OAK RIDGE
NATIONAL LABORATORY
MANAGED BY UT-BATTELLE
FOR THE DEPARTMENT OF ENERGY

ORNL/NRC/LTR-04/05

Probabilistic Risk Assessment for the ACR-700 Advanced CANDU Reactor

Review of Selected Technical Reports Related to the Methodology Used for Conducting a Probabilistic Risk Assessment for the ACR-700 Design

Michael D. Muhlheim
(Principal Investigator)

Donald A. Copinger
Joseph W. Cletcher II
Donald L. Williams, Jr.

John N. Ridgely
(NRC Project Manager)

Ronald J. Ellis
(ORNL Project Manager)

UT-BATTELLE

ORNL-27 (4-00)

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product, or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

ORNL/NRC/LTR-04/05

Nuclear Science and Technology Division
Oak Ridge National Laboratory

Probabilistic Risk Assessment for the ACR-700 Advanced CANDU Reactor

Review of Selected Technical Reports Related to the Methodology Used for Conducting a Probabilistic Risk Assessment for the ACR-700 Design

Michael D. Muhlheim
(Principal Investigator)

Donald A. Copinger
Joseph W. Cletcher II
Donald L. Williams, Jr.

NRC Project JCN Y6489

June 29, 2004

NRC Project Manager: John N. Ridgely
Division of Risk Analysis and Applications,
Office of Nuclear Regulatory Research

ORNL Project Manager: Ronald J. Ellis
Nuclear Science and Technology Division

Research sponsored by the U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, under Interagency Agreement DOE 1886-C000-9B with the U.S. Department of Energy under contract No. DE-AC05-00OR22725 with UT-Battelle, LLC

Page Intentionally Blank

TABLE OF CONTENTS

TABLES

FIGURES

EXECUTIVE SUMMARY

The U.S. Nuclear Regulatory Commission (NRC) is anticipating applications for licensing reactor facilities that are significantly advanced from the current generation of operating reactors. These new reactor designs include advanced high-temperature gas-cooled reactors (HTGRs), the gas-turbine modular helium reactor (GT-MHR), and the pebble-bed modular reactor (PBMR). Two boiling-water reactor (BWR) designs are being proposed: ESBWR and SWR-1000. Two pressurized-water reactor (PWR) designs are also being proposed: the international reactor innovative and secure (IRIS) and the AP-1000 (an advanced version of the NRC-approved AP-600). Finally, an Advanced CANDU Reactor (ACR), the ACR-700, has been proposed. This is an enhanced version of the CANDU 6 reactor. However, unlike the CANDU 6, the ACR-700 is a light-water cooled and heavy-water moderated reactor (vs a heavy-water cooled and moderated reactor).

Because NRC issued a Policy Statement on the use of probabilistic risk assessment (PRA), encouraging its use in all regulatory matters, it is necessary for the NRC to have the capability to review an applicant's PRA. The objective of this work was to review several generic CANDU (GC) and ACR probabilistic safety assessment (PSA) documents to gain insights into the strengths and weaknesses of the PRA methodology and analysis supporting the ACR-700 design. This work was performed with the understanding that any review of methodology and reference analysis documents can only yield insights into how the PRA will be performed; it is not a substitute for—nor can it be—an actual PRA review.

The work in this project involved reviewing the following documents:

1. Letter Report, "Response to the US-NRC Staff Request for Information on OPG PRAs,"
2. *Generic CANDU Probabilistic Safety Assessment—Methodology*,
3. *Generic CANDU Probabilistic Safety Assessment—Reference Analysis*,
4. *Probabilistic Safety Assessment Methodology, ACR* (ACR PSA),
5. *Design Assist Role of ACR Probabilistic Safety Assessment (PSA)*, and
6. *Preliminary Design Assist PSA Level 1 –Selected Full Power Event Trees*.

The GC PSA and ACR PSA methodology and reference analysis reports are based on a number of source PSA documents, relevant past Atomic Energy of Canada Limited (AECL) PSA work, and new analyses either for events that were not previously considered or to replace previous analyses that had become outdated.

In identifying any strengths and weaknesses of the GC PSA and ACR PSA methodology, the guidance provided in NUREG/CR-2300, *PRA Procedures Guide*, and American Society of Mechanical Engineers (ASME) RA-S-2002, *Standards for Probabilistic Risk Assessment for Nuclear Power Plant Applications* was considered. In addition, personnel insights from operational, design, and PRA experience of the ORNL staff conducting the review have been included.

For each section/appendix of the documents that were reviewed, this report contains an overview of the section/appendix, a brief summary of the PRA methodology described, and general comments on the methodology's strengths and weaknesses.

Because the ACR-700 incorporates unique features and design characteristics, the guidance provided by PRA guidance documents written for light-water reactors (LWRs) may not completely cover the safety basis for an ACR. For example, compared to LWRs, the use of heavy water for a moderator makes tritium production a unique concern applicable to the CANDU and ACR nuclear power plants (NPPs).

Thus, to thoroughly evaluate the strengths and weaknesses of the ACR PSA methodology, the CANDU and ACR methodology and reference analysis documents need to provide more detailed information. The benefit of reviewing the documents is that they provide a good overview of the PRA methodology. This overview can then be used to identify

1. differences from LWR-specific techniques,
2. where LWR-specific technology may not be appropriate for heavy-water moderated and/or cooled NPPs, and
3. deficiencies in current methods being applied to advanced NPPs.

From the review performed, general observations about the relative strengths and weaknesses (when compared to NUREG/CR-2300 and ASME RA-S-2002) of the GC and ACR PSA methodology were documented in the various sections. These observations and/or questions concerning the AECL PSA information (methodology, assumptions and results) are summarized in Sections 4.11, 5.10, 6.16, 7.3, and 8.3 of this report. The overall observations from reviewing all six documents is provided below. When the ACR-700 plant design details become available, the answers to these observations/questions may be resolved or confirm the existence of further strengths or weaknesses in the PRA methodology employed by AECL for the ACR-700 safety analysis.

Reporting Strengths

- The GC PSA process appeared to be generally consistent with typical PRAs,
- the information provided is generally complete and easily understood, and
- the ACR PSA is more thorough than the GC PSA for what is provided.

Reporting Weaknesses

- There is a lack of sufficient details, supporting information, assumptions, or references in describing plant systems or methodology,
- although many sections provide sufficient detail on what is reported, at times information necessary to fully understand the methodology or analysis is not reported, and
- errors or inconsistencies exist between tables, and some figures were too small to read.

The most significant reporting weakness is the use of proprietary documents as references. Although proprietary documents would be available to the NRC, they are not available to the general public.

Methodology Strengths

- PRA is used early in the design,
- occasionally, recent plant data were cited,
- PRAs are based on NUREG/CR-2300 but are updated with new methods when appropriate, and
- PRA uses 16-digit event identification nomenclature.

Methodology Weaknesses

- Calculational errors and inconsistencies questioned the calculation techniques, results, and sensitivity/uncertainty analyses,
- 20–30 year old data provide the basis for many failure probabilities,
- MAAP CANDU has not been reviewed and accepted by NRC,
- the use of new standards or methods provides uncertainty in calculations and models,

- some probabilities are based on judgments,
- not all components or systems appear to be considered,
- not all assumptions appear to be appropriate,
- the numerous weaknesses in the fire methodology, taken together, represent an important weakness, and
- the ACR PSA is an ASME RA-S-2002 Category I PRA; in practice, however, the ASME category varies over different elements of the PRA and is not a global category assignment.

If AECL updates its UPM values with NUREG information, they would need to justify the use of this data. Regardless, AECL should fully document the implementation of the UPM in its PSA.

Regarding the use of the ASME standard, this review did not incorporate NRC staff positions on implementation of that standard given in draft guide DG-1122 (Regulatory Guideline 1.200).

The peer review processes described in NEI 00-02, Appendix B of DG-1122, and Chap. 6 of the ASME standard were not used for this review of the ACR-700 methodology or analysis documents. A peer review based on the guidance given in these documents should be performed and documented by AECL.

Page Intentionally Blank

FOREWORD

This report documents the review of information provided by the Atomic Energy of Canada Limited (AECL) related to their method for developing probabilistic risk assessments (PRAs) for CANDU and ACR-700 reactors. The review was performed collaboratively between Oak Ridge National Laboratory personnel and NRC, Office of Nuclear Regulatory Research staff. This review was performed at the request of the Office of Nuclear Reactor Regulation (NRR) and was approved by the New Reactor Technical Advisory Committee. This report will form part of the basis for NRR to write their portion of the pre-application safety assessment report on PRA method for the ACR-700 reactor, as requested by AECL.

AECL provided six documents which were reviewed and compared to PRA guidance provided in NRC reports, industry standards (e.g., American Society of Mechanical Engineers Standard), and previous PRAs (e.g., NUREG-1150 PRA studies and the Individual Plant Examinations (IPEs)). This report documents that review and discusses the strengths and weaknesses in the AECL PRA method. The review found that the PRA method used by AECL was in general agreement with the current guidance and practice in the United States. However, there are some short comings in their method of developing a PRA which warrants careful attention during the review of the PRA for design certification. Strengths and weaknesses are identified in the report.

Page Intentionally Blank

ACKNOWLEDGMENTS

This project has been supported by the U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, under Interagency Agreement DOE 1886-C000-9B with the U.S. Department of Energy under contract No. DE-AC05-00OR22725 with UT-Battelle, LLC.

The authors are grateful for the assistance of the NRC's Office of Nuclear Regulatory Research (RES). The RES project manager, John N. Ridgely, was instrumental in providing guidance on technical issues. We would like to especially thank Douglas E. Peplow and Randall J. Belles for their technical review and analysis. In addition, the authors wish to thank L. B. Dockery, B. J. Smith, and C. C. Southmayd for their assistance in word processing and technical editing. The rapid turnaround of materials by these individuals was greatly appreciated.

Page Intentionally Blank

ACRONYMS

ac	alternating current
ACR PSA	*Probabilistic Safety Assessment Methodology, ACR*
ACR	advanced CANDU reactor
AECL	Atomic Energy of Canada Limited
AFW	auxiliary feedwater
AL	administrative letter
ASEP	Accident Sequence Evaluation Program
ASME	American Society of Mechanical Engineers
BHEP	basic human error probability
BOP	balance of plant
Btu	British thermal unit
BWR	boiling-water reactor
C&I	Control & Instrumentation
CAFTA	computer-aided fault tree analysis
CANDU	CANada Deuterium Uranium
CC	crash cooldown
CCDP	conditional core damage probability
CCF	common-cause failure
CDF	conservative deterministic failure
CDFM	conservative deterministic failure margin
CDS	core damage state
CET	containment event tree
CNSC	Canadian Nuclear Safety Commission
COG	CANDU Owners Group
COMPBRN	fire computer code
CSA	Canadian Standards Association
CSNI	Committee on the Safety of Nuclear Installations
CVIS	containment ventilation isolation system
D/S	detection/suppression
DBE	design basis earthquake
dc	direct current
DG	diesel generator
ECC	emergency core cooling
ECCS	emergency core cooling system
ECI	emergency coolant injection
ECIS	emergency coolant injection system
EFW	emergency feedwater
EPRC	ex-plant release category
EPRI	Electric Power Research Institute
EQESRA	earthquake computer code
ET	event tree
ETA	event tree analysis
EWS	emergency water supply
FD	flood damage state
FDC	fuel damage category
FDS	fire damage state
FMEA	failure mode and effects analysis

GC PSA	*Generic CANDU Probabilistic Safety Assessment—Methodology/Analysis*
GSS	guaranteed shutdown state
HCLPF	high confidence of low probability of failure
HEP	human error probability
HRA	human reliability assessment
HTGR	High-Temperature Gas Reactor
HTS	heat transport system
IAEA	International Atomic Energy Agency
IDCOR	Industry Degraded Core Rulemaking (Program)
IE	initiating event
IEEE	Institute of Electrical and Electronic Engineers
IPEEE	individual plant examination for external events
IRIS	International Reactor Innovative and Secure
ISLOCA	Interfacing System LOCAs
KEMA	N. V. Tot Keuring van Elekrotechnische Materialen
LBD	licensing basis document
LERF	large, early release frequency
LCD	limited core damage
LOCA	loss-of-coolant accident
LOECC	loss of emergency core cooling
LOOP	loss of offsite power
LRV	liquid relief valve
LTC	long term cooling
LTCS	long term cooling system
LWR	light-water reactor
MAAP	Modular Accident Analysis Program
MCC	motor control center
MCR	main control room
MFW	main feedwater
MGL	multiple Greek letter
MMI	man-machine interface
MSLB	main steam line break
MOV	motor-operated valve
NDF	not developed further
MSSV	main steam safety valve
NEA	Nuclear Energy Agency
NEI	Nuclear Energy Institute
NGS	nuclear generating station
NHEP	nominal human error probability
NPP	nuclear power plant
NPRDS	nuclear plant reliability database system
NRC	United States Nuclear Regulatory Commission
OECD	Organization for Economic Cooperation and Development
OPG	Ontario Power Generation (formally Ontario Hydro)
ORNL	Oak Ridge National Laboratory
PBMR	Pebble-Bed Modular Reactor
PC	post calibration
PDS	plant damage state
PHWR	pressurized heavy-water reactor
PIRT	phenomena identification and ranking table

PLG	Pickard, Lowe and Garrick
PM	post maintenance
PPSA	pre-project PSA
PRA	probability risk assessment
PSA	probabilistic safety assessment
PSF	performance shaping factor
PV	pneumatic valve
PWR	pressurized-water reactor
QA	quality assurance
RA	risk assessment
RC	release category
RCS	reactor coolant system
RCW	recirculating cooling water
RF	recovery factor
RIS	regulatory issue summary
RM	release mode
RSW	raw service water
RWS	reserve water system
RWT	reserve water tank
S	success
SCA	secondary control area
SCD	severe core damage
SCDF	severe core damage frequency
SDC	shutdown cooling
SDM	safety design matrix
SDS	shutdown system
SECY	Secretary of Commission, Office of the (NRC)
SG	steam generator
SGPR	steam generator pressure relief
SHA	seismic hazard analysis
SBLOCA	small break LOCA
SR	supporting requirements
SRP	systematic review of plant
SSC	structures, systems, and components
SSMRP	Seismic Safety Margin Research Program
THERP	Technique for Human Error Rate Prediction
UPM	unified partial method

Page Intentionally Blank

ABSTRACT

The U.S. Nuclear Regulatory Commission (NRC) is anticipating applications for licensing reactor facilities that are significantly advanced from the current generation of operating reactors.

The objective of this work was to review several CANDU and ACR PSA documents to gain insights into the strengths and weaknesses of the methodology and analysis supporting the ACR-700 design. This work is performed with the understanding that any review of methodology and analysis documents can only yield insights into how the PRA will be performed; it is not a substitute for—nor can it be—an actual PRA peer review.

For each section/appendix of the documents that were reviewed, this report contains an overview of the section/appendix, a brief summary of the PRA methodology described, and general comments on the methodology's strengths and weaknesses.

While the AECL methodology is consistent with the intent of NUREG/CR-2300 and ASME RA-S-2002, there are some weaknesses in the methodology and in reporting the methods and assumptions used.

Page Intentionally Blank

1. INTRODUCTION

1.1 Objectives of Proposed Work

The U.S. Nuclear Regulatory Agency (NRC) is anticipating applications for licensing reactor facilities that are significantly advanced from the current generation of operating reactors. These new reactor designs include advanced high-temperature gas-cooled reactors (HTGRs), the gas-turbine modular helium reactor (GT-MHR), and the pebble-bed modular reactor (PBMR). Two boiling-water reactor (BWR) designs are being proposed ESBWR and SWR-1000. Two pressurized-water reactor (PWR) designs are being proposed: the international reactor innovate and secure (IRIS) and the AP-1000 (an advanced version of the NRC-approved AP-600). Finally, the Advanced Canada Deuterium Uranium (CANDU) Reactor ACR-700, a light-water cooled and heavy-water moderated reactor has been proposed; it is an enhanced version of the CANDU 6 reactor.

Because NRC issued a Policy Statement[1, 2] on probabilistic risk assessment (PRA), encouraging its use in all regulatory matters, it is necessary for the NRC to have the capability to review the applicant's PRA. The objective of this work was to review several CANDU and ACR probabilistic safety assessment (PSA) documents to gain insights into the strengths and weaknesses of the methodology and analysis supporting the ACR-700 design. This work is performed with the understanding that any review of methodology and analysis documents can only yield insights into how the PRA will be performed; it is not a substitute for—not can it be—an actual PRA review. In reviewing the strengths and weaknesses of the PRA methodology, the guidance provided in NUREG/CR-2300, *PRA Procedures Guide*,[3] and American Society of Mechanical Engineers (ASME) RA-S-2002, *Standards for Probabilistic Risk Assessment for Nuclear Power Plant Applications*[4] was considered. In addition, personnel insights from operational, design, and PRA experience of the Oak Ridge National Laboratory (ORNL) staff conducting the review have been included.

1.2 Work Approach

The work in this project involved reviewing the following documents:

1. Letter Report, "Response to the US-NRC Staff Request for Information on OPG PRAs,"[5]
2. *Generic CANDU Probabilistic Safety Assessment—Methodology (GC PSA)*,[6]
3. *Generic CANDU Probabilistic Safety Assessment—Analysis (GC PSA)*,[7]
4. *Probabilistic Safety Assessment Methodology, ACR (ACR PSA)*.[8]
5. *Design Assist Role of ACR Probabilistic Safety Assessment (PSA)*,[9] and
6. *Preliminary Design Assist PSA Level 1 –Selected Full Power Event Trees*.[10]

References 6–10 are very detailed and lengthy documents. Consequently, to tailor the review to fit within the budget and schedule parameters of the project, a graded approach to the review of the documents was employed. The graded approach focused the resources dedicated to the review toward those sections of the documents that could provide more useful insights on the strengths and weaknesses of the methodology employed for the analyses. Table 1 indicates the type of review for each section.

For each section/appendix of the referenced documents that were reviewed, this report contains an overview, a brief summary of the PRA methodology, and general comments on the methodology's strengths and weaknesses.

Because the CANDU and ACR PSA methodology and analysis reports cover the same information and, in the case of the CANDU analysis report, rely on the same methodology, the comparisons to two PRA standards─NUREG/CR-2300 and ASME R-SA-2002─are made in the review of the GC PSA methodology document (see Section 4 of this report).

Table 1. Type of Review

Document Review	Type of Review		
	Cursory[a]	**Light Technical**[b]	**Technical**[c]
Response to the US-NRC Staff Request for Information on OPG PRAs			
Letter Report	✔		
GC PSA—Methodology (91-03660-AR-001)			
Sections 1–3	✔		
Section 4		✔	
Sections 5–9			✔
Sections 10–12	✔		
Appendices A–D[d]			✔
Appendix E	✔		
GC PSA—Analysis (91-03660-AR-002)			
Sections 1–3	✔		
Sections 4–11		✔	
Sections 12–13	✔		
Appendix A			✔
Appendices B–D		✔	
Appendices E, G, I, K, O, Q[d]			✔
Appendices F, H, J, L, M, N, P		✔	
ACR PSA (108-03660-AB-001)			
Sections 1–3	✔		
Section 4		✔	
Sections 5–9			✔
Sections 10–12	✔		
Appendices A–D			✔
Appendix E	✔		
Design Assist Role of ACR PSA (108-03660-ASD-008)			
Assessment Document			✔
Preliminary Design Assist PSA Level 1—Selected Full Power Event Trees **(10810-03660-AR-001)**			
Analysis Report			✔

[a] A cursory review is a brief, quick, and superficial review.

[b] A light technical review entails reading the entire text of the selected section or appendix and identify glaring or obvious errors. Apply engineering judgement and expertise as to what is important. This type of review is not an analytical, technical review.

[c] A technical review entails reading the entire text of the selected section or appendix and identify glaring or obvious errors; apply engineering judgement and expertise as necessary to complete the review. No duplication of calculations, or extensive comparison between references and material to be reviewed.

[d] For appendices with event trees, a selected event tree technical review is performed. This review is similar to the technical review, except the review is applied to selected event trees from the PRA.

Page Intentionally Blank

2. SUMMARY OF ACR-700 DESIGN AND DIFFERENCES FROM CANDU DESIGNS

The ACR-700 is an advanced CANDU design, which has several significant design changes from previous CANDU reactor designs. Three of the four documents reviewed under this activity pertain to generic CANDU 6 and CANDU 9 reactor designs; the fourth document pertains to the ACR design. The CANDU 6 system is Atomic Energy of Canada Limited's (AECL's) design for a single-unit containment pressurized heavy-water reactor (PHWR), with a nominal output of about 700 MW(e). The CANDU 9 system is a larger PHWR design [940 MW(e) nominal output] and contains a number of advanced features that enhance plant operability and safety.

AECL Technologies' ACR-700 design is a light-water-cooled, heavy-water moderated reactor that incorporates features from both CANDU and light-water reactor (LWR) technologies (Reference 6). The ACR-700 uses a conventional CANDU reactor cooling system, with two steam generators and four main coolant pumps. The design uses slightly enriched uranium dioxide fuel in a CANFLEX™ fuel design, light-water coolant, a separate heavy-water moderator, computer-controlled operation, and on-power refueling. The reactor has horizontal pressure tubes supported in a tank filled with the low-pressure, low-temperature heavy-water moderator. The tank also supports the reactivity regulating and safety devices, which are located within the low-pressure moderator. This is surrounded by a water-cooled shield. The engineered safety features include an emergency coolant injection (ECI) system and a long-term cooling system (LTCS).

The ACR-700 design is based on the CANDU 6 and CANDU 9 designs. The basic CANDU features that have been retained in the ACR-700 include

- horizontal pressure tubes;
- on-power fueling and the fuel handling system; and
- a separate low-pressure, low-temperature heavy-water moderator.

The evolved characteristics of the ACR-700 include

- the CANFLEX fuel design with slightly enriched UO_2 fuel,
- light-water coolant,
- a negative full-core coolant-void reactivity,[a]
- a more compact core configuration,
- increased steam pressure and temperature to the turbine, and
- a more compact plant layout.

The ACR-700 design is based largely on standard components from the CANDU 6 and CANDU 9 designs. The ACR-700 design consists of horizontal fuel channels (i.e., each comprised of a pressure tube surrounded by a calandria tube), in a conventional heavy-water-moderated calandria vessel (Figure 1). The reactor core uses calandria and fuel channel design features adapted from CANDU 6. The pressure tubes are similar to those of current CANDUs albeit slightly stronger because of the increased operating pressure. Also, the calandria tubes for the ACR-700 are larger in diameter and stronger. The stronger calandria tube design substantially reduces the risk of channel failure in the event

[a] This characteristic is currently under discussion. At this time, there are indications that under certain conditions the coolant-void reactivity coefficient may be positive. It should be noted that AECL's calculations are core averages and do not address localized conditions, uncertainties, or conservatisms.

of a spontaneous pressure tube rupture. Fuel channel external end fittings, with connections to the external coolant system piping, and the fuel channel closure plug are new components that are undergoing qualification testing at AECL's laboratories. The fuel is slightly enriched (i.e., 2 wt % ^{235}U) CANFLEX fuel. The light-water reactor coolant system (RCS) is a conventional layout with two steam generators and four pumps. Reactor coolant pumps, steam generators, and the RCS piping are based on the CANDU 6 and CANDU 9 designs. The turbine-steam-feedwater system is adapted from the current CANDU 6 design being built in China.

The ACR-700's safety systems are similar to current generation CANDUs. Two fully independent and diverse shutdown systems are provided. Shutdown system one (SDS1) uses mechanical shut-off rods, with modified dimensions to accommodate the reduced lattice pitch relative to existing CANDU designs. Shutdown system two (SDS2) injects liquid gadolinium nitrate into the moderator. The emergency core cooling system (ECCS) is similar to current generation CANDUs because it uses light water and has both a high-pressure injection stage and a recovery stage. The single-unit containment building is a steel-lined, pre-stressed concrete building. The containment building includes hydrogen control devices for severe accidents such as a loss-of-coolant accident (LOCA) coincident with failure of the ECCS (i.e., for which the moderator acts as a passive backup heat sink to prevent loss of core geometry). Severe accidents that progress to loss of core geometry are also explicitly addressed in the design. For example, an elevated water system provides backup passive decay heat removal for severe core damage accidents.

