for Use in Probabilistic Safety Assessment, IAEA Report, IAEA-TECDOC-478, 1988.

[24] USNRC, WASH-1400, Reactor Safety Study – An Assessment of Accident Risks in US Commercial Nuclear Power Plants, USNRC Report, NUREG – 75/014, 1975.

[25] Accident Sequence Evaluation Program Human Reliability Analysis Procedure", NUREG/CR-4772, Prepared for the USNRC by Sandia National Laboratories (SAND86-1996), Albuquerque, NM, February 1987.

[26] ASME, "Standard for PRA for Nuclear Power Plant Application", ASME-RA-S-2002, April 5, 2002.

[27] "Guidelines for Conducting Human Reliability Analysis in Probabilistic Safety Assessment", IAEA, Draft No. 1, 1989.

[28] USNRC - Handbook of Human Reliability Analysis with Emphasis on Nuclear power Plant Applications (Final Report) - NUREG / CR-1278-F, Prepared by Sandia National Laboratories (SAND80-0200), Albuquerque, NM, August 1983.

[29] "Zion NGS Units 1 and 2, IPEEE for Severe Accident Vulnerabilities Submittal Report", Commonwealth Edison Company, December 1996.

[30] "Byron NGS Units 1 and 2, IPEEE for Severe Accident Vulnerabilities Submittal Report", Commonwealth Edison Company, December 1996.

[31] "Calvert Cliffs Nuclear Power Plant PRA, IPEEE Summary Report", August 1997.

[32] J.T. Chen, N.C. Chokshi et al., Procedural and Submittal Guidance for Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, USNRC Report, NUREG-1407, 1991.

[33] IAEA, Probabilistic Safety Assessment for Seismic Events, IAEA Report, IAEA-TECDOC-724, Vienna, Austria, 1993.

[34] CSA (Canadian Standards Association), General Requirements for Seismic Qualification of CANDU Nuclear Power Plants, CAN3-N289.1-M80, R92, Canadian Standards Association, Rexdale, ON, 1992.

[35] CSA (Canadian Standards Association), Ground Motion Determination for Seismic Qualification of CANDU Nuclear Power Plants, CAN3-N289.2-M81, R92, Canadian Standards Association, Rexdale, ON, 1992.

[36] CSA (Canadian Standards Association), Design Procedures for Seismic Qualification of CANDU Nuclear Power Plants, CAN3-N289.3-M81, R92, Canadian Standards Association, Rexdale, ON, 1992.

[37] Analysis Basis- Trip Coverage Methodology, 10810-03550-AB-001, Rev. 0, December 2002.

[38] L.E. Cover et al., Handbook of Nuclear Power Plant Seismic Fragilities, USNRC Report, NUREG/CR-3558, 1985.

[39] R.D. Campbell et al., Compilation of Fragility Information from Available Probabilistic Risk Assessments, LLNL Report, UCID-20571, Revision 1, 1988.

[40] EPRI, A Methodology for Assessment of Nuclear Power Plant Seismic Margin, EPRI Report, NP-6041-M, Revision 1, Proprietary, 1991.

[41] DS & S, CAFTA Fault Tree Analysis System User's Manual, Version 5.0a, Data Systems & Solutions, Los Altos, CA, Proprietary, December 2002.

[42] DS & S, PRAQUANT Accident Sequence Quantification *User's Manual Version 4.0*, Data Systems & Solutions, Los Altos, CA, Proprietary, January 2001.

[43] IAEA, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants, Level 1, IAEA Report, Safety Series No. 50-P-4, 1992.

[44] U.S. Nuclear Regulatory Commission, Draft Regulatory Guide DG-1110, "An approach for using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific changes to the Licensing Basis", June 2001.

[45] Generic CANDU Probabilistic Safety Assessment Methodology, 91-03660-AR-001, July 2002

[46] Generic CANDU Probabilistic Safety Assessment Methodology-Reference Analysis, 91-03660-AR-002, July 2002

[47] Baltimore Gas and Electric, Calvert Cliffs Nuclear Power Plant - Individual Plant Examination for External Events (IPEEE) Summary Report, 1997.

[48] Braidwood Nuclear Power Plant - Individual Plant Examination for External Events (IPEEE) Submittal Report", June 1997.

[49] Byron Nuclear Power Plant - Individual Plant Examination for External Events (IPEEE) Submittal Report, December 1996.

[50] USNRC, Procedure for the External Event Core Damage Frequency Analyses for NUREG-1150, USNRC Report, NUREG/CR-4840, 1990.

[51] M. Missirlian, N. Alpy and M.P Kissane, "SOPHAEROS Code Version 2.0: Theoretical Manual", IPSN note technique SEMAR 00/39, March 2000.

[52] V. Ho, S. Chien and G. Apostolakis, COMPBRN IIIe, An Interactive Computer Code for Fire Risk Analysis, UCLA Report (prepared for EPRI), UCLA-ENG-9016, 1990.

[53] US NRC, An "Approach for Determining the Technical Adequacy of PRA Results in Risk Informed Activities" DG-1122, September 2002.

[54] "Development of Probabilistic Safety Assessment Methodology for Fire Events in CANDU Plants" by G. How Pak Hing and A. Stretch presented at International Workshop on Fire Risk Assessment OECD Nuclear Energy Agency (NEA), Committee on the Safety of Nuclear Installations (CSNI), Principal Working Group No. 5 (PWG5) - Risk Assessment, Helsinki, Finland, June 29 to July 01, 1999.

[55] REP/NUREG-CR-4482/1986, Recommendations to the Nuclear Regulatory Commission on Trial Guidelines for Seismic Margin Reviews of Nuclear Power plants, March 1986.

[56] USNRC - Fault Tree Handbook - NUREG-0492, January 1981.

[57] USNRC- Interim Reliability Evaluation Program Procedures guide- NUREG/CR-2728, Prepared by Sandia National Labs. Albuquerue, NM, January 1983.

[58] AECL –ACR Quality Assurance Manual - Quality Assurance Manual, 108-01913-QAM-001.

[59] GOTHIC - Containment Analysis Package, version 6.1bp2, RP4444-1 by Numerical Applications Inc (NAI 8907-06, Rev. 8) prepared for Electric Power Research Institute.

[60] IEEE- Guide to the Collection and Presentation of Electrical, electronic, Sensing Component, Mechanical Equipment Reliability Data for Nuclear Power Generating Stations, IEEE Standard 500, 1984.

[61] SRI- Nuclear Plant Reliability Data System 1982 Annual Reports of Cumulative System and Component Reliability- South west Research Institute, San Antonio, Texas, October 1983.

[62] AECL –ACR Design Verification - Design Verification Plan 108-01920-DVP-001.

[63] MAAP4-CANDU- Modular Accident Analysis Program for CANDU Power Plant, Volumes 1-3, Fauske and Associates, Inc., April 1998.

[64] AECL - Document Review and Comment - Procedure 00-531.4.

[65] AECL - Documentation Management - Production and Control of Final Project Documents - Procedure 00-414.3.

[66] AECL - Documentation Management - Production and Release of Documents using AIM and TRAK- ACR Procedure 108-414.3.1.

[67] AECL-Change Control-Procedure-00-681.1.

[68] AECL-Formal Design Documents Manual-00-03000-MAN-001.

[69] Design Earthquakes, 108-10170-DG-001, Rev. 0, Dec 2002.

[70] USNRC Policy issue, SECY-930-087, April 1993.

[71] ACR Safety Design Guide- Safety Related System, 108-03650-SDG-001, Rev. 2, January 2003.

[72] ACR Safety Design Guide-Seismic Requirement, 108-03650-SDG-002, Rev. 2, January 2003.

[73] ACR Safety Design Guide-Environmental Qualification, 108-03650-SDG-003, Rev. 2, January 2003.