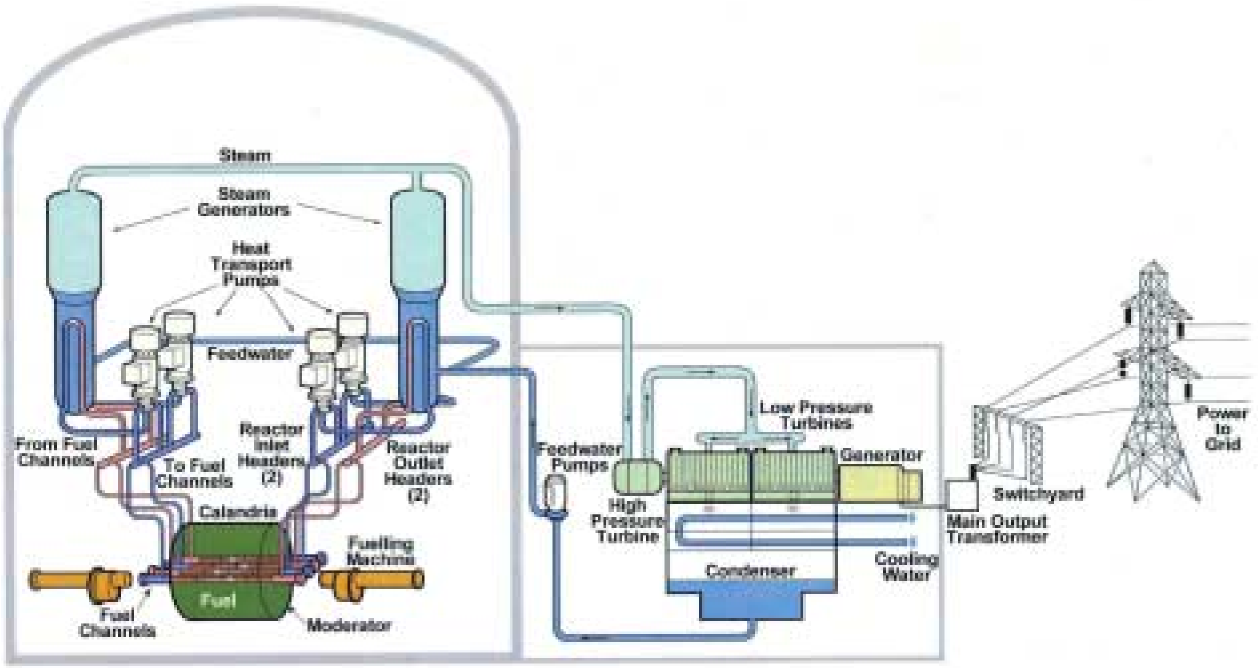

Figure 1. Features of ACR CANDU

3. CNSC's RESPONSE TO THE U.S. NRC STAFF REQUEST FOR INFORMATION ON OPG PRAs

This report[5] discusses the results from a review performed by the Canadian Nuclear Safety Commission (CNSC) staff of three Level III PRAs, internal events (including flood). Two of the PRAs were performed by Ontario Power Generation (OPG) for their Pickering A and Bruce B nuclear power plants (NPPs). The third PRA was performed by Bruce Power for their Bruce A NPP.

3.1 Methodology

OPG used a unique methodology to execute its PRAs. This resulted, in CNSC staff's words, in an "inscrutable model" with "low traceability" and made for a "very difficult review." However, CNSC staff was able to "create replicas" of these two PRAs using hard-copy event trees (presumably from the PRAs themselves) and electronic fault trees. Based on the results of the CNSC staff's reviews, the licensee decided "to migrate its PRAs under an industry standard tool." This latter phrase was interpreted to mean that the OPG PRAs were reconfigured for another computer code. Presumably this also means that the new code is, in the words of CNSC staff, "an industry standard." The report did not specify what computer codes were considered to be industry standards, thereby preventing comparison with the U.S. nuclear industry's PRA techniques or computer codes.

CNSC staff alluded to "the unique methodology" used by OPG to perform its PRAs and indicated that they (CNSC staff) had replicated the PRAs using two different codes (Risk-Spectrum[11] and SAPHIRE[12]). The methodology described in AECL's methodology reports[6, 7] and detailed (somewhat) in its analysis report[8] needs to be compared with both the OPG methodology (if available) and that used by CNSC staff (if available), before further review can be done.

The methodology for the Bruce Power's Bruce A NPP PRA was developed "according to standard techniques, under Risk-Spectrum." The methodology may be consistent with U.S. NPP standards and techniques; however, the methodology must be presented before further review can be done.

3.2 Strengths and Weaknesses

The results from the PRAs reviewed by CNSC staff (and indicated in its report) were clear, concise, and to the point. The level of detail for the material presented in the report is adequate; however, the reviewing task would be improved with some further exposition (CNSC's report consists of five pages). Based on its review, CNSC staff recommended several design changes for the Pickering A and Bruce B NPPs. CNSC staff indicated that the level of detail for the Bruce Power's PRA of the Bruce A NPP PRA was lower than that for the OPG PRAs. Because CNSC staff had not initiated a review of the Bruce A PRA, no indication was made on the relative differences between the PRAs. Thus, a review of the level of detail for that portion of the report devoted to the Bruce A PRA was not possible. CNSC reserved recommendations concerning the Bruce A NPP until after its review of that plant's PRA was completed.

Page Intentionally Blank

4. GC PSA─METHODOLOGY

The purpose of AECL's generic CANDU probabilistic safety assessment[6] (GC PSA) is to aid analysts in performing Level I and Level II PSAs for internal events, shutdown events, internal fires, internal flooding, and specific external events (i.e., earthquakes). "The intent of AECL's GC PSA program has not been to perform detailed assessments for every initiating event, but rather to establish PSA methodologies that are consistent with the current international state-of-the-art, and to apply them to those areas that were deemed to be most critical in prior PSA analyses."[6]

The GC PSA methodology document[6] presents the methods and tools

1. for developing full-scope Level I and II PSAs, including external events,
2. to generate a reference analysis to be used as a framework for future AECL projects; and
3. to gain insights into the design of the fully developed reactor products (CANDU 6 and CANDU 9).

Thus, the GC PSA describes methodologies for conducting the following analyses:

1. introduction and general PRA methodology (GC PSA Sections 1–3 and Appendix E)
2. internal events PRA (GC PSA Section 4 and Appendix A)
3. common-cause failure analysis (GC PSA Section 5)
4. human reliability analysis (GC PSA Section 6)
5. seismic events PRA (GC PSA Section 7 and Appendix B)
6. fire events PRA (GC PSA Section 8 and Appendix C)
7. flood events PRA (GC PSA Section 9 and Appendix D)
8. Level-II PRA (GC PSA Section 10)

The GC PSA methodology report also provides a brief overview of the generic CANDU design (Section 2), presents conclusions (Section 11), and, finally, provides a glossary of terms (Section 12). References, tables, and figures are provided at the end of each section.

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

The GC PSA report does not provide a separate methodology for the shutdown PRA because "it basically follows the same procedure as the internal PRA. However, for the shutdown PRA, special attention must be paid to manual operator actions, configuration of the systems, maintenance practices and available heat sinks." Although the GC PSA identifies the failure modes of the refueling machine in Appendices B and E, it is unclear how on-power refueling is addressed.

4.1 Section 1, "Introduction;" Section 2, "Description of CANDU Design;" Section 3, "PSA Methodology─General;" and Appendix E, "General CANDU Single Unit Design Description"

Section 1 (Introduction) describes the Level 1 enhancements regarding human reliability assessment (HRA), common-cause failures (CCFs), seismic concerns, fire issues, and flooding issues for the GC PSA. The introductory section also indicates that no specific shutdown PRA would be performed. Section 2 (Description of CANDU Design) indicates that the generic design would be a pressure tube type reactor, with heavy water to be used as both the moderator and coolant. (The ACR-700 uses light water for its coolant and heavy water for its moderator.) Ordinary (light) water would be used on the secondary side to generate steam for the main turbines. Two safety groups and associated support systems would meet the shutdown decay heat removal and post accident monitoring requirements. Two emergency shutdown systems are both functionally different and physically separated. The control rod system is a solid shutdown system that is functionally different from the moderator poison injection system.

Section 3 (PSA Methodology—General) describes the three levels of PSAs (i.e., Level I—System Analysis, Level II—System and Containment Analysis, and Level III—Consequence Analysis). The following references provide a list of generic initiating accidents, their frequency, and dose criteria: *Requirements for the Safety Analysis of CANDU Nuclear Power Plants*,[13] *Probabilistic Safety Assessment Goals in Canada*,[14] and *Basic Safety Principles for Nuclear Power Plants*.[15] Section 3 also defines severe accidents[**] and severe core damage accidents.[††] The NRC's and IAEA's safety goals of 1×10^{-4}/year are compared to AECL's safety goal of 3×10^{-5}/year for the CANDU 6 design and 3×10^{-6}/year for the CANDU 9 design. Finally, the following areas of study that will be covered in subsequent chapters are introduced: internal events PRA, external events analysis, seismic PRA, internal fire PRA, and internal flooding PRA.

4.1.1 Methodology

The methodology follows typical practices by using PRA as an "analytical technique used to integrate the many different aspects of design and operation to assess the safety of a particular facility and to develop an information base for analyzing plant-specific and generic issues. In particular, a PRA is used to determine core damage frequency and risk to the public." Thus, the objective of a PRA is to identify all fault sequences that contribute to risk, determine the weaknesses of plant design, and prioritize the need to make changes (modifications) in the plant design to mitigate any identified risks.

4.1.2 Strengths and Weaknesses

The presentation of Sections 1–3 is consistent with typical PRAs and is easy to follow. Sections 1–3 provide sufficient detail in introducing the methodology that will be presented in detail in the subsequent sections. The material presented in Sections 1–3 is complete and very detailed.

Appendix E appears to be complete, easily understood, and gives the basic design features and considerations for each reactor system design. Appendix E does not contain a lot of details—this is appropriate because this description provides an overview of reactor design philosophy. It describes the purpose of each of the following systems:

Nuclear Steam Supply System (NSSS)

- Reactor
- Fuel Handling System
- Heat Transport System (HTS)
- Moderator System
- Reactor Regulating System

[**] **Severe accident**—an accident, following which core heat removal by normal means is unavailable, due to initial or consequential failures of systems and structures. These events have moderate fuel temperature excursions (i.e., peak temperatures well below the melting point of core materials) and only a small, insignificant release of volatile fission products from the damaged core.

[††] **Severe core damage accident**—Severe core damage requires a loss of heat transport system (HTS) coolant, the failure of ECC injection, and a loss of the moderator cooling system. These events lead to core heatup, the disassembly of channels into debris, and high releases of fission products.

Balance of Plant (BOP)

- Feedwater and Steam Generator System
- Turbine Generator System
- Electric Power System

Safety Systems

- Electrical—not clear if separated into trains
- Class III Power Supply [alternating current (ac) source from diesel generator (DGs)]
- Class II Power Supply (uninterruptible ac source)
- Class I Power Supply [direct current (dc) source]

Safety Grouping

- Shutdown System No. 1
- Shutdown System No. 2
- Emergency Core Cooling
- ECCS System
- Backup Decay Heat Removal (Moderator Heat Sink)

The overview of the GC PSA process is provided in GC PSA Figure 3-1 and is based on Figure 2-1, "Risk Assessment Procedure," of NUREG/CR-2300. The figures are identical with only minor wording changes. One minor difference between the two overview figures is that "external event analysis" in NUREG/CR-2300 was replaced with "event sequence development" in the GC PSA This appears to be a terminology change because external events are covered in the GC PSA. The other minor difference is that the term "uncertainty" on Figure 2-1 in NUREG/CR-2300 was replaced with "uncertainty and sensitivity analysis" in Figure 3-1 in the GC PSA. Again, this appears to be a clarification to Figure 2-1 because the treatment of uncertainties in NUREG/CR-2300 covers procedures for both uncertainty and sensitivity analyses.

4.2 Section 4, "Internal Events PSA" and Appendix A, "Internal Events PSA Supporting Information"

Performing a PRA involves developing a set of possible accident sequences and determining their outcomes. Plant system models generally consist of event trees that depict initiating events and combinations of system successes and failures and fault trees that depict ways in which the system failures represented in the event trees can occur. These models are analyzed to assess the frequency of each accident sequence.

The methodology in the GC PSA for internal events analysis generally follows that described in NUREG/CR-2300, and is listed below:

1. collecting plant information,
2. initiating event (IE) analysis,
3. event tree development,
4. system reliability analysis,
5. dependent failure analysis,
6. human reliability analysis,
7. data-base development,
8. accident sequences quantification,
9. plant damage state analysis,

10. uncertainty and sensitivity analyses, and
11. quality assurance.

Appendix A details the collection and analysis of data. A failure rate is derived from the raw data called "mean time between failure." The data is described as exponentially distributed consistent with data gathered from

1. highly reliable components,
2. small population,
3. low number of failures, and
4. short time spans.

Confidence limits are calculated using the Chi-square distribution. Tables are presented detailing plant success states and mission times. Component types and boundary descriptions for the grouping along with component failure modes and mechanisms are presented.

4.2.1 Methodology

Initiating event analysis

Applicable IEs are selected from (Section 4.2, Initiating Event Analysis)

- a generic list of IEs that require safety analysis,
- systematic design review studies from previous CANDU plants, using master logic diagrams for each front-line system that contains radionuclides and their support systems, and
- a failure modes and effects analysis procedure that examines the consequences of the failure of individual and multiple components of the main systems that contain radionuclides and also examines the failure modes of their support systems for new designs; and a fault tree logic diagram (master logic diagram) that focuses on the release of radionuclides to containment and the potential causes of this event.

The method used to identify IEs meets the objective of ASME R-SA-2002─to identify events that challenge plant operations and that require successful mitigation to prevent core damage. The use of a systematic, structured process for identifying IEs is consistent with the high-level requirements in ASME R-SA-2002 and the process described in NUREG/CR-2300. The events that result from the development of the logic diagrams are subsequently grouped according to similarity of plant response, into a single, bounding, higher-level event. This agrees with the high-level requirements in ASME R-SA-2002. Based on these IEs 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.

This overall process for identifying IEs is the same in the GC PSA as that detailed in NUREG/CR-2300 (Sections 3.4.1–3.4.2) except that NUREG/CR-2300 divides IEs into transients and LOCAs and then further subdivides these categories in terms of general characteristics of the plant response. NUREG/CR-2300 notes that "The distinction between LOCAs and transient events has been carried over from licensing-type evaluations and is used only for convenience in a PRA study. It is retained in this discussion only for the sake of tradition." ASME R-SA-2002 divides IEs into transients, LOCAs, Interfacing System LOCAs (ISLOCAs), special initiators (e.g., support system failures), and internal flooding events. By focusing on radiation sources and equipment or systems that are required to contain radioactive materials from being released, the GC PSA identifies IEs in all five areas identified in ASME RA-S-2002. It is not clear if these events in the GC PSA include the events that could occur at shutdown or low-power operation, refueling accidents, or events resulting in a controlled shutdown as recommended in ASME RA-S-2002. The lack of adequate discussion regarding shutdown, low-power operation, and refueling IEs is viewed as a weakness.

After the IEs are identified, the safety functions necessary to prevent core damage are developed.

In the GC PSA, IEs with ten or more occurrences are classified as commonly occurring events (Section 4.2.6.1, Commonly Occurring Events). Rare events are IEs that occur one to ten times over the operating history or analyzed time frame (Section 4.2.6.2, Rare Event Occurrences). The IE frequencies are derived from CANDU operating experience and fault tree analysis. However, based on ASME RA-S-2002, it is unknown if plant availability is accounted for in the frequency, if any screening criteria were used, and if generic data for rare events were used. As far as this report is concerned, the lack of discussion regarding accounting for availability in the IE frequencies, the use of screening criteria, and use of generic data is viewed as a weakness.

Section 4.2.6.4 (Chi-Square Approximation) in the GC PSA further state that

> Component failures within a mature system occur randomly, but at a rate that is approximately constant with time. This behavior, which applies to failures that occur frequently, can also be assumed to apply to less frequent 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 limit for rare events. This method also provides a method for estimating these parameters for zero failures.

The use of the Chi-square distribution calculations for infrequent and randomly distributed data is subjective (Section 4.2.6.4, Chi-Square Approximation). Many distribution functions are available for use for random *continuous* functions or variables (data). The most commonly used is the normal (Gaussian or bell-shaped) distribution, which is useful if the number of observations in the sample is large. Other common distributions are the half-normal, the bivariate, the gamma (a special case of which is the Chi-square), the beta, the log-normal, the Rayleigh, the Cauchy, the exponential, and the Weibull. The gamma distribution is usually applied for random variables that are bounded at one end (e.g., 0 to ∞). According to NUREG/CR-2300, Section 5.3.1.1.1, "The gamma gives the distribution of time required for exactly k independent events to occur, assuming a constant rate of occurrence." The log-normal distribution is used when the logarithm of the variable (data) follows a normal distribution. The exponential distribution is the most commonly used time-to-failure distribution.

Similarly, there are many distribution functions that describe *discrete* variables (or data). The more commonly used distributions for discrete data are binomial, hypergeometric, geometric, Pascal, and Poisson distributions. Theoretically, there are an infinite number of probability distributions that could be used to describe the uncertainty in a basic event's probability. However, as indicated above, PRA analyses typically use the log-normal distribution while most of the others (e.g., Rayleigh, Cauchy) are not often used in NPP PRAs.

Uncertainty is treated in the same manner as randomly distributed data (Section 4.2.6.5, Treatment of Uncertainty). That is, the uncertainty (or error factor) for rare events as determined from CANDU operating experience is calculated using a Chi-square distribution. The error factor for events with more than 10 occurrences is 3. However, care must be taken when using the chi-square distribution for the uncertainty, because a credible uncertainty distribution may be broader than suggested by the chi-square confidence bounds if issues such as the applicability to the ACR-700 design of generic data, plant-to-plant variability, etc. are taken into account.

Event tree development

The event trees order and depict the safety functions according to the mitigating requirements of each group of IEs (Section 4.3, Event Tree Development). In constructing the event tree, the analyst considers the functions required to prevent core damage, potential consequences, and the relationships between safety functions. The CANDU event trees are developed from function event trees and are quantified by the method of fault-tree linking. The development of event trees is discussed in NUREG/CR-2300, Sections 3.4.4–3.4.5. More specifically, NUREG/CR-2300 discusses ordering of event trees and states that "A good starting point is the time of response . . . However, the time of response alone is not a sufficient basis for ordering headings." ASME RA-S-2002 states "where practical, sequentially order the events . . . according to the timing of events." The CANDU methodology appears to set the event sequences based on a time of response. This is not necessarily a limitation or error (it is not crucial to the analytical results), but it can be very important to the efficiency and brevity of the analysis.

Two sets of event trees are developed in the PSAs for CANDU plants. The first set of event trees is 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 terminate on a success state, a damage state in which the reactor core has disassembled (severe core damage), or a lesser damage state, that is, damage either to fuel bundles or to a limited number of channels within the core. To effectively interconnect Level I and Level II PRA activities, the CANDU PSA considers failures of containment mitigating systems, in addition to considering the state of the core. This is accomplished by creating a second set of event trees, which also consider the availability of containment systems whose availability can affect the accident progression analysis. These trees are called extended Level I event trees. They are identical to the Level I event trees, up to and including the failure of the last system that can prevent severe core damage. The event tree is then extended, by questioning the availability of containment mitigating systems at the end of these sequences.

ASME RA-S-2002 states that analysts should "use generic thermal hydraulic analyses . . . to determine accident progression parameters." The GC PSA uses these deterministic analyses to prepare the event trees when the information is available. In those cases where analyses must be performed to support the event tree development, AECL identifies as "PSA support analyses" to indicate that further analyses are required.

ASME RA-S-2002 discusses dependencies that can impact the ability of the mitigating systems to operate. Items to be addressed include identifying the mitigating systems, identifying dependence, phenomenological conditions created by the accident progression, split fractions, and time-phase dependencies. Although all of these are not specifically addressed in the GC PSA, the evaluations must be performed to identify the end states of the event trees (e.g., success, plant damage states, and severe plant damage states).

Mitigating systems are addressed by fault trees underlying the top events of an event tree (Section 4.3.2.4, Mitigating Systems). The modeling of the systems include both running failures as well as starting failures. However, this section states,

> 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.

Most PSAs for U.S. LWRs treat two (or more) redundant systems individually the same. The repair time is addressed in other areas, and without a more detailed description provided in the report or a review of the references, it is not possible to compare the two methods; this is viewed as a weakness of the report.

ASME RA-S-2002 states that the minimum mission time should be 24 h. The GC PSA typically uses a mission time of 24 h, but has IEs where the mission time could be 72 h or 1 month. However, the success criteria for the IEs with supporting engineering bases, as called out in ASME RA-S-2002, are not provided in the GC PSA. This appears to be attributable to the scope of the GC PSA rather than an omission by AECL.

A truncation limit of 1×10^{-10}/year is used in accident sequence quantification (Section 4.3.4, Event Sequence Termination). The rationale is that "Since the expected summed SCDF is on the order of 1×10^{-6}/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." ASME RA-S-2002 allows screening out of IEs if the IE is $<1 \times 10^{-7}$/year when the event does not involve either an ISLOCA, containment bypass, or a reactor vessel rupture; or 1×10^{-6}/year and core damage could not occur unless at least 2 trains of mitigating systems are failed independent of the initiator. Because it is unknown how the GC PSA algorithm works or the sequence of truncating sequences (i.e., if the sequences are truncated once the cut off value is exceeded even if all event tree tops and fault trees have been evaluated), the validity of their statement cannot be addressed. The concern is that subtle dependencies between two (or more) systems could be missed. A review of the sensitivity studies that were performed would answer this question.

System reliability analysis

NUREG/CR-2300, Section 3.5 covers system reliability analysis and fault tree modeling and addresses the specification of the analysis ground rules. Elements of a fault tree include component-failure characteristics, testing and maintenance, human errors, and dependent failures. ASME RA-S-2002 requires that "the system analysis provides a reasonably complete treatment of the causes of system failure and unavailability modes in the initiating events analysis and sequence definition." The GC PSA methodology document states that the methodology to be used in the fault tree analysis of CANDU plants follows that described in CNSC Consultative Document C-70[16] and NUREG-0492[17] (Section 4.4, System Reliability Analysis). Because no further details are available, an assessment of the method to develop fault trees cannot be made.

The fault-tree coding schemes used as inputs to various qualification codes in NUREG/CR-2300, Section 3.5.4 reference an eight-digit event identifier nomenclature. ASME RA-S-2002 simply states that analysts need to "develop system model nomenclature in a consistent manner to allow model manipulation and to represent the same designator when a component failure mode is used in multiple systems or trains." The GC PSAs uses a 16-digit identifier (Section 4.4.5, Fault Tree Event

Nomenclature). This effective labeling scheme is helpful in interpreting the results of the computer analysis. However, the use of a 16-digit identifier does not reduce the importance of a complete text description.

Dependent failure analysis

(See Section 4.3, Dependent Failure Analysis.)

Human reliability analysis

(See Section 4.4, Human Reliability Analysis.)

Database development

Data for component reliability is obtained from operating CANDU plants, in particular OPG's generating stations, Institute of Electrical and Electronic Engineers (IEEE) Standard 500,[18] and the nuclear plant reliability database system (NPRDS)[19] (Section 4.7.2, Component Reliability Database). Although none of these sources (IEEE Std. 500 and NPRDS) were reviewed and the veracity of the data was not confirmed, the age of the data is viewed as a weakness (1984 and 1983 respectively).

Accident sequences quantification

The modularization process is said to reduce the time spent reviewing the cut sets, but this process is not presented in the GC PSA (Section 4.8.2.6, Modularization). For example, "By implementing the modularization technique, the analyst can greatly reduce the number of cutsets that require review." However, that is the extent of the information regarding the technique. So, the concept is explained, but the technique is not presented. Therefore, an assessment of how to employ the process, (or even more importantly, how to analyze the process) is not possible.

Plant damage state analysis

(See Section 4.10, Level II PSA.)

Uncertainty analyses, sensitivity analyses, and quality assurance

The identification, evaluation, and comparison of uncertainties are important because they provide a deeper insight into the risk analyses, add to the credibility of the results, and aid in the process of decision making. Uncertainty analysis can be performed qualitatively or quantitatively. Sensitivity analysis is often a useful adjunct to uncertainty analysis.

The GC PSA and NUREG/CR-2300 identify the major sources of uncertainty as

1. completeness of the analysis,
2. uncertainties in modeling, and
3. parameter value uncertainty.

Completeness uncertainties are related to the inability of the analyst to evaluate exhaustively all contributions to risk. They refer to the problem of assessing what has been omitted and might be regarded as a type of modeling uncertainty. Modeling uncertainties stem from inadequacies in the various models used to evaluate accident probabilities and consequences and from the deficiencies of the models in representing reality. Parameter uncertainties arise from the need to estimate parameter values from data. Such uncertainties are inherent because the available data is usually incomplete and the analysts must make inferences from a state of incomplete knowledge.

The GC PSA describes uncertainties with respect to the completeness of the analysis as uncertainties in the conceptual understanding of systems, processes, and their interactions that can lead to the omission of potential contributors or to the inclusion of unrealistic contributors to the risk. NUREG/CR-2300 agrees by stating that "The quantification of uncertainty on the completeness of a PRA is a difficult and paradoxical problem . . . because it requires the quantification of all possibilities for incomplete descriptions and models and their probabilities within an already complex PRA calculation. . . the logical assessment of what one knows and what one does not know is not formally well structured." When the GC PSA states that "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," it is in agreement with NUREG/CR-2300 that concludes "the quantification of completeness is not feasible for PRA calculations."

Modeling uncertainties reflect the limitations of knowledge regarding the phenomenological progression through the plant systems and the human response to abnormal conditions. 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 modeling process manageable. The GC PSA addresses modeling uncertainties "by making conservative modeling assumptions in the safety analysis." The problem with using "conservative modeling assumptions" to address modeling uncertainties is that an analyst does not always know that the assumptions are, in fact, conservative. Modeling uncertainties should be addressed through sensitivity analysis. Current regulatory practice is to address uncertainty in PRA results by applying defense-in-depth concepts.