[74] ACR Safety Design Guide- Separation of Systems and Components, 108-03650-SDG-004, Rev .2, January 2003.

[75] ACR Safety Design Guide-Fire Protection, 108-03650-SDG-005, Rev. 2, December 2002.

[76] ACR Safety Design Guide-Containment, 108-03650-SDG-006, Rev. 2, January 2003.

15. ACRONYMS

AB	Analysis Basis
ACR	Advanced CANDU Reactor
ACI	American Concrete Institute
A/E	Architect/Engineer
AECB	Atomic Energy Control Board
AECL	Atomic Energy of Canada Limited
AISC	American Institute of Steel Construction
ALWR	Advanced Light Water Reactor
AOM	Abnormal Operating Manual
ASD	Assessment Document
ASEP	Accident Sequence Evaluation Program
ASI	AECL Subject Index
ASME	American Society of Mechanical Engineers
ASQ	Accident Sequence Quantification
BE	Basic Event
BHEP	Basic Human Error Probability
BNL	Brookhaven National Laboratory
BOP	Balance of Plant
BWR	Boiling Water Reactor
CAFTA	Computer Aided Fault Tree Analysis
CANDU	CANada Deuterium Uranium
CCDP	Conditional Core Damage Probability
CCF	Common Cause Failure
CD	Complete Dependence
CDS	Core Damage State
CDFM	Conservative Deterministic Failure Margin
CE	Containment Events
CET	Containment Event tree
C&I	Control & Instrumentation
CN	Component Number
CNSC	Canadian Nuclear Safety Commission
COMPBRN IIIe	Fire Computer Code
CRO	Control Room Operator
CRT	Control Room Terminal
CT	Calandria Tube
CSA	Canadian Standards Association
CSRAM	Cutset Ram (CAFTA Program)
DARA	Darlington NGS A Risk Assessment
DBE	Design Basis Earthquake
DCC	Digital Control Computers
DCS	Distributed Control System
DG	Diesel Generator
DIST	Distribution Type

DS&S	Data Systems & Solutions
DVP	Design Verification Plan
ECI	Emergency Core Coolant Injection
ECC	Emergency Core Cooling
EF	Error Factor
EOP	Emergency Operating Procedure
EPRI	Electrical Power Research Institute
EPS	Emergency Power Supply
ETA	Event Tree Analysis
FM	Failure Mode
FO	Field Operator
FS	Flow sheet
FW	Feed Water
GERS	Generic Seismic Ruggedness Spectra
GPSA	Generic CANDU Probabilistic Safety Assessment
GOTHIC	Containment Analysis Computer Code
HCLPF	High Confidence of Low Probability of Failure
HD	High Dependence
HEP	Human Error Probability
HRA	Human Reliability Assessment
HTS	Heat Transport System
HVAC	Heating Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
IEEE	Institute of Electrical and Electronic Engineers
IE	Initiating Event
ILD	Instrument Loop Diagram
IPEEE	Individual Plant Examination for External Events
IST	Industry Standard Tool Set
LBD	Licensing Basis Document
LCD	Limited Core Damage
LER	Large Early Release
LLNL	Lawrence Livermore National Laboratory
LOCA	Loss of Coolant Accident
LOECC	Loss of Emergency Core Cooling
LR	Large Release
LRF	Large Release Frequency
LRV	Liquid Relief Valve
LTC	Long Term Cooling
LWR	Light Water Reactor
MAAP	Modular Accident Analysis Program
MCR	Main Control Room
MD	Moderate Dependence
MGL	Multiple Greek Letter
MM	Maintenance Manual
MMI	Man Machine Interface