The term "parameter uncertainties" refer to parameters that possess a significant natural random variability and whose characteristics can be represented probabilistically. Parameters of interest include failure rates, component unavailabilities, IE frequencies, and human error probabilities. The GC PSA quantifies the uncertainties using the UNCERT program. This program determines the uncertainty of system failure probabilities or accident sequence frequencies for the PRA based on model input uncertainties. A Monte Carlo technique is used for the calculations. According to the GC PSA,

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

This is consistent with NUREG/CR-2300 that states that the "Monte Carlo method presents the most direct approach to the problem of uncertainty propagation when input uncertainties are represented as distributions on parameters. . . Monte Carlo simulation thus constructs an approximation to the output-variable probability distribution."

The sensitivity analyses for the GC PSA are carried out with the following objectives in mind:

1. to test the sensitivity of PRA results to certain changes in key input assumptions, and

2. to optimize the design by highlighting systems or subsystems that are especially large contributors to risk.

Because "it is difficult to provide a detailed list of items to be covered in a sensitivity analysis for a generic methodology," a sensitivity analysis will be performed on a specific plant when the initial accident sequence quantification is complete. When this is completed, the results of the importance analysis will be used to select items for the sensitivity analysis. The sensitivity of results is tested for key aspects of the analysis, i.e., different maintenance practices, testing procedures, and mission time. NUREG/CR-2300 states the "Sensitivity studies can be particularly useful for assessing the impacts of different models, system-success criteria, and the like." Thus, it appears that the GC PSA, with its focus on performing sensitivity analyses on human-related errors, should be expanded to include assessing the impacts of different models, system-success criteria, etc. The lack of information regarding sensitivity studies assessing the impacts of different models, system-success criteria, etc. is viewed as a weakness.

According to NUREG/CR-2300, "the most important contribution to quality comes from the practices followed by the team conducting the PRA." These practices fall into five general areas: planning, methods, internal review, documentation, and computer codes. Planning, methods, and computer codes are discussed throughout the GC PSA. Quality assurance for the GC PSA is assured by using the following methods:

1. the analyst’s informal day-to-day record keeping (comparable to planning in NUREG/CR-2300),
2. project operating instructions (comparable to methods in NUREG/CR-2300),
3. a review of PRA work (comparable to internal review in NUREG/CR-2300),
4. an update of PRA methodology, and
5. archiving the results for repeatability where possible (comparable documentation in NUREG/CR-2300).

The GC PSA notes that a thorough review of the PRA is performed by the team leader who reviews all aspects of the PRA work, the PRA analysts, relevant system designers, and external review by other experts within AECL. NUREG/CR-2300 indicates that to achieve quality in general, reviews should be performed not only by those indicated in the GC PSA but by managers as well. The management review should concentrate on perspective, scope, and product suitability in meeting program objectives. In addition, the reports from the peer review should be a part of the management review.

4.2.2 Strengths and Weaknesses

Overall, the methodology for performing an internal events PRA is consistent with that used in NUREG/CR-2300 and the high-level requirements of ASME RA-S-2002.

Section 4 and Appendix A provide a fairly complete presentation of the information. However, many times a representative example or calculation would have enhanced the reader’s understanding of the methodology. It is considered to be a weakness that in numerous cases, details of the methodology are provided in other reports[19-27] and not in the CANDU methodology report. For example, an adequate description is necessary to understand and evaluate AECL’s modularization process as it is applied to accident sequence quantification. Another example is the sample calculation in Appendix A—the example calculation in Appendix A is not detailed enough to duplicate the end results. The plant success states and mission times are fully developed and easy to follow. The component types, boundary descriptions, failure modes, and mechanisms are fully developed and easy to review.

The use of the Chi-square distribution is thought to be a weakness. Furthermore, a Chi-square distribution is considered more appropriate for large sample sizes; a sample with less than ten events is not "large." The use of the Chi-square distribution calculations in Appendix A is not considered appropriate for exponentially distributed data described in Section A.1. As in the preceding argument, the error factor determination for uncertainty needs a more thorough review.

Care must be taken when using the chi-square distribution for the uncertainty, because a credible uncertainty distribution may be broader than suggested by the chi-square confidence bounds if issues such as the applicability to the ACR-700 design of generic data, plant-to-plant variability, etc. are taken into account.

4.3 Section 5, "Dependent Failure Analysis"

Operating experience and current PSAs show that dependent failures are extremely important in risk quantification and must be given adequate treatment to avoid a gross underestimation of risk. Dependent failures are those failures that defeat the redundancy or diversity that is used to optimize the availability of some plant functions. Thus, dependencies increase the frequency of multiple, concurrent failures—meaning that risk estimates can err by many orders of magnitude if the possibilities for common-cause failures and systems interactions are overlooked.

According to NUREG/CR-2300,

> It is a well-known characteristic of common-cause failures that, if the cause or causes are shared by two or more components in the same minimal cut set, the assumption that the component unavailabilities are independent leads to optimistic predictions of system reliability. It is not so well known that, if the dependence exists between two or more units in a series system (i.e., in different minimal cut sets), the assumption of independent failures can lead to conservative predictions, depending on how the data are analyzed. However, the former effect is more important and can lead to considerably larger errors in calculations for highly reliable redundant systems.

According to NUREG/CR-2300, a dependent failure analysis consists of the following two tasks:

4. definition of dependent failures, and
5. method of dependent failure analysis.

4.3.1 Methodology

<u>Definition of dependent failures</u>

Dependencies tend to increase the frequency of multiple, concurrent failures. Dependent failures are those failures that defeat the redundancy or diversity that is used to optimize the availability of some plant functions. The GC PSA defines dependent failures as involving two types of relationships:

1. explicit dependencies between components or systems, and
2. failure mechanisms that affect more than one component, but that are not explicitly identified in the systems analysis.

NUREG/CR-2300, Section 3.7, identifies the following three specific types of dependent failures:

1. common-mode failures─multiple, concurrent, and dependent failures of identical equipment that fails in the same mode;
2. propagating failures─when equipment fails in a mode that causes sufficient changes in operating conditions, environments, or requirements to cause other items of equipment to fail; and
3. common-cause failures (CCFs)─the occurrence of multiple-component failures induced by a single, shared cause.

Numerous explicit dependencies are taken into account in the processes of event tree development, system reliability analysis, and accident sequence quantification. The GC PSA breaks these dependencies down into the following main categories:

1. Functional dependencies: dependencies among systems or components that follow from the plant design philosophy, system capabilities and limitations, and design bases.
2. Physical interactions: physical phenomena (e.g., severe environmental conditions) that can impact multiple systems and components.
3. Human interactions: preaccident and postaccident operator actions.

"Apart from the explicitly modeled dependencies described above, historical component reliability data indicate that a variety of additional causes can render multiple redundant components simultaneously unavailable." Because of the rarity of these CCFs, "it is difficult to obtain frequency of failure estimates for each cause. Furthermore, it is difficult for the systems analyst to ensure that all possible causes are individually taken into account, and it is impractical to include many CCF events in the fault trees. For these reasons, CCFs are modeled implicitly, in the sense that a single fault tree basic event is used to capture all of the possible causes. Identically labeled CCF events are introduced as inputs to an 'OR' gate, adjacent to each redundant component's independent failure modes to model the failure dependency. The failure rate for these events is usually based on the total component failure rate and a number of additional parameters that are derived from generic CCF data and expert judgments."

NUREG/CR-2300 has a category of dependent failures called intersystem dependencies (called inter-system CCFs in ASME RA-S-2002). Intersystem dependencies are defined as those events or failure causes that create interdependencies among the probabilities of failure for multiple systems. Intersystem dependencies include *functional dependencies*, *shared-equipment dependencies*, *physical interactions*, and *human-interaction dependencies*.

However, in addition to intersystem dependencies, NUREG/CR-2300 defines two other categories of dependent failures:

- Common-cause initiators: events that have the potential for initiating and influencing the progression of accident sequences.
- Intercomponent dependencies: events or failure causes that result in a dependence among the probabilities of failure for multiple components or subsystems. These intercomponent dependencies are defined to correspond with the intersystem dependencies of *functional dependencies*, *shared-equipment dependencies*, *physical interactions*, and *human-interaction dependencies*, except that the multiple failures occur at the subsystem and component level instead of at the system level.

Method of analysis

The recommended procedure in the analysis of dependent failures in NUREG/CR-2300 consists of a method or synthesis of methods for each type of dependent failure as given in Table 2.

The GC PSA method uses the Unified Partial Method (UPM) to quantify the CCF probabilities.

Table 2. Recommended Methods in NUREG/CR-2300 for the Analysis of Dependent Failures

Method	**Dependent-failure type**					
	CCF-IEs	**Intersystem functional dependencies**	**Intersystem shared equipment**	**Intersystem physical interactions**	**Intersystem human interactions**	**Inter-component dependencies**
Event-specific models	✔✪			✔✪		✔
Event-tree analysis	✔	✔✪	✔✪		✔✪	
Fault tree analysis	✔	✔	✔✪	✔	✔✪	✔✪
Cause-table analysis				✔	✔✪	✔✪
Human-reliability analysis				✔	✔✪	✔
Beta factor						✔✪
Binomial failure rate						✔✪
Computer-aided analyses	✔✪		✔✪	✔✪		✔

✔ = Method suitable for identifying dependent failures.
✔✪ = Method recommended in NUREG/CR-2300, Section 3.7 for identifying dependent failures.

According to the GC PSA method, the CCFs can be quantified in one of two ways: (1) the CCFs can be evaluated at the system level by estimating a system cut-off probability, or (2) a beta-factor can be estimated from sets of similar components. NUREG/CR-2300 recommends, among others, the beta-factor method for evaluating intercomponent dependencies. However, it is recognized that more current techniques are available for evaluating dependent failures.

Because of limited information on the UPM method, the following screening and analysis methods from the GC PSA methodology report are excerpted here (Section 5.3.4, Calculation of Beta Factors):

> Having identified a common cause component group and created an appropriate fault tree basic event, the analyst must then calculate a beta factor, and hence, a basic event probability. Since the UPM incorporates an in-depth qualitative assessment for each component group, the time required by the analyst to document his or her assumptions,

and to fill out the UPM judgment tables to arrive at a beta factor may be substantial. Therefore, a quantitative screening shall be performed before applying the UPM directly.

NUREG-CR-4780[28] suggests using a quantitative screening value of $\beta = 0.1$ for each CCF basic event. NUREG/CR-5485[29] provides quantitative CCF screening parameters greater than the 0.1 value mentioned in NUREG/CR-4780. The 0.1 value should be conservative for most situations, although conservatism is not the main objective of the screening. The intent is to help the analyst to identify the common cause component groups that contribute most to the top event unavailability of a given fault tree. This determination can be made by examining the top 100 minimal cut sets or, alternatively, by examining the importance measures of the fault tree solution. Then, the probabilities of the selected CCF events can be refined using the UPM procedure, and the fault tree can be re-evaluated.

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

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

1. The system to be analyzed must be clearly defined. It is necessary to define the physical boundary of the system, i.e.: the components and parts of the system that are to be considered in the analysis. See Section 5.3.1 for further discussion of this step, which is not unique to the UPM.
2. The level of assessment must be established. Is the CCF analysis to be carried out at a system (cut-off) level, or at a component (partial beta factor) level? For CANDU 6 and CANDU 9 PSAs, a component level assessment is appropriate, because system reliability calculations will be made using detailed fault trees. See Section 5.2 for further information.
3. The judgement tables must then be consulted for each subfactor. Each table relates to a different aspect of system design or operation, including its effectiveness in defending against CCF. Out of the five system descriptions that are listed in the tables, the analyst must choose the description that most closely matches the system under consideration. The justification for the choices must be recorded in tables for each CCF component group, using the format shown in Table 5-1.
4. The estimation table, which summarizes the judgements made in the previous step, must then be filled in. This step can be combined with step three, by obtaining the numerical values for each subfactor from the UPM estimation table, and by entering the information in Table 5-1. This step constitutes the bulk of the analysis.
5. Finally, the value of the system cut-off or component beta factor is to be calculated, as appropriate. After obtaining the beta factor, the CCF probabilities should be calculated, and the values should be incorporated into the fault tree, in order to replace the screening values. The fault tree should then be reevaluated to obtain the final result.

These five main steps appear to meet the high-level requirement in ASME RA-S-2002 of providing a reasonably complete treatment of CCFs and intersystem and intrasystem dependencies.

Section 5.1.1 (Selection of CCF Analysis Method) states that "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." According to NUREG/CR-2300, the limitations and uncertainties associated with attempts to analyze CCFs can be largely attributed to a lack or a scarcity of data. The analysis of field-experience data is also the most effective and defensible way to establish the degree of dependence among the causes of multiple failures, to estimate the conditional frequencies of CCFs (e.g., beta factors), or to estimate multiple-failure frequencies directly, depending on the type of the model.

The beta-factor method can be used to model dependencies between dissimilar and not necessarily redundant equipment. In practice, however, it is most often applied to systems for which the most data is available—systems with redundant and identical equipment. The beta-factor method models dependent failures of two types: intercomponent physical interactions and human interactions.

AECL obtains generic beta factors from NUREG/CR-2098,[30] NUREG/CR-2770,[31] NUREG/CR-3289,[32] and NUREG-0666[33] (Section 5.3.5, Component Types and Boundaries). This data may be outdated because it nominally covers information from 1972–1981. In addition, the nuclear industry NPP population is much different today. Most of the plants in operation during the 1970s were older plant designs; numerous plants in operation at that time have since been permanently shutdown. The use of 20-year old data from an industry that has changed significantly during this time is considered to be a weakness. The current industry population has a very different makeup, and this should be accounted for. The U.S. NRC Regulatory Issue Summary regarding New Generic Issue No. 145[34] recommended that U.S. NRC Administrative Letter (AL) 98-04[35] be followed. AL 98-04 indicates that CCF data collection should be obtained from NUREG/CR-6268[36] and that CCF parameter estimation should follow NUREG/CR-5497.[37] The data in these two documents cover CCF events from 1980–1995. NUREG/CR-5485,[29] which is considered to be an update for NUREG/CR-4780,[28] should also be consulted in conjunction with CCF probability determination.

The GC PSA states that types of components listed in GC PSA Table 5-2 (motor-operated valves, air-operated valves, pumps, air compressors, air coolers, heat exchangers, batteries, diesel generators, and switches/transmitters) are to be modeled as part of the CCF analysis. That is, these components are active and appear in nondiverse, redundant structures within CANDU plants. According to the GC PSA, these entries are not intended to be an exhaustive listing for all projects, but rather a minimum requirement based on the types of components for which generic beta factors have been collected from the four NRC reports listed above. Other components covered in NUREG/CR-5497[37] that are not listed in GC PSA Table 5.2 are circuit breakers, check valves, strainers, relief valves, and safety valves. As far as reporting is concerned, the lack of adequate discussion whether these components are covered in the GC PSAs is considered to be a weakness.

AECL indicates in Section 5.3.6.3 (Interface with Human Reliability Analysis) the following:

> Since the UPM is designed for CCF analysis at both the system level and the component level, certain explanations in the manual are ambiguous. The text that refers to operator actions is very much geared to systems, because extensive mention is made of written procedures for system operation and checklists. Human actions that can cause unavailability of redundant components shall be modeled explicitly using HRA methods. Therefore, the MMI sub-factor shall be assigned a value of zero.

If AECL updates its UPM values with NUREG information, they would need to justify the use of this data. Regardless, AECL should fully document the implementation of the UPM in its PSA.

The UPM attempts to quantify the human contribution to CCFs through two of its subfactors: the man-machine interface (MMI) and safety culture subfactors. Because there is a potential overlap with human reliability assessment (HRA) methodologies within the MMI subfactor, AECL indicates that the analyst must take care to avoid double counting. The MMI subfactor is derived from two evaluations. One is performed for maintenance actions, and the other is performed for operator actions.

Section 5.3.6.4 in the GC PSA, (Interface with External Events PSA), states

> ...component unavailability due to certain causes is modeled explicitly, in order to arrive at plant damage frequency estimates. Ideally, then, these failure causes should be screened out from the CCF analysis to avoid double counting. Unfortunately, the nature of the UPM makes it difficult to do so. Since the subfactors are not generally based on cause, but instead on CCF deficiencies, it is difficult to break down the beta factor, in order to eliminate these events as contributors. . . A conservative approach shall be taken, in that no attempt will be made to screen out any overlap between the CCF analysis and the internal and external events analysis. The UPM will be applied without modification.

The GC PSA further indicates that the method described in the manual for the UPM method[38] is not suitable for large *m* and *n* in assessing *m* out of *n* successes (Section 5.3.6.6, High Levels of Redundancy). The UPM manual suggests mapping "*m* out of *n* to 1 out of (n-m+1), but only for $n \leq 5$;" this limits the effective range and reliability of analysis using this method and is considered to be a weakness.

Specifically, the GC PSA methodology states

> The particular *m* out of *n* success criterion affects the beta factor calculation (under the redundancy subfactor), but the fault tree model does not explicitly contain combinations of lower order failures. That is, if 7 out of 16 is the success criterion, the only fault tree CCF event will still be for all sixteen items being failed. 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 cut set that includes two CCF events for identically redundant components implies that the root cause of each event in the cut set is different (e.g., one CCF is maintenance related, the other is due to a harsh environment). The likelihood of this occurring would seem to be negligible, when compared with one root cause impacting all of the components.

According to NUREG/CR-2300, the beta-factor method is most useful for analyzing dependent failures in systems with limited redundancy (two or three units). For systems with more than two units, the beta-factor model does not provide a distinction between different numbers of multiple failures. This simplification can lead to conservative predictions when it is assumed that all units fail when a CCF occurs. Thus, the UPM method allowing up to five redundant "units" appears to overrun the capabilities of the beta-factor method that is its foundation (as noted above, being limited to ≤ 5 redundant units is considered to be a weakness). However, this issue is not specific to the UPM and the application of the beta-factor approach to highly redundant systems is generally believed to be conservative.

4.3.2 Strengths and Weaknesses

Section 5 is very detailed for the material that is presented. However, there are too many generalizations to perform an adequate review. Also, there is a lack of examples using the UPM in estimating CCF.

The UPM method is not fully described in the GC PSA (Section 5.2, Main Features of UPM). The "UPM Workbook" (Reference 38) is a company proprietary document. Because there is no CANDU-specific data for CCF, analysts assign beta-factors based on generic CCF data obtained from other sources such as PWRs and BWRs. AECL states that the UPM is "...preferable to using published data for parameters of other CCF models, such as the Multiple Greek Letter (MGL) technique." The UPM is a refinement of the partial beta-factor method; however, instead of decomposing the judgements into 19 groups, they are decomposed into 8 causal groups, with 5 system definitions to choose from.

AECL states that it will follow NUREG/CR-4780[28] for selecting the appropriate CCF component groups (Section 5.3.1, Selection of Common Cause Component Groups). This consolidation reduces the amount of analysis and time required for the particular CCF model (e.g., UPM vs MGL) employed in the analysis. However, in applying a refined partial beta-factor method some second-order cutsets may be lost. AECL states that retaining second-order cut sets "can lead to a proliferation of cutsets, without significantly altering the calculated system reliability" (Section 5.3.1, Selection of Common Cause Component Groups). The GC PSA notes that the loss of the physically meaningful second-order cut sets is an artifact of all beta-factor CCF techniques and that MGL and other methods have the advantage of preserving such combinations, by taking into account partial CCFs out of a larger group.

AECL notes that HRA interactions have the potential for double counting because the MMI and safety subculture subfactors overlap. Section 5.3.6.3 (Interface With Human Reliability Analysis) does not propose how to overcome this deficiency; therefore, this is viewed as a shortcoming for this part of the methodology.

The GC PSA indicates that staggered testing is not addressed in the UPM method (Section 5.3.6.5, Staggered Testing). Staggered testing should be accounted for, and without it the method has an inherent weakness in this regard.

Although the evaluation of external events is mentioned, it is not known if the event-specific models were used in conjunction with computer-aided analyses to identify IEs. The same combination is recommended in NUREG/CR-2300 for identifying physical interactions. Again, if this was done, the extent that computer-aided analyses was used in the GC PSA is unknown. Because event trees and fault trees alone can be used to identify CCFs in all six categories in Table 2, all CCF-type interactions will be identified. However, the best methods to identify specific types of CCF interactions were not used. The lack of information on identifying IEs, physical interactions, and computer-aided tools for performing the analyses is considered to be a reporting weakness.

The process of selectively reducing the number of causal groups and CCF component groups is consistent with the NRC-proposed Phenomena Identification and Ranking Table (PIRT) method as described in SECY-03-0059.[39]

4.4 Section 6, "Human Reliability Analysis"

In a PRA, it is necessary to consider the human tasks that are performed under normal operating conditions and those performed after accidents or abnormal occurrences. In the former situation, errors might be made during or after maintenance, calibration, testing, or in the normal operation of the plant. In either situation, most of the errors identified and analyzed in HRAs are those made in following plant procedures (written, oral, or standard shop practice).

The HRA method recommended and most fully described in NUREG/CR-2300 employs the "Technique for Human Error Rate Prediction" (THERP) that is described in NUREG/CR-1278.[40] ASME RA-S-2002 indicates that THERP is an acceptable method for estimating the probability of human events. According to NUREG/CR-2300, there are four phases of HRA: familiarization, qualitative assessment, quantitative assessment, and incorporation.

The HRA for the GC PSA generally follows NUREG/CR-1278, referred to as the "Handbook" in NUREG/CR-2300. The GC PSA classifies the different types of human actions into three categories:

1. preaccident human actions,
2. human actions that lead directly to IEs, and
3. postaccident human actions (procedural safety actions, aggravating actions, and recovery actions).

ASME RA-S-2002 lists only categories 1 and 3.

The HRA techniques described in the GC PSA and NUREG/CR-2300 divide the HRA into the following categories:

1. familiarization,
2. classification of tasks,
3. qualitative analysis,
4. quantitative analysis, and
5. recovery analysis.

4.4.1 Methodology

Familiarization

Familiarization is not explicitly discussed in Section 6 (Human Reliability Analysis); however, because it is discussed in Sections 3 (PSA Methodology—General) and 4 (Internal Events PSA), it is assumed that the human error probability (HEP) analyst is familiar with the plant, its documentation, and has had discussions with operators and plant personnel.

Classification of tasks (definitions)

In accordance with the Accident Sequence Evaluation Program (ASEP) for HRA (NUREG/CR-4772),[41] three different behaviors are modeled for human actions in the GC PSA: (1) skill-based; (2) rule-based; and (3) knowledge-based. This reference (NUREG/CR-4772) is a simplified version of NUREG/CR-1278.[40] These are the same definitions used in the GC PSA. Both NUREG/CR-4772 and NUREG/CR-1278[40] are acceptable methods in NUREG/CR-2300 and ASME RA-S-2002.

Qualitative analysis

The extent of elucidation of talk-throughs given in the GC PSA methodology is "In the evaluation of preaccident tasks for an existing plant design, the calibration, test and maintenance procedures and practices are reviewed for each front-line and support system." NUREG/CR-2300 states that "talk-throughs of the procedures in question are an important part of any human-reliability analysis. . . Performance specifics are identified along with any time requirements, personnel assignments, skill-of-the-craft requirements, alerting cues, and recovery factors." Thus, although the GC PSA, NUREG/CR-2300, and ASME RA-S-2002 agree on reviewing procedures, the lack of information regarding the GC PSA review means that an assessment of the completeness of this subtask cannot be made. Because walkdowns and talk-throughs are not feasible for the ACR-700, it is reasonable to expect that AECL will perform a minimal qualitative analysis and use conservative HEPs.

ASME RA-S-2002 allows human error activities to be screened out based on an assessment of how plant-specific operational practices limit the likelihood of errors in such activities. It is unknown if such an activity is undertaken in the GC PSA.

Preaccident tasks may include elements of skill-based, rule-based, or knowledge-based behavior. Modeling only rule-based behavior in the GC PSA, when assessing preaccident tasks, is considered to be a weakness. The ASEP HRA Procedure given in NUREG/CR-4772 presents a simplified model of human behavior for preaccident tasks.

Quantitative analysis

The human-error probabilities estimated using the "handbook" values for a given task must be modified to reflect the actual performance situation. According to NUREG/CR-2300,

> A primary consideration in conducting a human-reliability analysis is the variability of human performance. This variability is exhibited by any given individual in the performance of tasks over time . . Variability also results from the performances of different personnel . . . Variability is caused by performance-shaping factors (PSFs) acting within the individual or on the environment in which the task is performed. Because of this variability, the reliability of human performance usually is not predicted solely as a point estimate but is determined to lie within a range of uncertainty.

The GC PSA (Section 6.3.3, Performance Shaping Factors) states that "PSFs, other than recovery factors, dependence effects and radiation, are implicitly included in the (basic human error probabilities) BHEP and assume average, or better human factors or conditions. Radiation is explicitly considered as a PSF in the pre-accident screening HRA." The lack of details precludes a review of the adequacy of what was done; however, note that there is no mention of uncertainties in the GC PSA sections on HRA. Not addressing HRA uncertainties in the section of HRA is contrary to the other sections in the GC PSA because uncertainties are evaluated in each individual task; thus, this is considered to be a weakness.

The dependence between two tasks or activities refers to the situation in which the probability of failure for one task is influenced by the success or failure that has occurred for the other task. The dependence may exist between two tasks performed by the same person (within-person dependence), or between the same tasks performed by different persons (between-person dependence).[42]

Although dependence is a continuum, it is discretized for practical reasons into a number of levels, which vary from two levels (zero dependence and complete dependence) in the *ASEP HRA Procedure*,[41] to five discrete levels in the *Handbook of Human Reliability*.[42] Dependence effects in the GC PSA development follows NUREG/CR-1278, but uses four levels of dependence, from zero (no) dependence to complete dependence (Section 6.3.5, Dependence Effects). Again, this contrasts with the five levels found in NUREG/CR-1278 and the two levels found in the ASEP.

According to NUREG/CR-2300, an estimate of the probability of each human-error event on the HRA event tree may be derived from the data tables in NUREG/CR-1278. Section 6.4.5 in the GC PSA, Human Error Probability for Execution Tasks, states that "The NHEPs (nominal HEPs) for postaccident execution errors are quantified based on ASEP methodology" from NUREG/CR-4772. "The common practice for determining the NHEP is to use the median values for HEP" in NUREG/CR-4550,[a] which include the effects of stress and complexity of the task. It is considered to be a strength that the GC PSA assesses the HEPs for the type of task and stress level based on the values in Table 8-5 of NUREG/CR-4772[41] and in Table 7.3-14 of NUREG/CR-4550.[43]

Post-Accident Operator Errors

Post-accident human actions typically pertain to activities that are performed by reactor operators who are stationed in the main control room and that take place after the onset of an IE. The total failure probability for a post-accident operator action is taken as the failure of the operator to correctly diagnose the event or the failure to correctly execute the actions that must be taken within the total allowable time.

Postaccident HRA in the GC PSA divides human actions into diagnosis and post-diagnosis tasks and develops coping times to determine the diagnosis and allowable execution time tasks. In addition, procedural safety actions are usually explicitly modeled and generally include diagnosis and execution of tasks. Aggravating actions are not always modeled and are considered errors of commission.

Post-accident tasks that are intended to implement mitigation measures for ensuring or maintaining adequate fuel cooling are divided into the following tasks:

- diagnosis—determination of appropriate actions when an abnormal event has been recognized, within the allowable time constraints, and
- post-diagnosis—execution.

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

- failure of the automatic actuation of the mitigating systems;
- successful automatic actuation of a mitigating system with a requirement for operator action to ensure continuing operation; and
- the absence of design features for automatic mitigating action.

In the GC PSA, post-accident operator actions are generally modeled in the event trees as separate decision branch points (top events) and are usually placed just before the top event of the associated

[a] NUREG/CR-4550, Vol. 1[43] (p. 7-2) states that "Each estimated HEP is assumed to represent a median value on a lognormal distribution of HEPs." NUREG/CR-1278[42] (p. 7-8) states that "These nominal HEPs are single-point estimates and represent the median of a lognormal distribution."

system that requires manual initiation. In some cases, post-accident operator actions are modeled in the system fault trees.

In some situations, following a correct diagnosis, execution errors or system failure will mean that the success criteria for a particular operator action are not met. For the subsequent operator action in this case, a new diagnosis HEP may be considered.

The operator's response in coping with an abnormal event may be classified as either

- dynamic—one that requires a higher degree of interaction between operators, or
- step-by-step—routine, procedurally guided set of steps that is performed one step at a time on one particular task at a time without a requirement to divide the operator's attention between the task in question and other tasks.

Post-diagnosis actions are also assessed as being performed under moderately high stress.

The NHEPs for post-accident execution errors are quantified based on the ASEP methodology given in NUREG/CR-4772.[41] The common practice for determining the NHEP is to use the median values for the HEPs given in NUREG/CR-4550.[43] Again, 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 and to correctly execute the actions that must be taken within the total allowable time.

The GC PSA also credits a second or third operator based on the time available (30–60 min) or the location (main control room or locally). For zero dependence, consecutive operator actions are simply assigned the calculated HEPs. For complete dependence between operator actions, 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 modeled in the event tree. For moderate dependence and high dependence operator actions, the conditional failure probability equations are based on Table 10-2 in NUREG/CR-1278.[42]

Recovery analysis

HEPs for recovery actions include the contribution of diagnosis errors and of execution errors, which are calculated according to the methodology for the quantification of post-accident operator errors. [6] Recovery analysis deals with the probabilistic evaluation of recovery actions, and is usually performed after quantifying the accident sequences at the cut set level. Recovery analysis is performed on sequence cut sets for a PDS, if the probability of that core damage state is higher than anticipated. The operator actions that are credited during recovery analysis are usually based on component or equipment failure at the cut set level.

The potential recovery actions for a cut set are based on the equipment and component failures in that cut set and are usually applicable to one specific failure in the cut set. 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).

According to NUREG/CR-2300, the incorporation of recovery factors can be done in stages, the purpose being to decrease the amount of time required for each analysis. Further, if the estimated probabilities for a given task sequence are sufficiently low without considering the effects of recovery factors (RFs) such that the sequence does not appear as a potentially dominant failure mode, it can be dropped from further consideration. ASME RA-S-2002 states that "recovery actions . . . shall be modeled only if it has been demonstrated that the action is plausible and feasible for those scenarios to which they are applied."

In the GC PSA HRA, RFs are applied for the following conditions:

- if the components' status is unavailable as shown in the main control room (MCR) or secondary control area (SCA), and indicated by an annunciator, alarm, or other indicator;
- when a components' status is verified by a postmaintenance (PM) or postcalibration (PC) test;
- when there is independent, written verification of a components' status; and
- if personnel perform periodic check/inspection of the components' status using a written checklist.

The determination of the applicable RFs in the GC PSA for the specific activity under review is based on the ASEP HRA Procedure, Table 5-3 in NUREG/CR-4772.

AECL indicates that the following steps are involved in recovery analysis:

- obtaining information for post-accident analysis.
- identifying recovery actions that are included in event trees and fault trees.
- developing accident sequence descriptions.
- determining sequence and cut set timing.
- identifying potential recovery actions.
- determining the available operator time.
- determining the operator performance time.
- selecting viable operator actions, and
- determining the HEP.

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

The GC PSA indicates that for various sequences, the available recovery action time is between 30 min and 40 h, depending on the parameter that tripped the reactor, and whether or not feedwater and condensate train is available. For events that jeopardize end shield cooling, the available operator action time depends on the calandria tubesheet thermal stress rather than on the feedwater supply to the steam generators.

The operator performance time is the time required by the operator to execute the recovery action.
A recovery action is considered to be viable if the time required to perform the action is smaller than the amount of time that is available to perform the action.

According to AECL, the maximum credit for the human error composite should not be greater than 1.0×10^{-5} when the time available is between 4–8 h, and should not be greater than 1.0×10^{-4}, when the operator has between 2–4 h to act.

For dominant sequences which contain operator error actions, the GC PSA indicates that the HEPs for the accident sequences may be re-evaluated using NUREG/CR-1278.[42] Alternatively, the paired comparison/expert judgement method given in NUREG/CR-3688[44] may be used.[6]

4.4.2 Strengths and Weaknesses

Section 6 is fairly detailed for the material that is presented. There are many examples, and the review found no inconsistencies or errors.

The HRA process is consistent with current HRA techniques and is easy to follow. NUREG/CR-2300 was published in January 1983. NUREG/CR-1278 was originally published in 1980. Thus, it makes sense that NUREG/CR-1278 is heavily referenced throughout NUREG/CR-2300. The documents cited frequently in the GC PSA are NUREG/CR-1278, NUREG/CR-4772, and NUREG/CR-4550. The latter two documents were published after NUREG/CR-2300 and thus were unavailable at the time NUREG/CR-2300 was published. NUREG/CR-2300 concludes with "The state of the art of human-reliability analysis is changing rapidly at present. New methods are being developed, and older models are being revised and updated to accommodate the type of information needed for a PRA. The users of this guide are urged to investigate recent developments in human-reliability analysis that are or will shortly be available." NUREG/CR-4550 and -4772 are more recent HRA documents than NUREG/CR-1278 and are referenced in ASME RA-S-2002. Because the GC PSA is a recent document, it would be questionable if it only used the data from NUREG/CR-1278 rather than from more recent publications. This is deemed to be an advantage.

The methodology in the GC PSA for HRA follows accepted practices outlined in NUREG/CR-1278, NUREG/CR-4772, and NUREG/CR-4550. For dominant sequences that contain operator error actions, AECL reevaluates the sequences using NUREG/CR-1278 to recalculate the HEP, or alternatively, the paired comparison/expert judgement method, given in NUREG/CR-3688.[44] Particular attention in the GC PSA is given to modeling the postaccident execution errors in accordance with international practice, based on the ASEP procedures given in NUREG/CR-4772. Further, the task classification scheme, presented in Section 2 of the ASEP HRA procedure given in NUREG/CR-4772, is adopted. Thus, the HRA methodology to be used for the GC PSA HRA follows accepted practices. It is considered to be a strength that the GC PSA follows accepted practices for calculating the HEPs, postaccident operator errors, and recovery factors.

Errors or omissions in the GC PSA include the lack of discussion on HRA event tree development, sensitivity analyses, no clear interaction with systems analysts, and no person-to-person dependencies.

Although the methodology described in the GC PSA details the quantitative assessment outlined in NUREG/CR-2300, little information is given on the front-end (familiarization and qualitative assessment) and back-end analyses (incorporation).

Because no discussion is given concerning the development of the HRA event trees, the incorporation of RFs is assumed to be directly into the system fault trees. If so, this implies that procedures are not broken down into specific steps. It is not understood how these RFs are incorporated into the PRA.

4.5 Section 7, "Seismic Events PSA" and Appendix B, "Methodology for Seismic Fragility Analysis"

Seismic excitation has the potential for simultaneously damaging several redundant components. These events also have the potential of causing 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 failure of "passive" components.[6] Thus, the purpose of a seismic events analysis is to identify the sources of earthquakes, evaluate the earthquake history, estimate the intensity of earthquake-induced ground motion, and determine the seismic hazard.

According to AECL, its seismic analyses "follow the generally accepted worldwide practice for conducting a SHA (seismic hazard analysis)." However, merely completing an SHA will not provide adequate consideration of the earthquake risk. In order to assess the risk from earthquakes, either a seismic margins analysis (SMA) or a seismic PRA (that includes, among other tasks, an SHA) is required. Performing these analyses requires AECL to select a representative site on which to base the SHA for a standard design certification. It is understood that AECL will perform an SMA for the ACR. NUREG/CR-2300 divides the probabilistic SHA into four main steps:

1. Determine the seismic source characterization.
2. Calculate the frequencies of occurrence of earthquakes of different magnitudes (recurrence).
3. Model the ground motion attenuation.
4. Produce a single seismic hazard curve by integrating the information, to derive the seismic hazard curve.

The GC PSA follows these same steps.

NUREG/CR-2815 provides a procedural guide for conducting a seismic PRA. NUREG-1407 contains specific procedures and submittal guidance for conducting external event analyses, including seismic events. NUREG-1407 was written for the Individual Plant Examination for External Events (IPEEE) program. The IPEEE report states that two assessment methods are acceptable—seismic margins or seismic PRA.[45]

The methodology in the GC PSA methodology report follows accepted practices outlined in NUREG/CR-1278,[40] NUREG/CR-4772,[41] NUREG/CR-4550[43] (the contractor report that formed the basis for NUREG-1150[46]), NUREG/CR-2815,[47] NUREG/CR-6372,[48] NUREG-1407,[45] and NUREG/CR-3558.[49]

An SHA provides the frequency of earthquake motions at various levels of intensity at the site. This output is known as the seismic hazard curve and is expressed in terms of a particular measure of intensity (peak ground acceleration or spectral acceleration vs the annual probability of exceeding this level of intensity). However, the general requirements and methods for AECL's SHA are provided in CAN3-N289.2 M81 R92.[50]

Following the assessment of the seismic hazard for firm ground, AECL determines the local ground and building motions. Because soft soils affect the frequencies and amplitudes of the ground motion entering the structures, these effects must be taken into account. For rock sites, it may be acceptable to assume that the base motions are the same as the free field.

AECL uses EZ-Risk, developed by Risk Engineering, Inc., to calculate the earthquake hazard at a site both probabilistically and deterministically under certain assumptions that are specified by the user (Section 7.3.2, Methodology). These assumptions involve identifying the location of the earthquakes, their potential characteristics, and the ground motions that they may generate. These assumptions are site-dependent. The results of the program's probabilistic calculations are annual frequencies of exceeding various ground motion levels at the site of interest.

AECL also intends to estimate the ground acceleration capacity of all equipment or structures, first by defining failure for the structure or equipment, and then by determining the equipment or structure seismic capacity. NUREG/CR-3558[49] will be a source for generic fragilities.

Event tree development follows the accepted methods with a 72-h mission time. Results are to be reported consistent with NUREG/CR-4550.[43]

The HRA for the seismic PRA analysis is to be conducted in accordance with NUREG/CR-4772[41] (ASEP, a shortened version of NUREG/CR-1278) and NUREG/CR-1278[40] (the THERP method) and follows the HRA methodology of Section 6 of the GC PSA.

The seismic fragility calculations in Appendix A follow NUREG-1407[45] and NUREG/CR-2300, and they reiterate the methods presented in Section 7 of the GC PSA. This appendix provides guidance for performing seismic studies in four general areas: (1) civil structures; (2) equipment qualified by analysis; (3) equipment qualified by testing; and (4) relay chatter evaluation. Appendix A describes the methodology for seismic analysis of civil structures, concrete, steel, and nonseismically qualified structures. Appendix A also presents the seismic fragility methodology for equipment qualified by analysis; an example of this method applied to heat transfer process equipment, the reactor assembly, the fueling machines, and electrical cable trays is given.

4.5.1 Methodology

The fragility of a component is defined as the conditional frequency of its failure given a value of the response parameter, such as stress, moment, and spectral acceleration. According to NUREG/CR-2300, the first step in generating fragility curves is to develop a clear definition of what constitutes failure for each component. That is, the failure modes of the components must be defined. Further, consideration needs to be given to functional failures of structures, structural collapse onto other structures, and potential soil failure in various modes (e.g., liquefaction, toe-bearing pressure failure, slope failures, and base-slab uplift).

AECL recognizes the importance of defining and identifying the failure modes and recognizes that components have more than one failure mode (Section 7.4, Seismic Fragility Evaluation). Each component failure mode is considered in the analysis; therefore, there may be more than one fragility curve for a particular component. Similar to NUREG/CR-2300, the GC PSA usually analyzes three types of equipment failures: anchorage, structural, and functional (Section 7.4.1, Overview). However, in some cases in the GC PSA, the weakest link only may be assessed. In addition, failure modes identified in NUREG/CR-2300 such as soil liquefaction, toe-bearing, base slab uplift, and slope instabilities are also considered as possible failure modes in the GC PSA.

AECL uses three parameters to characterize the fragility curve: the median ground acceleration, A_m; the logarithmic standard deviation reflecting randomness in the capacity, β_r; and the logarithmic standard deviation reflecting uncertainty in the median capacity, β_u (Section 7.4.2, Fragility of Components and Structures). These parameters are estimated for each failure mode of the component, by taking into account the seismic design, qualification, and installation of the component. These are the same parameters identified in NUREG/CR-2300 for developing fragility curves.

AECL indicates that generic qualification test data may also be used for developing fragility data (Section 7.4.3, Sources of Fragility). A source of generic fragilities for components was developed in the

Seismic Safety Margin Research Program (SSMRP), NUREG/CR-3558.[49] This is consistent with NUREG/CR-2300 that states "Fragility curves must therefore be developed primarily from analysis supplemented with engineering judgment and limited test data."

According to the GC PSA, a seismic walk-down is performed at a site to determine any as-built construction deviations and to assist in the fragility analysis of components and structures (Section 7.5, Seismic Walk-Down). Equipment is usually divided into classes, such as horizontal pumps, vertical pumps, fans, valves, motor control centers, cable trays, transformers, inverters, pressure and level sensors, diesel generators, and heat exchangers. The GC PSA states that in some cases, it is not necessary to check all components of each equipment type, but only to check a representative sample (Section 7.6, Systems Analysis). This is consistent with NUREG/CR-2300, which states that "A walk-through inspection of the plant is essential to identify the status of component supports (equipment and piping) and any visible deviations from the as-built drawings."

Systems analysis in the GC PSA includes compiling a safe shutdown equipment list, correlating equipment failures, screening of equipment based on its failure rate, developing the seismic event tree, identifying operator actions and mitigating systems, quantifying the individual accident sequences, and reporting the results of the event trees. This is consistent with NUREG/CR-2300's "Plant-System and Accident Sequence Analysis," "Consequence Analysis," and "Display of Results" tasks.

According to AECL, in general, "manual valves, check valves, small relief valves, and other passive equipment are not included" on the safe shutdown equipment list (Section 7.6.2, Safe Shutdown Equipment List). AECL assumes that they are seismically rugged. However, during a seismic walk-down, these items can be checked. Solid state relays are also considered to be seismically rugged and are not included on the safe shutdown equipment list. Various sources of information for the safe shutdown equipment list include the seismic qualification equipment list, purchase orders, the basic event list for the internal events PRA, design or operational flow sheets, and elementary wire drawings. NUREG/CR-2300 states that "After reviewing plant design criteria, stress reports, and equipment-qualification reports and performing a walk-through inspection of the plant, the analyst may add to, or delete from, the list of components."

According to NUREG/CR-2300, "The need for a detailed fragility evaluation finally rests on the significance of the components in an accident sequence and the contribution of that sequence to the plant seismic risk." Rather than screening components by identifying components that have low fragilities even at extremely high ground accelerations as recommended by NUREG/CR-2300, AECL screens out components that contribute less than 1×10^{-6}/year to core damage because its contribution is considered minimal (Section 7.6.4, Screening of Equipment by Calculation). For equipment that is not screened out, a failure mode and effects analysis (FMEA) is conducted to determine the impact of the structure or equipment failure. The equipment that has been identified by the FMEA as having serious consequences is included in the quantification of the seismic event tree.

The objective of the seismic analysis in both the GC PSA and NUREG/CR-2300 is to define all the possible combinations of successful and unsuccessful system responses to a seismic IE. Their event tree starts with the IE, progresses through a logical set of decision branch points (mitigating system success or failure states), and concludes when stable conditions (with or without releases) are achieved, or when there are no more available mitigating systems. "Generally, accident sequence seismic event trees in the GC PSA are developed as one master event tree, unlike the internal events PRA, which has many separate IEs with their own event trees" (Section 7.6.5, Seismic Event Tree Development). "Two sets of event trees need to be developed. The first set of event trees is to be strictly used to define and quantify the Level I sequences" that lead to significant core damage. To interconnect Level I and Level II PRA activities effectively, "there is a need to consider failures of containment systems, in addition to considering the status of the core. This is accomplished by creating a second set of event trees that also question the availability of containment systems." This is unlike the identification of IEs recommended in NUREG/CR-2300. NUREG/CR-2300 identifies numerous IEs, identifies the dominant IEs, and then arranges them in an hierarchal order. Although the AECL GC PSA Methodology report fails to specifically mention fault trees linked to the seismic event trees, it is thought that this is how the event tree branches are quantified.

A desktop-computer based event tree program called ETA-II (Data Systems and Solutions, LLC) is used to produce the event trees (Section 7.6.6, Event Tree Construction). No specific event tree program is identified in NUREG/CR-2300. This is not a concern because numerous computer programs are available to evaluate event trees.

The AECL states that the following information should be fully documented in the GC PSA, as discussed in NUREG-1407[45] (Section 7.8, Accident Sequence Quantification):

1. the hazard curve(s) used and the associated spectral shape used in the analysis. (As well, the upper-bound cut-off to ground motion should be listed with any sensitivity analysis to determine the effects on the overall results, and the ranking of seismic sequences);
2. a summary of seismic walk-down findings, procedures used, a list of team members, and any subsequent actions taken;
3. all functional and systemic event trees. The manner by which nonseismic failures, human actions, dependencies, relay chatter, and seismic-induced fire or flood are taken into account should be described;
4. a description of dominant functional and systemic sequences that lead to severe core damage (SCD), including any recovery actions;
5. any seismically induced containment failures and other containment performance insights;
6. a table of component fragilities that are used for screening and that are used in the final quantification; and
7. a discussion of nonseismic failures and human actions that are significant contributors or that have an impact on results.

NUREG/CR-2300 states that "The final out-put of the consequence analysis is a family of risk curves."

4.5.2 Strengths and Weaknesses

Section 7 is very detailed for the material that is presented and provides several examples. No serious inconsistencies or errors were identified in the methodology. AECL intends to use CAN3-N289.2 M81 R92 (GC PSA Reference 7-7),[50] to obtain the seismic hazard. It is not indicated if this method is equivalent or comparable to the methods presented in NUREG/CR-6372. (NUREG/CR-6372[48] was published in 1997, and CAN3-N289.2 M81 R92 was published in 1992. NUREG/CR-2300 was published in 1983, and ASME RA-S-2002 was published in 2002.)

The methodology for seismic fragility analysis in Appendix B of the GC PSA is consistent with the standard process and philosophy of NUREG/CR-2300 and is easy to follow. There is only one IE in the GC PSA─the seismic event itself. There is not any information on which or how any IE identified in the internal events PRA are included or evaluated.

The HRA methodology to be used for the GC PSA seismic PRA follows currently accepted practices. The potentially reduced scope of the seismic walk-down of the site could be viewed as a weakness. This is also true for the component screening preliminary calculation.

How the high confidence of low probability of failure (HCLPF) is used to screen out components from further analysis is mentioned but not explained in Appendix B. Some additional information should be included explaining how the HCLPF is to be used to screen out components or structures from further analysis. The criteria for this screening process should also be included.

A site seismic walk-down is to be performed; however, it is not clear how this will be done for an as-yet-to-be-designed NPP. Moreover, Section 7.5 (Seismic Walk-Down) states that "In some cases, it is not necessary to check all components of each equipment type, but only to check a representative piece." This latter phrase indicates that some equipment will be left out of the walk-down, and this is viewed as a weakness.

The safe shutdown equipment list will not normally include manual valves, check valves, small relief valves, passive equipment, or solid state relays. In order "to reduce the amount of effort that is required to solve event trees, and to reduce the number of components in the Boolean equations," AECL proposes that "If a component contributes less than 1×10^{-6}/year to core damage, then the contribution is considered minimal, and it can be out." This also may be viewed as a weakness because possible significant events could be inadvertently screened that on further investigation could have a more realistic assessment and could have a final estimated frequency above 1×10^{-6}/year.

NUREG/CR-2300 does not specifically address HRAs in its discussion of seismic analyses. However, because it uses fault trees linked to the event tree branches, HRA is included. HRA is also typically included in event trees. AECL specifically includes and discusses operator actions and its placement in the event trees (Section 7.7, Human Reliability Analysis).

Section B.2.1.1 (Median Structure Capacity Factor) states that "it should also be noted that variability in modeling [sic] is predominantly considered all uncertainty and no randomness." It is not clear that variations in reinforcement location within the concrete are considered, that is, there is some randomness of the structure from location to location, and no location may match the "design," "theoretical," or "perfect" model for the structure. This is clearly a weakness, based on what is stated. However, if AECL actually uses the minimum reinforcement that is expected to be at any location, this weakness in their approach may not be important.[51]

Section B.3.2.3 (Steam Generator) states that the "Main Steam Line (MSL) is qualified up to the Main Steam Header." The report does not specify what standards or requirements the MSL is qualified for. It also implies that the main steam header is not important (as it is not qualified). Not considering the main steam header important and the effects of a main steam header break (double guillotine type LOCA)[51] is considered to be a weakness.

Section B.4 (Equipment Qualified by Testing) states that "cabinets are usually well constructed and resilient. Experiences have shown that as long as the cabinet does not collapse, the equipment mounted inside usually continue to function." Phrases such as "usually"and "experiences" with design basis earthquakes does not demonstrate that equipment will continue to function. Just because a cabinet does not collapse, does not mean that there may not be connection failures, for example, inside the cabinet. Virtually every cabinet will be different; thus, each cabinet should be assessed independently[51] and not providing a discussion as such is considered to be a weakness.

4.6 Section 8, "Fire Events PSA" and Appendix C, "Example of Fire Event Scenario Calculations"

4.6.1 Methodology

The purpose of the fire events PRA is to identify the dominant accident sequences that are initiated by fire and then to assess the frequency of occurrence for each. This process requires information about the ignition, progression, detection, and suppression of the fires; characteristics of materials under fire conditions; and the plant safety functions and their behavior under accident conditions.

The GC PSA fire methodology follows the outline provided in IAEA Safety Series No. 50-P-4, *Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants, Level I*[52] (and referenced in Chap. 19 of the NRC's Standard Review Plan[53]).

NUREG/CR-2300 assumes that fires are initiated at certain frequencies within various plant compartments; the analyst is to determine the fire event sequences and their frequency. To accomplish this, the fire analysis in NUREG/CR-2300, and followed in this review, is divided into four parts:

1. a fire-hazard analysis,
2. a fire-propagation analysis,
3. a plant and system analysis, and
4. a release-frequency analysis.

Fire-hazard analysis

A fire hazard analysis involves identifying important plant locations with respect to a fire and then determining the frequency of a fire in that location.