MOV	Motor Operated Valve
MTTR	Mean Time To Repair
NDF	Not Developed Further
NEA	Nuclear Energy Agency
NGS	Nuclear Generating Station
NHEP	Nominal Human Error Probability
NPP	Nuclear Power Plant
NPRDS	Nuclear Plant Reliability Data System
NSSS	Nuclear Steam Supply System
OM	Operating Manual
OP	Original Performer
OPP	Operating Policies and Procedures
OPG	Ontario Power Generation (formally OH - Ontario Hydro)
PC	Post Calibration
PDS	Plant Damage State
PGA	Peak Ground Acceleration
PHT	Primary Heat Transport
PHTS	Primary Heat Transport System
PHWR	Pressurized Heavy Water Reactor
PM	Post Maintenance
PPO	Principal Power Operator
PRA	Probabilistic Risk Assessment
PRAQUANT	Accident Sequence Quantification Computer Code
PRESCON2	Containment Pressure Computer Code
PRV	Pressure Relief Valve
PSA	Probabilistic Safety Assessment
PSAR	Preliminary Safety Assessment Report
PSF	Performance Shaping Factor
PT	Pressure Tube
PV	Pneumatic Valve
PWR	Pressurized Water Reactor
QA	Quality Assurance
QAM	Quality Assurance Model
RB	Reactor Building
RAB	Reactor Auxiliary Building
RC	Release Category
RF	Recovery Factor
RLE	Review Level Earthquake
RM	Release Mode
RRS	Reactor Regulating System
RS	Reactor Shutdown
RSW	Raw Service Water
RV	Relief Valve
RWT	Reserve Water Tank
SCA	Secondary Control Area

SCD	Severe Core Damage
SCDF	Severe Core Damage Frequency
SDE	Site Design Earthquake
SDG	Safety Design Guide
SDS1/2	Shutdown System One / Two
SERA	System and Equipment Reliability Analysis
SET	Seismic Event Tree
SMA	Seismic Margin Assessment
SRP	Standard Review Plan
SS	Shift Supervisor
SSE	Safe Shutdown Earthquake
SSCs	Structures Systems and Components
SSEL	Safe Shutdown Equipment List
SSMRP	Seismic Safety Margin Research Program
SV	Solenoid Valve
SW	Service Water
TC	Type Code
TED	Technical Description
T/G	Turbine/Generator
THERP	Technique for Human Error Rate Prediction
TS	Technical Specification
UNCERT	Uncertainty Analysis Computer Code
UPM	Unified Partial Method
USNRC	United States Nuclear Regulatory Commission
ZD	Zero Dependence

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 Long Term Cooling system (LTC), 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 one steam generator.

d) Steam generator water is supplied by either the main feedwater (MFW) or auxiliary feedwater (AFW) pumps or the RWT makeup to SGs.

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 one steam generator.

d) Steam generator water is supplied by either the main feedwater (MFW) or auxiliary feedwater (AFW) pumps or the RWT makeup to SGs.

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 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

d) Steam generator water is supplied by either the main feedwater (MFW) or auxiliary feedwater (AFW) pumps or the RWT makeup to SGs.

A.2.1.3 Long Term Cooling Operation

When Long Term Cooling is the heat sink, the mode of operation is “Long Term Cooling operation with LTC pumps”. This is further 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 Long Term 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 Long Term Cooling system are inter-connected.

c) Flow is maintained by means of the Long Term Cooling (LTC) pumps.

d) Decay heat is transferred via the Long Term cooling heat exchangers.

A.2.1.3.2 Long Term 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 Long Term Cooling systems are inter-connected.

c) Flow is maintained by the Long Term Cooling (LTC) pumps.

d) Decay heat is transferred to the Long Term 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.

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.3 Component Type and Boundary Description

In Table A-2, the typical 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	
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

Component	CT Code	Boundary Description
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.
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.

Component	CT Code	Boundary Description
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.
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	

Component	CT Code	Boundary Description
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.
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	

Component	CT Code	Boundary Description
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.
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.

Component	CT Code	Boundary Description
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 600-120 ac 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.
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.

Component	CT Code	Boundary Description
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.
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.

Component	CT Code	Boundary Description
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	-
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	