"For CANDU plants, fire events are defined as events that are characterized by the presence of flame, burning, or smoldering, and that have the potential for growth and propagation to the point of causing a reactor trip and/or damaging safety-related or PSA-credited equipment" (Section 8.2.1.1, Definition of Fire Events). "Generally, events with smoke and no fire are not included, as well as those that involve arcing, sparking, explosions, and other short bursts of energy that fail to result in ignition." In the AECL methodology, the initiation of a fire is considered to be the point where a flame occurs. This fails to take into consideration the effects of smoke in adjacent areas (as doors are opened for access to the fire) to imped access and for the potential of water misdirection by the fire brigade (delaying fire suppression).

The CANDU Fire Events Database consists of fire events that have occurred at CANDU plants in Canada, as well as the fire events that have occurred in light water reactors (LWRs) in the United States and that are relevant to CANDU plants (Section 8.2.1.1, Definition of Fire Events). Fire events are evaluated individually at the component/equipment level so that the differences of reactor types (CANDU vs LWR) are not relevant when screening LWR fire events for applicability to the CANDU design.

The CANDU Fire Events Database contains the relevant events from the U.S. LWR plants, as well as relevant events from the CANDU Owners Group (COG) database for the CANDU stations. ("U.S. LWR events are considered to be applicable to CANDU systems if they involve similar types of equipment in systems that provide similar functions to those in CANDU plants.") The AECL methodology report references a 1998 proprietary Pickard, Lowe, and Garrick (PLG) fire-event database. (The PLG database was used in U.S. LWR IPEEE studies.) It is assumed that the PLG database contains more events than those compiled by Hockenbury and Yater,[54] Fleming et al.,[55] and Hockenbury et al.[56] However, there is no readily available information to confirm this assumption. According to NUREG/CR-2300, the rate of occurrence can be established from the historical records.

AECL states that "To establish fire Initiating Event frequencies for PRA purposes, the specific plant operating history (on-power, shutdown) needs to be known, and the fire events must have been consistently reported throughout that period." Thus, the GC PSA did not use the IAEA and Nuclear Energy Agency (NEA) events databases because they only report major fire-related events and not all fire-related events (Section 8.2.1.1, Definition of Fire Events).

AECL uses a two-stage Bayesian method for quantifying the frequency of fire events (Section 8.2.2, Calculations of Fire Initiating Events Frequency). According to AECL, this method consists of establishing first a generic probability for each IE and then updating it with the plant-specific experience data. The process involves the following steps:

1. create an industry data set for each category of fire event sources,
2. create the prior distribution (first-stage updating), and
3. update the prior distribution with plant-specific data (second-stage updating).

NUREG/CR-2300 also outlines a Bayesian method for modeling the frequency of fires for various compartments. However, unlike NUREG/CR-2300, a rough outline of the Baysian method for updating fire frequency is not given in the AECL methodology report.

According to the GC PSA:

> The calculation of fire events frequencies applies to a generic CANDU plant design; therefore, plant-specific data for the third step (second stage updating) is not available—this step is used for the analysis of a plant that has been operating for some years. . . This updated frequency represents the frequency (in events per year) with which a fire (caused by sources included in the particular category) occurs in the plant during one year of operation. . . These generic frequencies will be used during the fire vulnerability analysis, with weighting factors that are based on the number of sources that exist in each fire area, relative to the total number of sources that exist in the plant.

The data related to plant systems, equipment, cables, and their locations are collected by AECL in the plant characteristics database (Section 8.3.1, Plant Characteristics Database). The fire characteristics of a CANDU plant are evaluated in terms of "fire zones," which are small sections of a plant that can be treated as a unit for evaluation purposes (Section 8.3.2, Fire Zone Data). "A fire zone usually corresponds to a single room, but can consist of two or more rooms that are spatially linked. A fire zone is not necessarily bounded by physical barriers; spatial separation may be used between fire zones. A fire area is one or more fire zones that are contained within a defined set of fire barriers."

Qualitative screening is used to eliminate areas that have an obviously low impact on plant safety from further analysis, without the use of PRA plant models. The quantitative screening of fire areas and/or scenarios is primarily based on the fire initiation frequency and an analysis of the impact on plant safety, using information from the PRA plant models. AECL uses qualitative and quantitative screening criteria by eliminating from further consideration fires in a number of areas of the plant that may have little or no impact on the plant damage or severe core damage frequencies (SCDFs) (Section 8.5.3, Fire Scenarios for Screening Analysis). According to NUREG/CR-2300,

> The ‘importance’ of a fire location is measured by its contribution to the frequency and the nature of a release of radioactive material. . . The primary measures are the type and the quantity of fire-vulnerable safety equipment at the location of interest. This information can be obtained directly from the fire-protection reviews. Other factors that may be used in the screening process are the frequencies of fires, the types and the amounts of combustible materials, and the available fire-suppression systems.

Thus, screening out unimportant locations can greatly reduce the amount of work required without sacrificing significant confidence in the results. However, with the GC PSA methodology, events and locations of interest are screened out after the data tables are compiled (see Section 8.5.3, Fire Scenario Screening Process), whereas NUREG/CR-2300 typically screens out locations prior to gathering all of the information. This additional review and gathering of information for each area can be advantageous.

The screening approach of the GC PSA agrees with the screening approach of NUREG/CR-2300 which states that "the methods discussed . . . include those that allow most fires to be screened out without the need for detailed investigation;" this is considered to be a strength.

Fire-propagation analysis

The purpose of a fire-propagation analysis is to determine the likelihood and extent of various levels of damage in a compartment, given that a fire has occurred.

AECL uses the COMPBRN IIIe computer code[57] to calculate fire propagation and to determine the time interval between fire initiation and damage to critical equipment (Section 8.5.4.1, Fire Progression Modeling and Fire Consequence Evaluation). COMPBRN IIIe calculates the time to damage critical equipment, once a fire has started. This failure time is used in conjunction with information on fire suppression to estimate the probability that a given fire will cause equipment failure, thereby leading to SCD if the fire is not suppressed. This method agrees with one of the three methods for fire-propagation analysis given in NUREG/CR-2300 that makes use of physical models called "deterministic reference model." For complex configurations, NUREG/CR-2300 states that the computer code COMPBRN is useful.

Plant-system analysis

Once the frequencies of fire-induced component losses are assessed, it is possible to estimate the frequency of fire-initiated accident sequences leading to core damage.

For each fire scenario, the response of the plant is analyzed using PRA methodology that involves

1. identification of the PRA IE,
2. the development of event trees and the description of accident sequences, and
3. the development of fault trees for the analysis of system availability.

AECL accounts for human error probabilities throughout its fire hazard analysis. In general, AECL assumes that fire events in various areas in the plant do not influence operator performance in the main control room (Section 8.6, Human Reliability Analysis for Fire Events). Therefore, human error probabilities for such fire events are considered to be the same as for the internal events PRA. For the case of fire in the main control room, a factor of 5 is applied to the human error probability for postaccident execution actions, compared to the human error probability for the internal events PRA, in order to account for the increased stress. NUREG/CR-2300 recognizes that human intervention plays an important role in the accident: "Not only can the operators extinguish the fire and operate equipment manually, they may make repairs and jury-rig replacement equipment as well."

Release-frequency analysis

The purpose of a release-frequency analysis is to derive the distributions for the various categories of radionuclide releases from the containment. Although AECL does not address release frequencies in Section 8 on fire analyses, it does address Level II PSAs in Section 10.

4.6.2 Strengths and Weaknesses

The AECL methodology for fire analysis follows the outline provided in IAEA Safety Series No. 50-P-4[52] (referenced by NRC's *Standard Review Plan* at bottom of page SRP 19-A24[53]). The steps for performing a fire analysis are basically the same as those given in NUREG/CR-2300; however, the order of performing these steps is different. Data from U.S. LWRs is used to provide a larger database of historical records. This is an advantageous use of existing information to supplement sparse data.

AECL is proactive in considering fire risk studies at the conceptual or detailed design stage. According to NUREG/CR-2300,

> In certain applications of risk analysis, such as those performed during the conceptual or detailed design stage, it may not be practical to attempt a fire-risk analysis because of the need for factoring in details of the physical layout and construction. However, whenever the results of a risk study are to be interpreted on an absolute scale, the omission of fires appears to create a high risk of overlooking potentially dominant accident sequences.

The fire analysis not only accounts for the effects of a fire on the components inside a room and the subsequent plant response, it also takes into account the inventories of combustible materials, the characteristics of adjacent locations, fire-brigade access, and ventilation systems. It also uses qualitative assessments of the likelihood of fire initiation and progression. Because the characteristics of adjacent compartments are explicitly considered, the possibility of fire spreading from rooms containing large inventories of combustibles to compartments containing safety equipment is not overlooked. The level of detail is sufficient to understand how AECL performs a fire analysis and where its data originates.

NUREG/CR-2300 states that "Because of the inherent variability of fire phenomena and the relatively primitive understanding of these phenomena, the large uncertainties in the models leading to these release-category frequency estimates should be treated explicitly throughout the analysis." NUREG/CR-2300 also states that "The analyst should be aware that the existing fire-growth and fire-suppression models do not span the set of all possible scenarios and that even the existing models exhibit large uncertainties. Every attempt should be made to quantify the effects of these uncertainties." If uncertainties in the fire analysis are addressed in the GC PSA, it was not included in the methodology report; this is considered to be a weakness in reporting.

NUREG/CR-2300 also addresses the radionuclide releases from the containment and states that "The release-category analyses should take into account that the same fire that damaged the reactor core may well have damaged containment mitigating functions also. A careful investigation of the entire accident sequence, and not just the portion following core damage, is required." Containment response to fire events was not addressed in the fire analysis section of the GC PSA methodology report.

In Section 8.2.1.1 (Definition of Fire Events), AECL states that "events with smoke and no fire are not included." However, smoke can inhibit operator actions, have a detrimental effect on electrical equipment, and result in misdirected fire brigade action (e.g., the fire brigade spraying water on operating equipment unintentionally and thereby introducing the possibility of failing otherwise operating or operable equipment). Failing to consider smoke, its caustic effects, and its propagation through the plant is considered to be a weakness. Section 8.2.1.1 also states that "explosion events that involve mechanical effects but no fire are not considered." It is not clear if this includes explosion events of high-voltage switchgear and transformers. In addition, it is unclear how one would know *á priori* that an explosion will not generate, either by itself or as the result of impacting something else, a fire.

The frequency of each fire event is calculated by totaling the number of events (occurring during power operations and shutdown) during the time for plant operation (years) multiplied with the plant availability factor during this time. Because plant availability is based on plant operation, this could underpredict the frequency; this is considered to be a weakness.

Switchyard fires were explicitly excluded from consideration in Section 8.2.1.2 (Screening Criteria) of the GC PSA. Switchyard fires should not be categorically eliminated until they can be shown not to adversely affect the plant. For example, switchyard fires could be a source of loss-of-offsite power and as such should be counted. Further, transient fire sources were only considered in selected areas (Section 8.2.1.3, Categories of Fire Event Sources). A transient fire should be postulated to occur at any location in the plant. Historically, transient combustibles have been found in areas where none were suppose to be located.

In Section 8.5.4 (Fire Scenarios for Detailed Analysis), the GC PSA identified cable damage and ignition temperatures of 662°F and 932°F, respectively. The ignition temperature appears to be derived from earlier Electric Power Research Institute (EPRI) data extrapolation results.[58] However, it has since been shown that those extrapolations do not reflect the actual threshold behavior.[59] The conclusion, based on Reference 59, is that both the cable damage and ignition temperatures should be the same temperature, in AECL's case 662°F. In addition, cables that do not meet the IEEE-383 standard need to have a significantly lower cable damage and ignition temperature, specifically 425 °F.[60]

Section 8.6 (Human Reliability Analysis for Fire Events) states that human error probabilities for actions outside of the control room would be the same as those in the internal events assessment. This does not consider the potential influences of stress, time availability, fire location, accessability, available paths to the fire (or remote equipment that needs to be operated locally), smoke levels, use of breathing apparatuses, barriers to communication, relevant training and experience, adequacy of indication in the main control room and at local sites, effects of spurious signals and alarms, and the number of concurrent actions needed on the individual's performance.[60]

Section C.1.3 (Fire Scenarios) states "that it would take about 55 minutes for the hot gases to damage the cable trays that carry the other train." This value of 55 min is used throughout this appendix. The basis for the 55 min has not been provided. Not all compartments will be the same; thus the time to reach a failure temperature would be different for different compartments, fire locations, fire sources, and cable specification. This same paragraph implies that a separation of approximately 4.5 ft is sufficient to prevent failures, except from hot gases. This has not been acceptable to the NRC. Appendix R and the Standard Review Plan, Chap. 9.5, require a free space separation of 20 ft or more.[51]

Section C.1.3 (Fire Scenarios) states that if the fire is not explosive and the switchgear is sealed, the fire will not propagate. This implies that fires may be explosive and switchgear is not explosive. Switchgear can be very explosive, and a fire may result in such an explosive condition. Under the best of circumstances, fire seals have been found to be missing or improperly installed. Thus, AECL should consider the effect of cabinet fires with missing fire seals.[51]

Section C.1.3 (Fire Scenarios) states that fires (transient, transformer, or switchgear) cannot damage or ignite cables if they are located more than 9 ft above the floor. The basis for this assumption and a discussion on the hot gas layer has not been provided. Based on the IPEEE reviews, this appears to be an unfounded assumption.[51]

Section C.1.3 (Fire Scenarios) states that "since it is judged that transient fires cannot cause damage to more than two cabinets, the impact of damage to this equipment is not considered further." The basis for this judgement has not been provided. Transient fires can be fueled by any combination of substances, including oil, which could engulf more than two cabinets (unless every two cabinets are surrounded by a 3-h fire barrier). The effects of the fires started in the cabinets and the hot gas layer effects have not been provided. Based on what was presented, this appears to be an extremely liberal assumption, which is likely to lead to nonconservative results. Based on the IPEEE reviews, this appears to be an unfounded assumption.[51]

Section C.1.4 (Fire Scenario Event Tree) states under "Heading WID: Fires not Occurring within Critical Distance of the Cable Trays" that with one-half the floor covered by cable trays and the cable trays 9 ft above the floor, the factor for transient fires is 0.5. There is no discussion on the damaging effects of the hot gas layer. A hot gas layer could fail all the cables (depending on the temperature of the layer and the qualification of the cables).[51]

Section C.1.4 (Fire Scenario Event Tree) discusses, very briefly under "Heading SF ..." the use of severity factors. The severity factor approach does not fully consider plant-specific and scenario-specific features that may significantly influence the development of a given fire scenario. As a result, scenario quantification based on severity factor approaches tends to produce generic CDF results that may not fully reflect the actual plant-specific conditions of the fire scenario under analysis.[51]

If both a severity factor and credit for subsequent detection and suppression efforts is taken, this may be "double counting." The severity factors typically credit behaviors that impact the general duration of fires. These same statistics and behaviors are widely used to estimate fire durations and the likelihood that fire suppression efforts will be successful.

The severity factor approach may neglect the dependencies associated with subsequent suppression efforts. If, for example, the application of a severity factor means that only challenging fires are modeled, then subsequent firefighting efforts should reflect the fact that the fire brigade (or the fixed systems in some cases) would be faced with a "challenging" fire rather than a "typical" fire.

One feature that makes many fires nonthreatening is their location in the plant. That is, most fires do not occur in critical locations and, hence, have no real potential to spread and/or cause risk-significant damage. Fire location is explicitly treated in the partitioning of fire event frequencies to specific fire areas, specific locations within a fire area, and/or specific fire sources. Hence, use of a severity factor in addition to fire source partitioning factors may also represent "double counting."

The use of multiple severity factors in the quantification of a single fire scenario carries a significant potential for double-counting mitigating features.

The use of severity factors has a notable impact on the fire-induced CDF estimates for the scenarios where they were applied. In most cases where severity factors are applied, fire CDF values are reduced by at least a factor of 5, and commonly by 1 order of magnitude or more. Whether this credit is fully warranted in all cases is a point of uncertainty. As noted above, the approach tends toward production of generic rather than case-specific CDF results.

There is also a potential for optimism in the severity factor approach depending on the how the severity factors were implemented and on case-specific details of the quantified scenarios. Severity factor approaches are, in effect, "short-cuts" to the analysis of phenomena that may mitigate or prevent fire damage. Hence, a more detailed analysis may well reach the same conclusion or result as the analysis that takes the severity factor "short-cut." For example, if no additional detection/suppression credit is taken beyond the severity factor, an argument can be made that application of more traditional methods of detection and suppression analysis might well yield similar, or perhaps lower, CDF results. It is considered to be a weakness to provide the details of the fire scenario under analysis in second tier documentation and not in the GC PSA methodology report.

Section C.1.4 (Fire Scenario Event Tree) discusses the probability of fire detection, lists four functions, states that each function has a failure rate of 0.01, and provides an equation for P(FD). However, the equation does not address the potential failure to activate the fire suppression system or the potential to close the dampers (two of the four functions listed), and no explanation is provided.[51]

Section C.1.4 (Fire Scenario Event Tree) states that "a transient fire is likely to occur as a result of some operator activities in the area; therefore, the operator(s) is (are) likely to be present in the vicinity of the fire origin, thus enhancing the fire suppression reliability." Thus they assign a low failure probability for early suppression. This may be true in the control room, but it is not true anywhere else. An example is a carelessly discarded rag (which was used with a chemical) into a bin or pile of other debris with other chemical compositions. After the operators leave, the chemical reaction will progress to the point of ignition. This is an actual example. Thus, to assume that the operators will be there when the transient fire starts is not a valid assumption. Likewise, welding fires (next paragraph) are not limited to during welding operations. Welding fires have started as much as 30 min after the welding was completed. This is why fire watches are established for at least an hour after the cessation of all welding activities. However, this extended fire watch is not discussed in the report even though a very low failure of early suppression (0.07) is assumed.[51]

Section C.1.4 (Fire Scenario Event Tree), under "Heading LMFS..." states that "the hot gas layer that develops can damage all the cables located in the area—preliminary estimate shows that this will take about 55 minutes." It is unclear if the development of a hot gas layer or failure of the cables occurs in 55 min. The basis for this "estimate" is also not provided. This number is used throughout, and thus, the basis should be well documented. This section then goes on to assign a low probability (0.15) of manual fire nonsuppression, presumably based on having 55 min. The basis for this low probability is a 1988 report. This report should not be the sole basis for this number. Other factors need to be considered, that is, location of the fire, means of ingress and egress, fire brigade response times—specific to each fire location, and consideration of the effects of smoke in adjacent areas (as doors are opened for access to the fire) to imped access and for the potential of water misdirection by the fire brigade (delaying fire suppression).[51]

Section C.1.4 (Fire Scenario Event Tree), under "Heading CCDP..." states (in summary) that the specific spray header is activated for the specific area where the fire is and, thus, no additional electrical equipment will be damaged by the spray water. This would require extremely tight resolution of the fire detectors and the spray headers to distinguish between a fire in each cabinet and exclude spraying water on the adjacent cabinets or any other cabinet in a room that is filled with switchgear cabinets, OR spraying water on the cables that lead to other cabinets. Information has not been provided that shows that this level of resolution has been installed in any CANDU plant and that this system has been tested and its ability to extinguish a full cabinet on fire without wetting any other cabinet or cable has been demonstrated. This is considered a weakness.[51]

There is no discussion on the following topics in the GC PSA risk analysis methodology for fires:[60]

- it is unknown if electrical cables are qualified to the IEEE standards, specifically the IEEE-383 standard,[61]
- heat release rate and heat loss factors that should be used for electrical panel fires (the heat release rate should be 190 BTU/s, and the heat loss factor should be 0.7),
- the probability of abandoning the main control room, given a fire in the main control room. Because the main control room is manned constantly, there is reason to believe that some fires in the main control room would be detected and extinguished sufficiently early so as to not result in abandonment,
- the fire brigade makeup, minimum required training, or minimum failure probability, i.e., failure to extinguish the fire (credit is taken for manual firefighting in the quantitative assessment of fires),
- whether recovery activities are credited for failed fire suppression systems and the probability of the fire suppression system failing on demand,
- electrical fires in enclosures have been known to be energetic and fail the enclosure, or they may generate sufficient heat to warp the enclosure and allow the fire to propagate outside of the enclosure (these issues have not been discussed in the report equipment that should be considered include transformers of greater than 480 V, switchgear, any electrical panel of 480 V or greater fed by a high-energy source (such as a diesel generator or transformer), and motor control centers of 480 V or greater),
- the timing of events, for example, detector response time, acknowledgment response time, fire brigade response time, and time required for initiation of component damage,
- the independence and reliability of any remote (outside of the main control room) shutdown capability,
- the effects of spurious actuation of the fire suppression system, for example, from an earthquake,
- the effects of spurious fire alarms, for example, from an earthquake, which could mask a real fire alarm and send the fire brigade to the wrong location,
- consideration for on-site combustible fluids, for example, oil, diesel fuel, and hydrogen (which is usually used to cool the generator), in tanks and piping; This could be a concern for seismic events as well as other fires where a line could rupture, and the hydrogen could contribute to the fuel supply for the fire,
- the potential for cable tray to cable tray fire propagation; Information on the spread of fire between cable trays can be found in NUREG/CR-5384,[62]
- effects of smoke in the main control room from fires outside of the main control room (this is important because sneak pathways for smoke to enter the main control room would adversely affect the operators and invalidate the assessment if not considered),

- effects of fire and smoke propagation through barriers, for example, from failed or missing seals in the barrier (consideration of multizone and multiarea fires is important because a fire in one area, even with no safety significance, could propagate into another area with safety-related equipment and should be treated differently than, a car fire in the parking lot),
- effects of fire-induced hot shorts (which are very important because hot shorts could spuriously open valves, start pumps, etc. which could initiate a reactor accident, divert flow, provide false indications in the control room, or inhibit operator actions to bring the plant into a safe condition) or shorts to ground (which are very important because it could result in the loss of system power or control),
- effects of potential plume, ceiling jet, and hot gas layer (which is important because it could affect cables, components, or equipment that is not otherwise directly affected by the fire; and if there is a nonfunctioning barrier penetration, the hot gases could enter another compartment and fail components in the second compartment),
- the use of fire severity factors (while not necessarily important by itself, the use of severity factors has, in a number of instances, lead to overcounting—thereby artificially lowering the fire damage probability),
- effects of using a fire barrier failure probability (which would represent the probability that a fire could exist when a door or other barrier penetration was left open, either intentionally or inadvertently), and
- fire protection should follow NFPA 805.

These comments, taken together, are considered to be a important weakness in the fire methodology.

4.7 Section 9, "Flood Events PSA" and Appendix D, "Example of Flood Scenario Calculations"

Operating experience at NPPs shows that flooding has resulted in the coincident loss of multiple components and even multiple systems. This history indicates that, at least for certain NPPs, internal floods may be an important cause of multiple, dependent failures. Operating experience also shows that differences in design features, such as provisions for physical separation, and plant layout can give rise to significant differences in the plant’s response to the same flooding condition. The purpose of a flooding hazard analysis is to identify the dominant accident sequences that are initiated by each flood damage state and then to assess the frequency of occurrence for each.

The major analysis tasks in the GC PSA involve a *qualitative screening* analysis, a *quantitative screening* analysis, and a *detailed analysis* of the potentially significant flooding sources and scenarios.

The *qualitative screening* analysis in the GC PSA methodology report consists of

1. reviewing drawings,
2. performing plant walk-downs, and
3. identifying flood areas, equipment that may cause a flood, and safety equipment that may be affected by a flood and verifying that mitigation features are installed (i.e., drains, flood doors).

Their *quantitative screening* analysis consists of

1. deriving flood IE frequencies from COG flood data and other documents that list CANDU operating experience. (Plant-specific frequencies from piping data will be used in the detailed analysis.)
2. If flooding causes more than one type of IE, then only evaluating the most severe IE.

The *detailed analysis* of the potentially significant flooding sources and scenarios that are identified in the screen analysis consists of

1. determining the flooding frequency based on plant-specific data (i.e., summing all of the flood frequencies from all sources),
2. more realistically evaluating the capability of flooding damage to spread to adjacent areas, and
3. crediting local operator recovery actions, which are performed in areas that are not affected by the flood.

The review of the GC PSA flood hazard analysis is divided into the same four parts identified in NUREG/CR-2300:

1. a flood-hazard analysis,
2. a fragility and vulnerability evaluation,
3. a plant and system analysis, and
4. a release-frequency analysis.

The plant information that is required for the GC PSA flood analysis includes the location of major flood sources, major piping, major equipment for safe shutdown, any potential flood barriers for preventing propagation, and the location of electrical and instrumental equipment that may be affected by water (Section 9.2.1.1, Assembly of Plant Information). This agrees with the high-level requirements of ASME RA-S-2002 for identifying flood areas, identifying flood sources, identifying propagation paths, estimating the IE frequency, and quantifying the flood-induced accident sequences.

4.7.1 Methodology

<u>Flood-hazard analysis</u>

"The major concern in the GC PSA for assessing flood hazards is equipment failure because of submergence or sprayed water" (Section 9.2, General Approach for Flooding Event Analysis). Flood events are of particular concern if 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 shutdown condition. According to the GC PSA, "the basic approach is a screening analysis that first establishes key safety equipment locations and potential flood sources. Flood scenarios are identified based on the source of flooding, the extent of propagations to adjacent locations, and the equipment impact."

The following considerations in the GC PSA provide the limits to the flood analysis (Section 9.2, General Approach for Flooding Event Analysis):

(a) only one flood event is assumed to occur at a time (e.g., only pipe break or tank rupture);
(b) the internal events analysis treatments of LOCAs inside containment adequately address flood sources and their effects;
(c) temporary hose/piping connections can be excluded from the analysis as flood sources, since they are used relatively infrequently;
(d) seismic induced floods are analyzed in the seismic PRA;
(e) floods are treated as IEs and not as events that are subsequent to another initiator;
(f) spurious activation of sprinkler systems is considered;

(g) areas surrounded by walls are assumed to be properly sealed, so that flood propagation via walls will not be considered, although the effect of drains must be taken into account;
(h) the critical height of the electrical cabinets is generally assumed to be 6 in. (15.2 cm) and the critical height of the pumps is generally assumed to be 3.28 ft (1.0 m), if specific information is not available. The critical height of motor operated valves (MOVs) is assumed to be the same as that of the pumps;
(i) the vacancy factor of the area occupied by the mechanical equipment and by the electrical cabinets is generally assumed to be 0.6 and 0.8, respectively, based on U.S. LWR experience (for the CANDU 6 turbine building, the vacancy factor is in the order of 0.9 based on a general system layout. These values should be assessed on a case-by-case basis);
(j) a closed loop system is not generally considered to be a flooding source because a closed system contains a limited amount of inventory, and the pumps circulate the flow(usually, breaks in a closed loop would trip the pumps, which would stop the flood); and
(k) only random failures will be considered in the flooding analysis (flooding due to human errors (caused by leakage from a component that is incorrectly assembled or is left in a disassembled state following maintenance) is not analyzed and it is assumed that the operator can take immediate corrective action to mitigate the accident).

Item g takes exception to the minimum requirements given in NUREG/CR-2300. Specifically, NUREG/CR-2300 states "The following mechanisms should be considered at a minimum: loss of structural integrity through collapse, sliding, overturning, ponding, excessive impact and hydrostatic loads; flooding and wetting of equipment from seepage through walls and roof; flow through openings; sprays, thermal shocks, missile impacts; and the blockage of cooling-water intakes by trash." In addition, although listed as being considered in the GC PSA flooding hazard evaluation, not all of the "minimum" mechanisms listed to be considered are specifically addressed in the CANDU methodology report.

Identification of the flood areas by AECL 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.).

While AECL relies significantly on walk-throughs to identify source and impact locations, qualitative screening in NUREG/CR-2300 describes the use of a special type of qualitative fault-tree analysis that takes into account the location of system components. The fault tree need only be developed to the level of major subsystems (e.g., high-pressure injection train A) so that the singular effect of the loss of groups of components in specific locations can be resolved. The relative importance of each location is determined by postulating that a flooding condition exists in each location, one at a time, and assuming that all the subsystems in that location are failed with a probability of unity.

One other factor that may contribute to the independence of an area is physical separation, that is, walls. The GC PSA indicates that the collapse of walls or leakage through construction joints need not be considered because the leakage rates are minor, and they can be easily accommodated by installed drainage systems (Section 9.2.1.2, Identification of Flood Areas). However, NUREG/CR-2300 specifically mentions "loss of structural integrity through collapse" and "flooding and wetting of equipment from seepage through walls." In addition, ASME RA-S-2002 recommends including the potential for structural failure (e.g., doors, walls) because of flooding loads.

In the GC PSA, the major flooding sources, together with their water capacity are identified. For CANDU plants, the major water sources are (Section 9.2.1.3, Identification of Flooding Sources):

1. the raw service water system,
2. the condenser circulating water system,
3. the emergency water supply system,
4. the dousing water system,
5. the ECCS, and
6. the fire protection system.

In these systems, the GC PSA evaluates

- pipe failure,
- valve rupture,
- expansion joint failure, and
- tank failures.

NUREG/CR-2300 states that in addition to identifying internal causes from breaks and leaks in major water systems, internal causes should also include the "overfilling of tanks, sump-pump malfunctions, and the backing up of drains." ASME RA-S-2002 requires including "human-induced mechanisms that could lead to overfilling tanks, diversion of flow through openings created to perform maintenance; inadvertent actuation of fire suppression." Not including these sources in the GC PSA is considered to be a weakness.

AECL determines the impact of flooding in each flooding area through a two-step process (Section 9.2.1.4, Identification of Equipment in Each Flooding Area):

1. identifying the systems used for accident mitigation, and
2. identifying the safety system components, based on active components that are likely to change state during an accident (pumps, valves), components that induce IE upon failures, and sensors or transmitters that are essential for plant monitoring.

The equipment reviewed should also include cables (including junctions), switchgear, and motor control centers.[63]

Each flood scenario can be divided into subscenarios that are based on the individual sources that are present in the flood location, if their impact is expected to be greatly different (Section 9.2.2.6, Refining the Initial Screening Model). Then, the flood scenario frequency is reduced by empirical factors (<1) that lower the frequency used in the screening analysis. However, no reference is given in the GC PSA for these "empirical factors" (factors include location, direction, propagation, severity, and operator). The results are then compared with conservative deterministic failure (CDF) of 1×10^{-6} to identify those flood areas that require further detailed analysis (Section 9.2.2.7, Final List of Potentially Significant Flooding Areas and Scenarios). The lack of traceability of the empirical numbers used in the flood analysis is considered to be a weakness.

Data sources used in the assessment of LOCAs are

- piping failure frequency from WASH-1400[64] (published 1975),
- valve rupture frequency from NUREG/CR-1363[65] (published 1980),
- expansion joints failure frequency from Calvert Cliffs PSA[66] (published 1993), and
- tank failure frequency IAEA-TECDOC-478[67] (published 1988).

The GC PSA recommends using the WASH-1400 approach for estimating the generic pipe break frequency in the flooding GC PSA (Section 9.2.3.2.1, Piping Failure Frequency). The use of component failure and pipe failure data for the assessment of LOCAs is consistent with NUREG/CR-2300. However, ASME RA-S-2002 requires the use of generic data enhanced by any plant-specific information.

The GC PSA defines three flow rates similar to the Calvert Cliffs PRA (Section 9.2.3.5, Categorization of Flood)—small, medium, and large. However, NUREG/CR-2300 defines the following four flood severity categories:

1. small—flooding on the order of hundreds of gallons,
2. moderate—flooding on the order of several thousands of gallons,
3. large—flooding on the order of tens of thousands of gallons, and
4. very large—flooding on the order of hundreds of thousands of gallons.

NUREG/CR-2300 defines one more category than that given in the CANDU methodology report. Further, the CANDU methodology report does not define the flood categories in terms of volume.

Fragility and vulnerability evaluation

The flooding area is defined to be the area that is bounded by the walls or barriers that are able to reasonably contain the floodwater in the area. According to the GC PSA, the barriers do not need to be watertight doors or barriers (failure probabilities are given). A fire door is considered to be able to reasonably contain floodwater for a sufficient amount of time (Section 9.2.3.1, Definition of Flooding Areas).

After the flood areas and the flooding sources in each specific flood area are identified, the flood scenarios are developed. The flood scenarios are dependent on the flooding source, the area’s layout, the flood propagation, and the time that is available for the operator to isolate the flood (Section 9.2.3.8, Classification of Flood Scenarios).

Plant and systems analysis

The end points of the flood scenario diagrams are the flood damage states that are assessed by developing event trees (for the failure of mitigating systems after the flooding event). After quantification, the end points of the event tree for each specific flood damage state are summed together, and they represent the conditional core damage probability (CCDP) (Section 9.2.3.9, Evaluation of Flood-Induced Accident Sequence Probabilities).

For each flood scenario, the flood frequency, the probabilities of operator error in terminating the flood, the flood propagation probability (flood barrier failure probability) and the CCDP of flood-induced accidents are required to evaluate the SCDF of flood-induced accidents. The results are the final SCDFs for each flooding sequence (Section 9.2.3.10, Evaluation of the Severe Core Damage Frequencies due to Flooding Event). This is consistent with the intent of NUREG/CR-2300 and ASME RA-S-2002 of identifying and quantifying the flood scenarios/sequences that contribute to CDF and large, early release frequency (LERF).

The GC PSA factors the likelihood of spray on equipment (Section 9.2.2.6, Refining the Initial Screening Model) into its flooding analysis. The GC PSA also indicates that "the major concern in the flood PRA is equipment failure due to submergence or sprayed water (Section 9.2.2.2, Identification of Flood-Induced Initiating Events). This is consistent with NUREG/CR-2300 that states that "Special attention should be given to component failures and whether the flooding entails sprays of water or just a rising pool." However, ASME RA-S-2002 is more prescriptive in requiring the evaluation of the dynamic effects from HELBs such as jet blast impingement, spray, pipe whip, humidity, condensation, temperature concerns, and steam flooding. It is not clear that dynamic effects are addressed in the GC PSA; this is considered to be a weakness in reporting.

The GC PSA factors the likelihood of operator recovery actions (Section 9.2.2.6, Refining the Initial Screening Model) into its flooding analysis. This is consistent with NUREG/CR-2300 that states that "special attention should be given to flood termination possibilities . . . and recovery of failed systems via local manual actuations." ASME RA-S-2002 also allows the screening of potential flooding scenarios because of human mitigative actions.

Release-frequency analysis

The purpose of a release-frequency analysis is to derive the distributions for the various categories of radionuclide releases from the containment. Although AECL does not address release frequencies in Section 9 on flood-hazard analyses, it does address Level II PSAs in Section 10.

Details of the quantification of the flood analysis are limited in the GC PSA. For example, ASME RA S 2002 says to "use appropriate models and codes." Event trees are used in the GC PSA methodology, but code-specifics are not given. ASME RA-S-2002 also addresses method-specific limitations, uncertainties, and the review of the important contributors to CDF. These details are not given in the GC PSA flooding assessment methodology.

4.7.2 Strengths and Weaknesses

According to NUREG/CR-2300, "there are no well-established methods for the analysis of either external or internal floods." Section 9 and Appendix D in the GC PSA adequately describe core damage probability calculations for flood scenarios for the CANDU plants. They address the major tasks of a flood analysis of identifying flood areas, identifying flood sources, identifying propagation paths, estimating IE frequency, and quantifying flood-induced accident sequences.

Many of the design and operational features required to protect against external floods may not provide the same degree of protection against internally initiated floods. In fact, the experience with flooding at NPPs indicates that internal floods may have a relatively greater potential to cause a reactor accident with nonnegligible risk. Certain details, particularly in the areas of hazard and fragility analysis are different, depending on whether the flood results from external or internal causes. Internal floods are the only flood initiating events addressed in the GC PSA; external floods are plant-specific and have to be assessed on a case-by-case basis (Section 9.1, Introduction). Thus, although ASME RA-S-2002 addresses external sources of water, not addressing external floods is not considered to be a weakness in the GC PSA methodology report as long as external sources are evaluated on a plant (site) specific basis.

The Flood Hazard Analyses in GC PSA, NUREG/CR-2300, and ASME RA-S-2002 cover both qualitative and quantitative screening. The identification of important locations is made from two perspectives. For a flood analysis, it is necessary to identify both the source locations (i.e., the locations where floods are most likely to start) and the critical impact locations (i.e., the locations where the existence of a flooding condition would have the greatest impact on the availability of key safety-related systems). The Fragility Evaluation and Plant and Systems Analysis steps in NUREG/CR-2300 are covered in the detailed analysis for the CANDU plants. Not addressed in the CANDU methodology report but covered in NUREG/CR-2300 is frequency analysis to estimate the conditional frequency of exceeding levels of accident consequences, given the occurrence of each flood-damage state. The CANDU methodology report's chapter of flood analysis does not cover accident consequences.

NUREG/CR-2300 repeatedly reminds analysts to address uncertainty issues: "regardless of the magnitude of the uncertainty, the PRA should include a flooding analysis and attempts should be made to quantify the effects of uncertainties to the extent that this can be done" and "The methods should ensure that all sources of uncertainty in the risk estimates are identified and their effects quantified if possible, including the uncertainties associated with sparse or inadequate data, uncertainties in the models used to calculate flood variables, uncertainties and variabilities in the failure limits of components and structures, uncertain increases in component-failure rates in abnormal flooding environments, and other uncertainties associated with risk estimation." ASME RA-S-2002 states that "uncertainties in the PRA results shall be characterized. Sources of model uncertainty and key assumptions shall be identified, and their potential impact of the results understood." The CANDU method lists sensitivity analysis as a major task. However, no details are provided in the chapter of flood analysis. The lack of details in performing sensitivity analyses is considered to be a weakness in reporting.

Section 9.2(g) states that "areas surrounded by walls are assumed to be properly sealed." This is appropriate for determining the maximum flood height in the area and assessing the impact of the flood. However, leakage paths (e.g., under nonwatertight doors), should be considered to assess the impact of flooding of adjacent areas to ensure that no safety-related component will be adversely affected. The direction that the nonwatertight door opens can also be important. If the door opens into the flooded area, the water will tend to keep the door closed until it starts to buckle. If it opens into the adjacent area the leakage past the door will be greater and someone could inadvertently open the door, thereby initiating a flood in the adjacent area. This situation, and similar possibilities, should all be considered as part of the flood evaluation.[63]

AECL in Section 9.2.1.2 (Identification of Flood Areas) recommends not to "consider the collapse of walls or leakage through construction joints. The leakage rates are minor and can be easily accommodated by installed drainage systems." However, the "Acceptable Methods" in NUREG/CR-2300 specifically addresses collapsing of walls. The methods section in NUREG/CR-2300 also address backing-up of drains, overfilling tanks, and sump-pump malfunctions, none of which are addressed in the CANDU methodology report.

The equation used to estimate "flow rate under a door" is stated with no reference or development (Section 9.2.3.6, Other Calculations for Flooding PSA). In addition, the equation used to estimate "flow rate via drains" is stated with no reference or development.

Section 9.2.2.1 (Evaluation of Flood Frequencies) states that they are going to only use the flood initiation frequencies for each flood area based on CANDU operating experience. There are two exceptions to the use of CANDU operating experience—expansion joint failure frequency and tank failure frequency. Section 9.2.3.2.3 states that "The failure rate [for expansion joints] includes external leaks, therefore, it is conservative to be applied in the flooding PSA and therefore not selected." Similarly, Section 9.2.3.2.4 states that "the failure frequency [for tank ruptures] is considered too conservative for use in this flooding PSA methodology" because the failure frequency is for all types of failure modes rather than just ruptures. For pipe break probabilities, if there is insufficient experience, it would seem more appropriate to use generic pipe break frequencies.[63]

Section 9.2.3.2.3 (Expansion Joints Failure Frequency) implies that AECL has information related to expansion joint failure frequency based on its own CANDU reactors and concludes that their experience is not applicable to their next generation design (ACR-700), but a foreign reactor design's (U.S. design) is applicable. PRAs are suppose to use generic numbers when they have none better and to modify those numbers with real experience information, when available. No evidence is provided to support the conclusion that AECL's expansion joint design for the ACR-700 (and CANDU 6 and CANDU 9) should not experience a similar failure rate to what other CANDUs have experienced. This is considered a weakness.[63]

For the purpose of the screening analysis only, the flood initiation frequencies for each flood area are determined on the basis of CANDU operating experience data (Section 9.2.2.1, Evaluation of Flood Frequencies). Because quantitative screening in NUREG/CR-2300 consists of reviewing historical data of incidents that involved flooding of some sort, the GC PSA is consistent with NUREG/CR-2300. However, ASME RA-S-2002 allows screening out of IEs if the IE is $<1 \times 10^{-7}$/year when the event does not involve either an ISLOCA, containment bypass, or a reactor vessel rupture; or 1×10^{-6}/year and core damage could not occur unless at least two trains of mitigating systems are failed independent of the initiator. Because it is unknown how the GC PSA algorithm works or the sequence of truncating sequences (i.e., if the sequences are truncated once the cut off value is exceeded even if all event tree tops and fault trees have been evaluated), the validity of their statement cannot be addressed. The concern is that subtle dependencies between two (or more) systems could be missed.

Section 9.2.2.5 (Preliminary List of Potentially Significant Flooding Areas and Scenarios) states that the screening criterion is a frequency of 1×10^{-6}/year. This appears to be a rather high screening frequency criterion. While the total results need not be reported below 1×10^{-6}/year, possible significant events could be inadvertently screened that on further investigation could have a more realistic assessment and could have a final estimated frequency above 1×10^{-6}/year. It appears more reasonable to have the preliminary screening criterion set at 1×10^{-7}/year. A comparison of flooding event frequencies to internal event frequencies is not an appropriate basis for exclusion.[63]

Section 9.2.3.2.4 (Tank Failure Probability) states that the CANDU's experience data for the frequency of external leaks for tanks is 2.3×10^{-3}/year. The GC PSA methodology report further states that because this frequency "is for all types of failure modes," it is considered too conservative for use in this flooding PRA methodology. The difference between leakage and rupture is not defined. The potential for flooding should include an assessment of the maximum acceptable leakage rate that will not cause unacceptable component degradation and then identify the frequency of exceeding that leakage rate. The report then goes on to quote two PWR tank rupture rates and then selects the smaller rate. The basis for selecting the rupture frequency of the PWR refueling water storage tank 2.3×10^{-4}/year instead of the PWR feedwater storage tank 2.8×10^{-4}/year was not provided.[63]

Section 9.2.3.3 (Flood Flow Rate) discusses the determination of the flooding rate using pumps, orifices, and maximum pipe flows. It does not address determination of the flow rate from failed tanks. Specifically, it does not address evaluating the tank leakage that could cause unacceptable component degradation. This paragraph also states that the operators can isolate the flooding source before it affects safety functions. This is not necessarily true for tank failures. Indeed "keep full" systems could sense the level reduction and start adding more water into the failed tank. The water provided by such systems should be included in the flooding assessment.[63]

The flooding flow rate would be limited by the maximum pumping rate, maximum flow rate of orifices, and maximum flow rate of pipes. Because all three factors can limit the flow, the lowest flow rate among them would be the flooding flow rate (Section 9.2.2.3, Identification of Flood Propagation Paths). The flood flow rate is used to calculate the time available for operator action to mitigate a flood. The equation used to estimate "orifice flow rate" is stated with no reference or development. The GC PSA states that "If all the required information for estimating the flood rate is not available (e.g., the operating pressure of piping flooding sources is not available), then the orifice flow rate is estimated using the pump discharge pressure." However, there is no discussion about uncertainties or whether this results in a conservative estimate of flow rate. Also, the equation used to estimate "maximum flow rate of piping" is stated with no reference or development. The GC PSA also states that "If both the operating pressure at the orifice point and the pump discharge pressure are not available, then the normal pumping flow rate, multiplied by the number of operating pumps is used for the flood flow rate." However, there is no discussion about whether this results in a conservative estimate of flow rate. Nor does it discuss pump "run-out" flow rates if discharge pressure is reduced to atmospheric, etc.

Section 9.2.3.4 (Operator Recovery Actions) discusses possible operator actions in response to a flooding event. One action identified is "the closing of the door in the flooded area." This seems that it could be conditional. If water is flooding over the threshold of the door, this could be defined as "heroic" because of the potential for radioactivity in the water and the temperature of the water. This needs to be considered in giving credit for this operator action.[63]

The second paragraph in Section 9.2.3.4 states that "the time available for the operator action to isolate the flood can be estimated, by dividing the amount of flooding water by the flow rate." This does not appear to be correct. It would seem that to estimate the operator action time would be the available volume to contain the flooding water (i.e., before adversely affecting any safety-related component) divided by the flow rate minus the time for initiation of the alarm in the main control room.[62]

Drain obstruction from the failure of any check valve or drain blockage must be addressed in the GC PSA (Section 9.2.3.7, Probabilistic Evaluation of Flood Growth). However, backflow through drains, which has been observed in operating NPPs, is not addressed.

Section 9.2.1.5 (Qualitative Screening of Flood Areas) states that "flood areas are screened out if they do not contain any susceptible equipment for safe shutdown, or if they do not contain any equipment that, if damaged, would lead to an IE." Before an area is screened out, it should also include a review to ensure that there are no "sneak" pathways for water to enter into other areas that might include important equipment. This includes drain lines with potential drain line plugging elsewhere in the pipe and nonwatertight doors.[63]

This review also identified a potential licensing issue. In the licensing of currently operating reactors, U.S. nuclear power plants were explicitly reviewed for potential internal flooding before receiving an operating license. Every compartment and area was reviewed for failure of the largest pipe, largest capacity, and, where pumped, assumed that the pumps continued to run. All means of water egress were evaluated, and the flood water level was determined. An assessment was made concerning the survivability of the equipment and, if it was not expected to be above the flood water elevation, appropriate measures were taken. All potential water pathways (drains, penetrations, passageways, doors) were evaluated to investigate potential flooding of other compartments. In today’s parlance, this would be called a deterministic review. It is important to note that the flooding assessment in AECL’s PRA does not include this type of review and no indication has been given by AECL that such a review will be performed as part of the design certification process. The AECL PRA review only includes those potential flooding scenarios that have an estimated frequency in excess of 1.0×10^{-6}/year, i.e., it is a risk-based evaluation of potential flooding scenarios. A key assumption in the AECL PRA is that all barriers are installed properly and function as designed, i.e., water-tight. This includes all penetration seals and doors. This is expected to lead to few, if any, analysis of adjacent compartment flooding. It should be recognized that this is risk-based, not risk-informed, and this will not result in the same detailed level of review as was received by the current operating nuclear power plants.

These comments, taken together, indicate a important weakness in the flood methodology.

4.8 Section 10, "Level II PSA"

According to ASME RA-S-2002, "The objectives of the LERF analysis element are to identify and quantify the contributors to large early releases, based upon the plant-specific core damage scenarios." The goal is to identify significant operator actions, mitigation systems, and phenomena that can alter sequences; properly reflect dependencies; and present success criteria to support the individual function successes, mission times, and time windows for operator actions and equipment recovery for each critical safety function.

The GC PSA divides the containment performance analysis into four tasks (Section 10.2, Implementation):

1. identify containment performance features,
2. develop accident sequences,
3. develop the containment event trees (CETs)—including containment bypass events, and
4. develop containment release model.

NUREG/CR-2300 divides the containment performance analysis into nine tasks. The first two tasks in NUREG/CR-2300 are concerned with the collection of data and the modeling of the plant for analysis. In the third task, potential failure mechanisms for the containment and levels of failure are investigated in preparation for the construction of the containment event tree. Tasks 4–6 involve identifying the methods of analysis, reducing the number of sequences to be analyzed by grouping sequences into plant-damage states or bins, and developing the CETs. The representative sequences are analyzed with the core-melt codes in Task 7. Performing sensitivity studies to quantify event-tree branching probabilities and to estimate the contribution of uncertainties in physical processes to the uncertainties in the total risk, and supplying results (accident timing, temperatures, flows, pressures, and rate of leakage from containment) to the radionuclide-transport task comprise Tasks 8 and 9.

The methodology in ASME RA-S-2002 consists of three tasks: grouping core damage sequences into plant damage states, analysis of credible severe accident phenomena, and analysis of containment system performance.

4.8.1 Methodology

Identify containment performance features

"This task involves the collection of plant data, the identification of unique features of the specific plant being analyzed, and the selection of deterministic analyses from relevant CANDU safety reports" (Section 10.3, Containment Performance Features). This is considered to be a weakness because the meaning of identifying "unique" containment features is unknown.

The collected CANDU 6/CANDU 9 containment systems and related reactor data are organized and related to parameters that impact accident progressions (Section 10.4, Collection/Review of Plant Data). This is consistent with NUREG/CR-2300 except that there is no reference to failure modes or studies from similar plants.

Develop accident sequences

Accident sequences that do not lead to SCD but do cause releases into containment are grouped into plant-damage states (PDSs). PDSs are defined for both limited core damage accidents (LCDAs) and severe core damage accidents (SCDAs); however, the Level 2 analysis only considers SCDAs. "The sequence groupings are based on similarities in accident progressions and systems that impact the containment response to accident loads" (Section 10.5, Development of Accident Sequences).

According to NUREG/CR-2300, these "special cases [of plant damage states] cannot be conveniently fit into the generalized containment event tree." Examples from NUREG/CR-2300 include vessel rupture as an IE or as the result of a transient and containment isolation after an accident. It is considered to be a weakness in reporting because neither of these special cases (calandria vessel rupture [a] and containment isolation after an accident) appear to be addressed in the GC PSA. Not evaluating these special cases is considered to be a weakness. Otherwise, the GC PSA method report is consistent with NUREG/CR-2300 and ASME RA-S-2002 because the plant damage states are defined. (PDSs are defined for both limited core damage accidents and severe core damage accidents; however, the Level 2 analysis only considers severe core damage accidents.) In addition, NUREG/CR-2300 recommends that failure modes or studies from similar plants be reviewed; there is no mention of this in the GC PSA report.

Develop the CETs

NUREG/CR-2300 states that

> The containment event tree is developed to describe the progression of an accident sequence from the start of core melt to the release of radionuclides after containment failure, with particular emphasis on branch points that can result in containment failure or significantly affect the release of radionuclides. . . Typically, containment event trees follow from the final branch points of system event trees. . . In the Reactor Safety Study, the headings of the containment event tree were events postulated to lead to containment failure. However, it might be appropriate to include in the containment event tree events that significantly change accident consequences without failing the containment.

Similar details are not given in the GC PSA on the development of the CETs. However, it is known from the GC PSA that frequencies are determined in the development of the CETs (Section 10.6, Containment Event Tree Model Development).

During the CET analysis in the GC PSA, an assessment is made of the likely containment failure modes, such as isolation failures, containment bypass, loss of local air coolers, etc. A complete list of containment failure modes (containment impairment states) is identified during the process of CET

[a] Although the ACR-700 does not have a reactor vessel, AECL refers to the calandria as a "calandria vessel." In fact, the GC PSA analysis document has a section (12.5.2) titled "Calandria Vessel Failure Criteria."

development (Section 10.7, Containment Bypass Events). This meets the intent of NUREG/CR-2300 and ASME RA-S-2002.

Develop containment release model

The number of system sequences that are identified in a typical PRA is very large—much too large for the physical processes of each to be analyzed. Two approaches can be used to reduce the large number of system sequences to be analyzed: probability screening and the development of plant-damage bins. For CET analysis in the GC PSA, containment failure "bins" or release modes (RMs) are developed. The GC PSA bins events based on RMs only that appear to correspond to performance of containment safety features (Section 10.8, Environmental Transport and Consequence Analysis). The RMs are CET end states with similar source-term characteristics and are combined into a few release categories (RCs) for off-site consequence analysis. RCs define the sequence of radioactive releases outside the containment boundary and are quantified in terms of dose.

NUREG/CR-2300 recommends a combination of probability screening and binning such that a variety of sequences are selected for analysis, and the binning is done after a significant number of sequences have been evaluated. Typical bin characteristics given in NUREG/CR-2300 are IEs, timing of core melt, and performance of engineered containment safety features.

The Modular Accident Analysis Program[68] (MAAP) is an integral systems analysis code for assessing severe accidents and was initially developed during the industry-sponsored Industry Degraded Core Rulemaking (IDCOR) program. In addition, MAAP3B was expanded to include the Ontario Power Generation (OPG) CANDU designs, and this has been further updated to the MAAP4-CANDU model (Section 10.9, Severe Core Damage Accident Progression).

The MAAP for CANDU nuclear generating stations, MAAP4-CANDU[69] (M4C), is a computer code that can simulate the response of the Ontario Power Generation (OPG) or AECL CANDU 6 and CANDU 9 nuclear generating stations during severe accident conditions. According to the GC PSA, the validation and verification of the MAAP4-CANDU computer code is in progress.

At the time of publication of NUREG/CR-2300, MAAP was not yet available; however, its pending completion was noted. Although the MAAP code has not been reviewed recently, the static design suggests that it would yield less realistic results than the state-of-the-art code, e.g., MELCOR.

GC PSA Section 10.9.1.2 (Scope), lists the following accident sequences that could be reviewed:[70]

1. large-break LOCAs,
2. small-break LOCAs,
3. transient IEs such as loss of ac and dc power,
4. steam generator tube rupture, and
5. main steam line break.

Not considering a main feedwater line break assessment in the review is considered to be a significant weakness.

4.8.2 Strengths and Weaknesses

The Level II PRA analysis in the GC PSA methodology document meets the intent of both NUREG/CR-2300 and ASME RA-S-2002. The method identifies the plant damage states (although PDSs are defined for both LCDAs and SCDAs, the Level 2 analysis only considers SCDAs), the development of the CETs, and the analysis of the containment system performance.

Although the GC PSA provides an outline of the general approach to performing a Level II PRA, specific details such as binning characteristics, potential containment-failure modes and mechanisms, and plant input data to core-melt codes are not given. Further, details such as developing CETs based on timing of events are not discussed.

NUREG/CR-2300 repeatedly references other risk studies and states that only updating events not previously addressed is necessary. The GC PSA does not make any comparisons to other risk studies. It appears that the GC PSA provides the complete set of CETs that were modeled. Although it is more work, providing a complete set of all CETs modeled is deemed advantageous.

Although uncertainty is covered in general in previous chapters, it is not specifically addressed in the Level II analysis in the GC PSA; this is considered to be a weakness in reporting. According to NUREG/CR-2300, uncertainties in the analysis of the physical processes of core-melt sequences enter into the results of a PRA in two ways. First, the uncertainties affect the estimates of the frequencies of accident sequences. Second, the uncertainties appear as variations in the output variables from the analysis. Specifically, "The need for sensitivity studies is emphasized." This is considered to be a weakness.

ASME RA-S-2002 specifically addresses the analysis of severe accident phenomena, containment system analysis, and containment structural capability. The GC PSA did not clearly identify evaluating the containment structural capability; this is considered to be a weakness.

4.9 Section 11, "Conclusions"

The "Conclusions" in the GC PSA consist of a one-page set of conclusions that goes into very little detail but "concludes" that CCF, HRA, seismic, fire, and flood analyses can be performed. The conclusions also note that the validation and verification of the MAAP4-CANDU computer code is in progress.

4.10 Section 12, "Glossary"

The glossary appears to be sufficient because the definitions provided are understandable and appropriate.

4.11 Summary

The reporting and methodology strengths and weaknesses noted from the review of the GC PSA methodology document are summarized in Tables 3–6.

Table 3. Summary of Reporting Strengths Identified in the Review of the GC PSA Methodology

Topic	Observations
Overall	The presentation is consistent with typical PRAs and is easy to follow. In most cases, the material presented is complete and very detailed.
Overall	Appendix E appears to be complete, easily understood, and gives the basic design features and considerations for each reactor system design.
Internal Events Analysis	The plant success states and mission times are fully developed and easy to follow. The component types, boundary descriptions, failure modes, and mechanisms are also fully developed and easy to review.
Human Reliability Analysis	Section 6 is fairly detailed for the material that is presented. There are many examples that aid in understanding the material, and the review found no inconsistencies or errors.
Seismic Events Analysis	Section 7 is very detailed for the material that is presented and provides several examples that aid in understanding the material.
Glossary	The glossary appears to be sufficient because the definitions provided are understandable.

Table 4. Summary of Reporting Weaknesses Identified in the Review of the GC PSA Methodology

Topic	Observations
Internal Events Analysis	Many times a representative example or calculation would enhance a reader's understanding of the methodology. In addition, the example calculation in Appendix A is not detailed enough to duplicate the end results.
Internal Events Analysis	Details of the methodology are provided in other reports and not in the CANDU methodology report.
Internal Events Analysis	The GC PSA fails to adequately discuss shutdown, low-power operation, and refueling IEs.
Internal Events Analysis	It appears that the GC PSA, with its focus on performing sensitivity analyses on human-related errors (i.e., different maintenance practices, testing procedures, and mission time), should be expanded to include assessing the impacts of different models, system-success criteria, etc.
Internal Events Analysis	The IE frequencies are derived from CANDU operating experience and fault tree analysis. However, it is unknown if plant availability is accounted for in the frequency, if any screening criteria were used, and if generic data for rare events were used.
Internal Events Analysis	Most PSAs for U.S. LWRs treat two (or more) redundant systems individually the same. The repair time is addressed in other areas, and without a more detailed description provided in the report it is not possible to compare the two methods.
Internal Events Analysis	The GC PSA methodology document states that the methodology to be used in the fault tree analysis of CANDU plants follows that described in CNSC Consultative Document C-70 and NUREG-0492 (Section 4.4, System Reliability Analysis). Because no further details are available, an assessment of the method to develop fault trees cannot be made.
Internal Events Analysis	The modularization process is said to reduce the time spent reviewing the cut sets, but this process is not presented in the GC PSA. For example, the following statement is made: "By implementing the modularization technique, the analyst can greatly reduce the number of cutsets that require review." However, no additional information is provided regarding the use of the modularization technique.
Dependent Events Analysis	The UPM method is not fully described in the GC PSA (Section 5.2, Main Features of UPM). The "UPM Workbook" is a company proprietary document.
Dependent Events Analysis	There are too many generalizations in the dependent events analysis description to perform an adequate review. Also, there is a lack of examples using the UPM in estimating CCF.

Table 4. Summary of Reporting Weaknesses Identified in the Review of the GC PSA Methodology (Continued)

Topic	Observations
Dependent Events Analysis	AECL obtains generic beta factors from NUREG/CR-2098, NUREG/CR-2770, NUREG/CR-3289, and NUREG-0666 (Section 5.3.5, Component Types and Boundaries). This data may be outdated because it nominally covers information from 1972–1981. In addition, the nuclear industry NPP population is much different today.
Human Reliability Analysis	The extent of elucidation of talk-throughs given in the GC PSA methodology is provided in the following statement: "In the evaluation of preaccident tasks for an existing plant design, the calibration, test and maintenance procedures and practices are reviewed for each front-line and support system." The lack of information regarding the GC PSA review of procedures means that an assessment of the completeness of this subtask cannot be made. Because walkdowns and talk-throughs are not feasible for the ACR-700, it is reasonable to expect that AECL will perform a minimal qualitative analysis and use conservative HEPs.
Human Reliability Analysis	It is unknown if human error activities are to be screened out based on an assessment of how plant-specific operational practices limit the likelihood of errors in such activities.
Human Reliability Analysis	The GC PSA (Section 6.3.3, Performance Shaping Factors) states that "PSFs, other than recovery factors, dependence effects and radiation, are implicitly included in the basic human error probabilities (BHEP) and assume average, or better human factors or conditions. Radiation is explicitly considered as a PSF in the pre-accident screening HRA." The lack of details precludes a review of the adequacy of what was done.
Human Reliability Analysis	There is no mention of uncertainties in the GC PSA sections on HRA. Not addressing HRA uncertainties in the section of HRA is contrary to the other sections in the GC PSA because uncertainties are evaluated in each individual task.
Human Reliability Analysis	Errors or omissions in the GC PSA include the lack of discussion on HRA event tree development, sensitivity analyses, no clear interaction with systems analysts, and no person-to-person dependencies.
Human Reliability Analysis	Because no discussion is given concerning the development of the HRA event trees, the incorporation of RFs is assumed to be directly into the system fault trees. If so, this implies that procedures are not broken down into specific steps. It is not understood how these RFs are incorporated into the PRA.
Seismic Events Analysis	The potentially reduced scope of the seismic walk-down of the site could be viewed as a weakness. This is also true for the component screening preliminary calculation.

Table 4. Summary of Reporting Weaknesses Identified in the Review of the GC PSA Methodology (Continued)

Topic	Observations
Seismic Events Analysis	How the high confidence of low probability of failure (HCLPF) is used to screen out components from further analysis is mentioned but not explained in Appendix B.
Seismic Events Analysis	It is not clear that variations in reinforcement locations within the concrete are considered, that is, there is some randomness of the structure from location to location, and no location may match the "design," "theoretical," or "perfect" model for the structure.
Seismic Events Analysis	The GC PSA methodology report does not specify what standards or requirements the MSL is qualified for and implies that the main steam header is not important (as it is not qualified). Thus, it appears that the GC PSA does not consider the effects of a main steam header break (double guillotine type LOCA).
Fire Events Analysis	If uncertainties in the fire analysis are explicitly addressed in the GC PSA, it was not included in the methodology report.
Fire Events Analysis	Containment response to fire events was not addressed in the fire analysis section of the GC PSA methodology report.
Fire Events Analysis	The GC PSA states "that it would take about 55 minutes for the hot gases to damage the cable trays that carry the other train." This value of 55 min is used throughout this appendix. The basis for the 55 min has not been provided.
Fire Events Analysis	Details of the fire scenario under analysis are provided in second-tier documentation and not in the GC PSA methodology report.
Flood Hazard Analysis	Although the GC PSA evaluates equipment failing because of submergence or sprayed water, it is not clear that dynamic effects are addressed in the GC PSA; this is considered to be a weakness in reporting.
Flood Hazard Analysis	Details of the quantification of the flood analysis are limited in the GC PSA. Event trees are used in the GC PSA methodology, but code-specifics are not given. Method-specific limitations, uncertainties, and the review of the important contributors to CDF are not given in the GC PSA flooding assessment methodology.
Flood Hazard Analysis	The CANDU method lists sensitivity analysis as a major task. However, no details are provided in the chapter of flood analysis. The lack of details such as uncertainties associated with sparse or inadequate data, uncertainties in the models used to calculate flood variables, uncertainties and variabilities in the failure limits of components and structures, uncertain increases in component-failure rates in abnormal flooding environments, and other uncertainties associated with risk estimation in performing sensitivity analyses is considered to be a weakness in reporting.

Table 4. Summary of Reporting Weaknesses Identified in the Review of the GC PSA Methodology (Continued)

Topic	Observations
Flood Hazard Analysis	Although there is a list of minimum mechanisms to be considered in the GC PSA flooding hazard evaluation, not all of the "minimum" mechanisms listed are specifically addressed in the CANDU methodology report.
Flood Hazard Analysis	The flood scenario frequencies are reduced by empirical factors (<1) that lower the frequency used in the screening analysis; however, no reference is given in the GC PSA for these "empirical factors" (factors include location, direction, propagation, severity, and operator).
Flood Hazard Analysis	For a flood analysis, it is necessary to identify both the source locations (i.e., the locations where floods are most likely to start) and the critical impact locations (i.e., the locations where the existence of a flooding condition would have the greatest impact on the availability of key safety-related systems). Not addressed in the CANDU methodology report is frequency analysis to estimate the conditional frequency of exceeding levels of accident consequences, given the occurrence of each flood-damage state.
Flood Hazard Analysis	The CANDU methodology report's chapter of flood analysis does not cover accident consequences.
Flood Hazard Analysis	Section 9.2.2.1 (Evaluation of Flood Frequencies) states that they are going to only use the flood initiation frequencies for each flood area based on CANDU operating experience. There are two exceptions to the use of CANDU operating experience—expansion joint failure frequency and tank failure frequency. Section 9.2.3.2.3 states that "The failure rate [for expansion joints] includes external leaks, therefore, it is conservative to be applied in the flooding PSA and therefore not selected." Similarly, Section 9.2.3.2.4 states that "the failure frequency [for tank ruptures] is considered too conservative for use in this flooding PSA methodology" because the failure frequency is for all types of failure modes rather than just ruptures. For pipe break probabilities, if there is insufficient experience, it would seem more appropriate to use generic pipe break frequencies.
Flood Hazard Analysis	The GC PSA implies that AECL has information related to expansion joint failure frequency based on its own CANDU reactors and concludes that their experience is not applicable to their next generation design (ACR-700), but a foreign reactor design's (U.S. design) is applicable. No evidence is provided to support the conclusion that AECL's expansion joint design for the ACR-700 should not experience a similar failure rate to what other CANDUs have experienced.
Flood Hazard Analysis	The GC PSA states that the CANDU's experience data for the frequency of external leaks for tanks is 2.3×10^{-3}/year. The methodology report further states that because this frequency "is for all types of failure modes," it is considered too conservative for use in this flooding PRA methodology. The difference between leakage and rupture is not defined.

Table 4. Summary of Reporting Weaknesses Identified in the Review of the GC PSA Methodology (Continued)

Topic	Observations
Flood Hazard Analysis	The GC PSA quotes two PWR tank rupture rates and then selects the smaller rate. The basis was not provided for selecting the rupture frequency of the PWR refueling water storage tank (2.3 × 10^{-4}/year) instead of the PWR feedwater storage tank (2.8 × 10^{-4}/year).
Flood Hazard Analysis	The GC PSA discusses the determination of the flooding rate using pumps, orifices, and maximum pipe flows. It does not address determination of the flow rate from failed tanks. Specifically, it does not address evaluating the tank leakage that could cause unacceptable component degradation.
Flood Hazard Analysis	The flood flow ***rate*** is used to calculate time available for operator action to mitigate a flood, instead of a *time* based on the flow rate and the available free volume until adversely affecting equipment. The equation used to estimate "orifice flow rate" is stated with no reference or development.
Flood Hazard Analysis	The GC PSA states that "If all the required information for estimating the flood rate is not available (e.g., the operating pressure of piping flooding sources is not available), then the orifice flow rate is estimated using the pump discharge pressure." However, there is no discussion about uncertainties or whether this results in a conservative estimate of flow rate.
Flood Hazard Analysis	The equation used to estimate "maximum flow rate of piping" is stated with no reference or development.
Flood Hazard Analysis	The GC PSA states that "If both the operating pressure at the orifice point and the pump discharge pressure are not available, then the normal pumping flow rate, multiplied by the number of operating pumps is used for the flood flow rate." However, there is no discussion about whether this results in a conservative estimate of flow rate. Nor does it discuss pump "run-out" flow rates if discharge pressure is reduced to atmospheric, etc.
Level II PRA	The meaning of "unique" containment features in performance of the Level II analysis is undefined. No discussion is provided as to why only unique feature are important.
Level II PRA	Neither of the special cases of IEs nor plant damage states (calandria vessel rupture and containment isolation after an accident) appear to be addressed in the GC PSA. In addition, there is no mention that failure modes or studies from similar plants were reviewed in identifying the IEs.
Level II PRA	Although the GC PSA provides an outline of the general approach to performing a Level II PRA, specific details such as binning characteristics, potential containment-failure modes and mechanisms, and plant input data to core-melt codes are not given. Further, details such as developing CETs based on timing of events are not discussed.

Table 4. Summary of Reporting Weaknesses Identified in the Review of the GC PSA Methodology (Continued)

Topic	Observations
Level II PRA	Although uncertainty and sensitivity analyses are covered in general in previous chapters, they are not specifically addressed in the Level II analysis.
Level II PRA	The GC PSA addresses the analysis of severe accident phenomena and containment system analysis but did not clearly identify evaluating the containment structural capability.

Table 5. Summary of Methodology Strengths Identified in the Review of GC PSA Methodology

Topic	Observations
Overall	The overview of the GC PSA process is provided in GC PSA Figure 3-1 and is based on Figure 2-1, "Risk Assessment Procedure," of NUREG/CR-2300. As such, the methodology follows typical practices by using PRA as an analytical technique used to integrate the many different aspects of design and operation to determine core damage frequency and risk to the public.
Internal Events Analysis	The GC PSA uses a systematic, structured process for identifying IEs that challenge plant operations and that require successful mitigation. The events are grouped according to similarity of plant response, into a single, bounding, higher-level event. Safety systems that are required to operate are identified, along with its success criteria and any required support systems.
Internal Events Analysis	The CANDU methodology appears to set the event tree sequences based on a time of response.
Internal Events Analysis	The GC PSAs uses a 16-digit event identifier nomenclature in its qualification codes. This effective labeling scheme is helpful in interpreting the results of the computer analysis, because only the labels (and not the full descriptions) for the failure events are retained in the evaluation process. However, the use of a 16-digit identifier does not reduce the importance of a complete text description.
Internal Events Analysis	Although the uncertainty on the completeness of a PRA cannot be quantified, efforts were made to minimize their impact by adopting a highly systematic approach to event identification.
Internal Events Analysis	The GC PSA addresses modeling uncertainties "by making conservative modeling assumptions in the safety analysis."
Internal Events Analysis	Parameters uncertainties are assessed using a Monte Carlo technique to determine the uncertainty of system failure probabilities or accident sequence frequencies such as failure rates, component unavailabilities, IE frequencies, and human error probabilities.
Dependent Failure Analysis	The process of selectively reducing the number of causal groups and CCF component groups is consistent with the NRC-proposed Phenomena Identification and Ranking Table (PIRT) method as described in SECY-03-0059.
Human Reliability Analysis	The HRA process is consistent with current HRA techniques and is easy to follow. NUREG/CR-2300 was published in January 1983. However, the documents cited frequently in the GC PSA are NUREG/CR-1278, NUREG/CR-4772, and NUREG/CR-4550, which were published after NUREG/CR-2300.
Human Reliability Analysis	Three different behaviors are modeled for human actions in the GC PSA: (1) skill-based; (2) rule-based; and (3) knowledge-based using NUREG/CR-4772.

Table 5. Summary of Methodology Strengths Identified in the Review of GC PSA Methodology (Continued)

Topic	Observations
Human Reliability Analysis	The GC PSA assesses the HEPs for the type of task and stress level based on the values in Table 8-5 of NUREG/CR-4772 and in Table 7.3-14 of NUREG/CR-4550.
Human Reliability Analysis	For dominant sequences that contain operator error actions, AECL reevaluates the sequences using NUREG/CR-1278 to recalculate the HEP, or alternatively, the paired comparison/expert judgement method, given in NUREG/CR-3688. Particular attention in the GC PSA is given to modeling the postaccident execution errors in accordance with international practice.
Seismic Events Analysis	AECL recognizes the importance of defining and identifying component failure modes and recognizes that components have more than one failure mode. In addition, failure modes such as soil liquefaction, toe-bearing, base slab uplift, and slope instabilities are also considered as possible failure modes in the GC PSA.
Seismic Events Analysis	The methodology for seismic fragility analysis in Appendix B of the GC PSA is consistent with the standard process and philosophy of NUREG/CR-2300 and is easy to follow.
Seismic Events Analysis	The HRA methodology to be used for the GC PSA seismic PRA follows currently accepted practices.
Seismic Events Analysis	Although NUREG/CR-2300 does not specifically address HRAs in its discussion of seismic analyses, AECL specifically includes and discusses operator actions and its placement in the seismic event trees.
Seismic Events Analysis	Screening out unimportant locations in a seismic event analysis can greatly reduce the amount of work required without sacrificing significant confidence in the results. However, with the GC PSA methodology, events and locations of interest are screened out after the data tables are compiled. The retention of lost information in the data tables is a strength although the use of a screening criteria can be a weakness.
Fire Events Analysis	AECL accounts for human error probabilities throughout its fire hazard analysis.
Fire Events Analysis	Data for the fire events analysis is supplemented with data from U.S. LWRs to provide a larger database of historical records; this is an advantageous use of existing information to supplement sparse data.
Fire Events Analysis	AECL is proactive in considering fire risk studies at the conceptual or detailed design stage.
Flood Events Analysis	The GC PSA flood analysis identifies flood areas, flood sources, and propagation paths; estimates the IE frequency; and quantifies the flood-induced accident sequences.

Table 5. Summary of Methodology Strengths Identified in the Review of GC PSA Methodology (Continued)

Topic	Observations
Flood Events Analysis	The GC PSA flood analysis identifies and quantifies the flood scenarios/sequences that contribute to CDF and LERF.
Flood Events Analysis	The GC PSA adequately describes core damage probability calculations for flood scenarios for the CANDU plants by addressing the major tasks of a flood analysis, i.e., identifying flood areas, identifying flood sources, identifying propagation paths, estimating IE frequency, and quantifying flood-induced accident sequences.
Level II PRA	The Level II PRA analysis in the GC PSA methodology document identifies the plant damage states (although PDSs are defined for both limited core damage accidents and severe core damage accidents, the Level 2 analysis only considers severe core damage accidents.), the development of the CETs, and the analysis of the containment system performance.
Level II PRA	In its containment events analysis, the GC PSA does not make any comparisons or references to other risk studies. Thus, it appears that the GC PSA provides the complete set of CETs that were modeled.

Table 6. Summary of Methodology Weaknesses Identified in the Review of GC PSA Methodology

Topic	Observations
Internal Events Analysis	Data for component reliability is obtained from operating CANDU plants, in particular OPG's generating stations, IEEE Standard 500, and the NPRDS database system. Although none of these sources (IEEE Std. 500 and NPRDS) were reviewed and the veracity of the data was not confirmed, the age of the data is viewed as a weakness (1984 and 1983 respectively).
Internal Events Analysis	Care must be taken when using the Chi-square distribution for uncertainty because a credible uncertainty distribution may be broader than suggested by the Chi-square confidence bounds if issues such as the applicability to the ACR design of generic data, plant-to-plant variability, etc. are taken into account.
Internal Events Analysis	The GC PSA addresses modeling uncertainties "by making conservative modeling assumptions in the safety analysis." The problem with using "conservative modeling assumptions" to address modeling uncertainties is that an analyst does not always know that the assumptions are, in fact, conservative. Modeling uncertainties should be addressed through sensitivity analysis. Current regulatory practice is to address uncertainty in PRA results by applying defense-in-depth concepts.
Dependent Events Analysis	The GC PSA states that motor-operated valves, air-operated valves, pumps, air compressors, air coolers, heat exchangers, batteries, diesel generators, and switches/transmitters are to be modeled as part of the CCF analysis. Components not listed in GC PSA are circuit breakers, check valves, strainers, relief valves, and safety valves.
Dependent Events Analysis	If AECL updates its UPM values with NUREG information, they would need to justify the use of this data. Regardless, AECL should fully document the implementation of the UPM in its PSA.
Dependent Events Analysis	The beta-factor method is most useful for analyzing dependent failures in systems with limited redundancy (two or three units). Thus, the UPM method allowing up to five redundant "units" appears to overrun the capabilities of the beta-factor method that is its foundation. (Being limited to $\leq$5 redundant units is also considered to be a weakness). However, this issue is not specific to the UPM and the application of the beta-factor approach to highly redundant systems is generally believed to be conservative.
Dependent Events Analysis	In applying a refined partial beta-factor method some second-order cutsets may be lost. The GC PSA notes that the loss of the physically meaningful second-order cut sets is an artifact of all beta-factor CCF techniques and that MGL and other methods have the advantage of preserving such combinations.
Dependent Events Analysis	AECL indicates that HRA interactions have the potential for double counting because the MMI and safety subculture subfactors overlap. The GC PSA does not propose how to overcome this deficiency.

Table 6. Summary of Methodology Weaknesses Identified in the Review of GC PSA Methodology (Continued)

Topic	Observations
Dependent Events Analysis	The GC PSA indicates that staggered testing is not addressed in the UPM method.
Dependent Events Analysis	Although the evaluation of external events is mentioned, it is not known if the event-specific models were used in conjunction with computer-aided analyses to identify IEs. If identifying physical interactions was done, the extent that computer-aided analyses were used in the GC PSA is unknown.
Human Reliability Analysis	Preaccident tasks may include elements of skill-based, rule-based, or knowledge-based behavior. The GC PSA models only rule-based behavior when assessing preaccident tasks.
Seismic Events Analysis	The GC PSA states that "In some cases, it is not necessary to check all components of each equipment type, but only to check a representative piece." This phrase indicates that some equipment will be left out of the seismic walk-down.
Seismic Events Analysis	The safe shutdown equipment list will not normally include manual valves, check valves, small relief valves, passive equipment, or solid state relays.
Seismic Events Analysis	In order "to reduce the amount of effort that is required to solve event trees, and to reduce the number of components in the Boolean equations," AECL proposes that "If a component contributes less than 1×10^{-6}/year to core damage, then the contribution is considered minimal, and it can be screened out." Possible significant events could be inadvertently screened that on further investigation could have a more realistic assessment and could have a final estimated frequency above 1×10^{-6}/year.
Seismic Events Analysis	Section B.4 (Equipment Qualified by Testing) states that "cabinets are usually well constructed and resilient. Experiences have shown that as long as the cabinet does not collapse, the equipment mounted inside usually continue to function." Virtually every cabinet will be different; thus, each cabinet should be assessed independently and not providing a discussion as such is considered a weakness.
Fire Events Analysis	The screening approach of the GC PSA uses methods that allow *most* fires to be screened out without the need for detailed investigation and this is considered a weakness.
Fire Events Analysis	"Generally, events with smoke and no fire are not included, as well as those that involve arcing, sparking, explosions, and other short bursts of energy that fail to result in ignition." In the AECL methodology, the initiation of a fire is considered to be the point where a flame occurs. This fails to take into consideration the effects of smoke in adjacent areas (as doors are opened for access to the fire) to imped access and for the potential of water misdirection by the fire brigade (delaying fire suppression).

Table 6. Summary of Methodology Weaknesses Identified in the Review of GC PSA Methodology (Continued)

Topic	Observations
Fire Events Analysis	The GC PSA fails to consider smoke, its caustic effects, and its propagation through the plant.
Fire Events Analysis	It is not clear if explosion events that involve mechanical effects but no fire are considered; this includes explosion events of high-voltage switchgear and transformers. In addition, it is unclear how one would know *á priori* that an explosion will not generate, either by itself or as the result of impacting something else, a fire.
Fire Events Analysis	The frequency of each fire event is calculated by totaling the number of events (occurring during power operations and shutdown) during the time for plant operation (years) multiplied with the plant availability factor during this time. Because plant availability is based on plant operation, this could underpredict the frequency.
Fire Events Analysis	The GC PSA identified cable damage and ignition temperatures of 662 °F and 932 °F, respectively. Both the cable damage and ignition temperatures should be the same temperature, in AECL's case 662 °F. In addition, cables that do not meet IEEE-383 standard need to have a significantly lower cable damage and ignition temperature, specifically 425 °F.
Fire Events Analysis	The human error probabilities for actions outside of the control room during a fire event are the same as those in the internal events assessment. This does not consider the potential influences of stress, time availability, fire location, accessability, available paths to the fire (or remote equipment that needs to be operated locally), smoke levels, use of breathing apparatuses, barriers to communication, relevant training and experience, adequacy of indication in the main control room and at local sites, effects of spurious signals and alarms, and the number of concurrent actions needed on the individual's performance.
Fire Events Analysis	The GC PSA states that the time to reach a failure temperature would be different for different compartments, fire locations, fire sources, and cable specification and that a separation of approximately 4.5 ft is sufficient to prevent failures, except from hot gases. This has not been acceptable to the NRC. Appendix R and the Standard Review Plan, Chap. 9.5, requires a minimum free space separation of 20 feet.
Fire Events Analysis	The GC PSA states that if the fire is not explosive and the switchgear is sealed, the fire will not propagate. This implies that fires may be explosive and switchgear is not explosive. Switchgear can be very explosive, and a fire may result in such an explosive condition.

Table 6. Summary of Methodology Weaknesses Identified in the Review of GC PSA Methodology (Continued)

Topic	Observations
Fire Events Analysis	The GC PSA states that fires (transient, transformer, or switchgear) cannot damage or ignite cables if they are located more than 9 ft above the floor. The basis for this assumption and discussion on the hot gas layer has not been provided. Based on the IPEEE reviews, this appears to be an unfounded assumption.
Fire Events Analysis	The GC PSA states that "since it is judged that transient fires cannot cause damage to more than two cabinets, the impact of damage to this equipment is not considered further." The basis for this judgement has not been provided. Based on the IPEEE reviews, this appears to be an unfounded assumption.
Fire Events Analysis	The GC PSA states under that with one-half the floor covered by cable trays and the cable trays 9 ft above the floor, the factor for transient fires is 0.5. There is no discussion on the damaging effects of the hot gas layer. A hot gas layer could fail all the cables (depending on the temperature of the layer and the qualification of the cables).
Fire Events Analysis	The GC PSA discusses very briefly the use of severity factors. The severity factor approach does not fully consider plant-specific and scenario-specific features that may significantly influence the development of a given fire scenario.
Fire Events Analysis	Fire location is explicitly treated in the partitioning of fire event frequencies to specific fire areas, specific locations within a fire area, and/or specific fire sources. Hence, use of a severity factor in addition to fire source partitioning factors may also represent double counting.
Fire Events Analysis	There is also a potential for optimism in the severity factor approach depending on the how the severity factors were implemented and on case-specific details of the quantified scenarios.
Flood Hazard Analysis	NUREG/CR-2300 states "The following mechanisms should be considered at a minimum: loss of structural integrity through collapse, sliding, overturning, ponding, excessive impact and hydrostatic loads; flooding and wetting of equipment from seepage through walls and roof; flow through openings; sprays, thermal shocks, missile impacts; and the blockage of cooling-water intakes by trash." The GC PSA specifically excludes seepage through walls.
Flood Hazard Analysis	The GC PSA indicates that the collapse of walls or leakage through construction joints need not be considered because the leakage rates are minor, and they can be easily accommodated by installed drainage systems. The GC PSA does not evaluate the loss of structural integrity through collapse, flooding and wetting of equipment from seepage through walls, and the potential for structural failure (e.g., doors, walls) because of flooding loads.

Table 6. Summary of Methodology Weaknesses Identified in the Review of GC PSA Methodology (Continued)

Topic	Observations
Flood Hazard Analysis	The GC PSA identifies internal flooding causes from breaks and leaks in major water systems. Lacking appears to be internal causes such as the overfilling of tanks; sump-pump malfunctions; the backing up of drains, human-induced mechanisms that could lead to overfilling tanks, diversion of flow through openings created to perform maintenance; and inadvertent actuation of fire suppression.
Flood Hazard Analysis	The GC PSA states that the screening criterion for a flood hazard analysis is a frequency of 1×10^{-6}/year. Possible significant events could be inadvertently screened that on further investigation could have a more realistic assessment and could have a final estimated frequency above 1×10^{-6}/year.
Flood Hazard Analysis	The GC PSA states that operators can isolate a flooding source before it affects safety functions. This is not necessarily true for tank failures. Indeed "keep full" systems could sense the level reduction and start adding more water into the failed tank. The water provided by such systems should be included in the flooding assessment.
Flood Hazard Analysis	Drain obstruction from the failure of any check valve or drain blockage is addressed in the GC PSA. However, backflow through drains, which has been observed in operating NPPs, is not addressed.
Level II PRA	Not considering a main feedwater line break is considered to be a weakness.
PSA Methodology Overview	The GC PSA analysis report specifically performs a shutdown event analysis. The GC PSA methodology report does not specifically address shutdown events. The analysis report states that "The method used for event tree analysis and HRA is described in" the GC PSA methodology report. The analysis report then addresses modeling issues related to a shutdown state PSA. It is considered to be a weakness that shutdown event analysis is not addressed in the methodology report.

5. GC PSA—REFERENCE ANALYSIS

Because the PRA methodology and analysis reports cover the same information and rely on the same methodology, the comparison to two PRA standards—NUREG/CR-2300 and ASME R-SA-2002—are made in the review of the GC PSA methodology document (see Section 4 of this report).

5.1 Section 2, "Description of CANDU 6 Reactor;" Section 8, "CANDU 6 Shutdown Events Analysis;" Appendix J, "CANDU 6 Shutdown Events Analysis—Supporting Information;" and Appendix K, "CANDU 6 Shutdown Events Analysis—Event Trees"

Section 2 (Description of CANDU 6 Reactor) indicated that the CANDU 6 design is a pressure tube type reactor with heavy water to be used as both the moderator and coolant. Ordinary water would be used on the secondary side to generate steam for the main turbines. Two safety groups and associated support systems would meet the shutdown decay heat removal and postaccident monitoring requirements. There are two emergency shutdown systems—both are functionally different and physically separated. One system consists of mechanical shutdown rods that are functionally different from the moderator poison injection system. The other system injects a concentrated solution of gadolinium nitrate into the low-pressure moderator.

Section 8 (CANDU 6 Shutdown Events Analysis) addresses the shutdown state concerns that are in addition to those that are addressed in a full-power operation PRA. These concerns include 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 PRA can provide insight for outage planning, plant operations and procedures during an outage, outage management practices (e.g., maintenance restrictions), and design modifications aimed at lowering the risk of core damage.

Appendix J (CANDU 6 Shutdown Events Analysis - Supporting Information) calculated and presented in tabular form the IE frequencies, the human error probabilities, and the branch point probabilities for the total loss of service water.

Appendix K (CANDU 6 - Shutdown Events Analysis - Event Trees) presented one event tree. Actually, the event tree is presented in 12 parts, because the event tree was too large to be placed in one drawing. All branch point probabilities are listed and each sequence has been quantified.

5.1.1 Methodology

Section 3 describes the CANDU 6 reactor and does not present any information regarding methodology.

The methodology for the shutdown events analysis follows the internal events methodology described in the *Generic CANDU Probabilistic Safety Assessment - Methodology*[6] (see Section 4.2 of this report).

Section 8 (CANDU 6 Shutdown Events Analysis) performed a PRA for CANDU 6 shutdown conditions. Additional issues beyond those that were addressed in the full-power PRA are discussed. Seven initiating events (IEs) were identified. The event tree for these seven IEs were assessed as part of the analysis; however, only one IE was discussed in detail. The IE frequencies were developed from past CANDU PRA experience. Two plant shutdown states were considered: (1) reactor shutdown and the heat transfer system is cold, depressurized and full; and (2) reactor shutdown with the heat transfer system drained to the header level. The modeling of these two plant states, along with the operator actions required to handle accidents while the plant is in these states, for the analysis was extensively developed. Plant outages were also considered. The HRA for operator response was analyzed in detail since the plant conditions for shutdown are unusual and any events that occur while shutdown almost always require operator action.

The analysis determined that the most risk dominant IE was the total loss of service water because shutdown cooling is completely disabled by the loss of service water. As a result, the total loss of service water IE was thoroughly discussed and analyzed. A core damage of 1.51×10^{-5}/year was calculated for this case (i.e., when there was a total loss of service water and the reactor was in "drained to the headers level" configuration). The two dominant accident sequences for this analysis were also presented.

5.1.2 Strengths and Weaknesses

Section 3 (Description of CANDU 6 Reactor) is detailed enough to understand only the simplest structure and functions of the CANDU 6 reactor. No detailed description of front-line systems or associated plant diagrams were given.

The presentation of Section 2 is consistent with standard techniques and is easy to follow.

The level of detail was excellent for the material presented in Section 8 and Appendices J and K. The review found no inconsistencies or errors.

A minor concern was discovered in Section 8.6, Items t and v.

Item t states:

> If the reactor is in a GSS, then (1) the moderator purification system shall be isolated, with the closed isolation valve padlocked; (2) any source that could add D_2O to the moderator shall be isolated and locked closed; and (3) and at least one shutdown system shall be poised.

Item v states:

> When the reactor is in any other condition than a GSS, both shutdown systems must be fully available and poised.
>
> As far as practical, the maintenance of the regulating system and of the neutron power instrumentation associated with the shutdown systems is to be avoided during shutdown conditions.

The entry for "Total HEP" for the branch or top event "OPEWS4" in Appendix J could not be verified. This is possibly a typographical error since the top event does not appear in the event tree in Appendix K.

Results for the two dominant accident sequences were verified and no errors or inconsistencies were noticed. The IE frequencies and HEP factors were all verified and no errors or inconsistencies were found. The core damage frequencies for several sequences of the event tree in Appendix K were hand calculated based on the event tree branch probabilities provided and were verified to be correct. Further, these sequences were determined to be consistent with the methodology and no errors, omissions, or inconsistencies were found.

5.2 Section 3, "Description of CANDU 9 Reactor;" Section 11, "CANDU 9 Shutdown Events Analysis;" Appendix P, "CANDU 9 Shutdown Events─Supporting Information;" and Appendix Q, "CANDU 9 Shutdown Events Analysis─Event Trees"

Section 3 (Description of CANDU 9 Reactor) provides a general description of the CANDU 9 plant design requirements and system descriptions. The CANDU 9 is similar to the CANDU 6 design; however, it is based on a single-unit adaptation of the 900-MW(e) class of reactors currently operating in Canada as four-unit sites.

Section 11 (CANDU 9 Shutdown Events) provides a preliminary shutdown state analysis to demonstrate the adequacy of the single-unit CANDU 9 plant design to events that occur during reactor shutdown. The IEs analyzed included loss-of-offsite power, loss of service water, loss of shutdown cooling, and leaks from the heat transport system. Detailed system fault trees were not developed because the system design(s) is not complete. The mitigating system unreliabilities are targets based on previous analyses of similar systems and/or engineering judgment.

Appendix P (CANDU 9 Shutdown Events Analysis - Supporting Information) calculated and presented in tabular form the IE frequencies, the human error probabilities, and the branch point probabilities for the total loss of service water.

Appendix Q (CANDU 9 - Shutdown Events Analysis - Event Trees) presented one event tree - loss of service water with the heat transport system drained to headers. The report stated that "other event trees are similar, but they credit different mitigating systems, depending on the IE." All branch point probabilities are listed and each sequence has been quantified.

5.2.1 Methodology

Section 2 describes the CANDU 6 reactor and does not present any information regarding methodology.

The methodology for the shutdown events analysis follows the internal events methodology described in the *Generic CANDU Probabilistic Safety Assessment - Methodology*[6] (see Section 4.2 of this report).

Section 11 (CANDU 9 Shutdown Events Analysis) performed a PRA for CANDU 9 shutdown conditions to demonstrate the adequacy of the single unit CANDU 9 plant design in response to events that occur during reactor shutdown. Additional issues beyond those that were addressed in the full-power PRA are discussed. Seven initiating events (IEs) were identified. The event tree for these seven IEs were assessed as part of the analysis; however, only one IE was discussed in detail. The IE frequencies were developed from past CANDU PRA experience.

The analysis determined that the most risk dominant IE was the total loss of service water with the heat transport system cold, depressurized, and drained to the header level.

5.2.2 Strengths and Weaknesses

The level of detail in Section 11 and Appendices P and Q is inadequate only because the CANDU 9 system design is incomplete. Thus, detailed system fault trees were not developed because the system design is not complete. Because system fault trees were not developed, the mitigating system unreliabilities are targets based on previous analyses of similar systems and/or engineering judgment.

The seven IEs evaluated in Section 11 on the CANDU 9 plant match up with 4 of the IEs presented in Section 6 on the CANDU 6 plant. Not addressed in Section 9 are loss of reactor regulation, loss of instrument air, and freeze plug failure.

5.3 Section 4, "CANDU 6 Internal Events Analysis;" Appendix A, "CANDU 6 Internal Events Analysis—Event Trees;" Appendix B, "CANDU 6 Emergency Water Supply System Reliability Analysis;" and Appendix C, "CANDU 6 Internal Events Analysis—Dominant Accident Sequences"

The GC PSA reference analysis report provides examples on:

1. the initiating events analysis,
2. event tree development,
3. system reliability analysis,
4. accident sequence quantification,
5. results and discussion, and
6. summary of IEs.

Not addressed in the reference analysis for IEs are

1. dependent failures,
2. human reliability,
3. data-base development,
4. plant damage states,
5. uncertainty and sensitivity analysis, and
6. quality assurance.

Appendix A (CANDU 6 Internal Events Analysis—Event Trees) is a compilation of all the event trees for the 59 internal events described in Section 4 of the report. The scope of work was to pick one representative event tree and review it. The small-break LOCA (SBLOCA) event tree was selected for its simplicity and because it was one of three event trees described in detail in Section 4.3.2 of the report.

Appendix B (CANDU 6 Emergency Water Supply (EWS) System Reliability Analysis) summarized the modeling of the EWS system that is to be used to evaluate the EWS system’s reliability.

Appendix C (CANDU 6 Internal Events Analysis—Dominant Accident Sequences) lists the sequences that were determined to be the most dominant in previous AECL CANDU 6 PSAs and are to be reassessed for the GC PSA. The reassessment is to take into account CCF, changes in HRA approach, and other assumptions.

5.3.1 Methodology

Identification of IEs is discussed in Section 4.2. This involves the identification of the mechanisms by which radioactive materials can be displaced and possibly impact public safety. A list of all possible internal IEs can then be developed from this identification process. This section further explains how a review of all the possible internal IEs can reduce the list of potential IEs to only those IEs that require evaluation. The review process identifies those events that can cause public exposure to radiation and also classifies the IEs into four categories. Category A IEs are from the safety report (this presumably is Reference 13), Category B IEs are from the systematic review of plant design for IEs, Category C IEs are from common cause events, and Category D are from very low frequency IEs. The PRA assesses Category B (which includes Category A IEs) and Category C IEs. A logic process is then used to review the plant systems and develop the initial list of IEs. The IEs are then grouped according to their respective effect on the plant. This reduced the initial list of IEs from 125 events to 59 events. The IE frequencies were then determined based on plant operating histories at the CANDU NPPs and mathematical derivations.

Section 4.3 describes the event tree development for each of the IEs. The event trees are used to quantitatively assess the IE accident sequences. Three typical event trees (small-break loss of coolant accident, steam generator tube rupture, and reactor transient) are discussed in more detail.

The methodology for the internal events analysis was already outlined in Section 4 of the GC PSA methodology report and Appendices A–C only implement that methodology.

5.3.2 Strengths and Weaknesses

Section 4 is very detailed for the material that is presented. The IE definitions are clear, concise, and complete.

Table 4-2 lists the IE frequencies of occurrence developed in Section 4.2.5. Some of the frequencies are presented without supporting documentation or references.

The five references for Chapter 4 were not consulted or reviewed; however, four of these references are user manual’s for the computer software that is used to produce event trees and quantify them. These references are not necessary for this review. The fifth reference is to the CNSC document that lists the IEs required (Reference 13).

The IE frequency database determination (Section 4.2.5) and its associated listing (Table 4-2) are not fully explained. For example, when operating plant history is used to determine the frequency, the frequency is usually presented without supporting documentation. Table 4-2 needs to have its column headers defined. In particular, it is not clear what the column headed by "dist" is used for. Table 4-2 indicates that the transient IE (IE-T) has a frequency of 2.8/year. This seems to a be rather conservative value.

The level of detail in Appendix A is good and is sufficient to assess the information presented in the appendix.

The SBLOCA event tree in Appendix A is legible, clear, and complete. The event tree is consistent with Section 4.3.2. Further, the event tree adequately represents the progression of the SBLOCA and the resulting sequences. No errors or omissions were found.

There was a possible typographical error in the second sentence of Section B.2.1- should PV8 be PV7? Section B.2.2 does not explain why boiler level instrument measurements that initiate opening of the main steam safety valves (MSSVs) are assumed to be from Group 2 of SDS2 Channels G, H, and J. In Section B.2.3 if the assumption that all four pumps are located in a common pump house is a conservative choice, then that assumption should be supported with additional information. This is also true of the assumption that the pumps have no common header, which should also be identified as a suction or discharge header. Most the entries in Tables B-1 and B-2 are from Reference 38 and were not be confirmed. The reviewer assumed that the entries in Tables B-1 and B-2 in the columns labeled "Category/Numerical Value" were taken from Reference 38 and are also called "subfactors." Again, these values were not verified, however, it is not clear why the values are summed at the bottom of the column. This last detail needs further explanation and development. In addition, further review of Table B-3 is needed. This represents a significant weakness in the review of the PRA.

The level of detail in Appendix C is adequate and is sufficient to assess the information presented in the appendix. Because of the extensive nature of Tables C-1, C-2, and C-3, a spot-check of the tables was performed. The spot-check did not identify any errors or omissions in the tables.

The large number of event trees found in Appendix A should have a more thorough review than the single event tree review performed for this study. Tables B-1 through B-3 require the use of Reference 38 for adequate verification. Because of the extensive detail of Tables C-1 through C-3, only a limited review was performed.

5.4 Section 5, "CANDU 6 Seismic Events Analysis;" Appendix D, "CANDU 6 Seismic Event Analysis—Mitigating Systems Heading Description;" and Appendix E, "CANDU 6 Seismic Events Analysis—Event Trees"

Section 5 (CANDU 6 Seismic Events Analysis) conducts a preliminary evaluation of the generic CANDU 6 design's response and vulnerability to seismic events. The evaluation assumes a CANDU 6 two-unit site. High seismic capacity items are screened out and the remaining components and structures are retained for evaluation in the PRA model. The evaluation first assesses status of systems expected to survive an earthquake (i.e., the seismically qualified systems). It is assumed that the failure of all nonseismically qualified equipment leads directly to core damage. If equipment in these systems are not failed, then the status of each nonqualified system is questioned. The results from a hazard 1 curve design basis earthquake [(DBE) level of 0.25 g] are compared to the results from a hazard 2 curve (DBE level of 0.2 g). The preliminary analysis indicated that the dominant contributors to the severe seismic core damage frequency for hazard curve 1 at a two-unit site are about 1×10^{-5}/year.

Appendix D (CANDU 6 Seismic Events Analysis—Mitigating Systems Heading Description) lists in tabular form all the top event labels from the seismic event trees found in Appendix E. Also listed in tabular form are the postaccident operator action. Both of these tables give a full explanation of the sequence of events that determine the top events.

Appendix E (CANDU 6—Seismic Events Analysis—Event Trees) contains the three event trees depicting the main seismic event tree and the two secondary seismic event trees.

5.4.1 Methodology

The methodology for the seismic events analysis is consistent with the methodology described in Section 7 of *GC PSA—Methodology*[6] (see Section 4.5 in this report). The methodology is consistent with standard techniques and is easy to follow The sequence quantification was performed using the EQESRA computer code.[69–71]

5.4.2 Strengths and Weaknesses

The level of detail is very good for the material that is presented in Section 5 and Appendices D and E. The review found no inconsistencies or errors.

With the exception of the methodology comments mentioned in Section 4.5.1 of this report, these appendices were of high quality, and the documentation was good.

In addition, the data presented in GC PSA Table 5-2 should be spot-verified to confirm the results.

5.5 Section 6, "CANDU 6 Fire Events Analysis;" Appendix F, "CANDU 6 Fire Events Analysis─Supporting Information;" and Appendix G, "CANDU 6 Fire Events Analysis─Event Trees"

Section 6 (CANDU 6 Fire Events Analysis) contains a preliminary assessment of the generic CANDU 6 response to fire events. Appendix F identifies the fire zones of a generic CANDU 6 plant and estimates the core damage frequency for those fire zones that are considered to be safety-significant. Appendix F also discusses the two fire scenario event trees provided in Appendix G. The first event tree describes the fire scenarios for the fixed ignition sources, and the second event tree describes the fire scenarios for transient fires. Appendix F also provides a description of each top event of both event trees in Appendix G and estimates the value for each top event. Fault trees were not developed for either fire scenario event tree.

If the water from the normal emergency source fails, then a gravity feed from the deaerator storage tank, located in the turbine building, can maintain the steam generator heat sink for an additional 8 hours. A sensitivity study showed that the combined effect of the gravity feed from the deaerator and fire retardant cables reduces the fire-induced core damage frequency from 2.40×10^{-5}/year to 2.77×10^{-6}/year.

5.5.1 Methodology

The methodology for the fire events analysis is consistent with the methodology described in Section 8 of *GC PSA─Methodology*[6] (see Section 4.6 of this report). The data sources[72-73] for estimating fire frequencies were not reviewed; however, data from U.S. LWRs from approximately January 1, 1964 through January 26, 1994, and from the COG from commercial operation of each CANDU plant through December 1997 was used. The use of more recent fire event data is considered to be advantageous. The methodology was not compared with the June 2003 draft of NUREG-1805.[74]

5.5.2 Strengths and Weaknesses

The level of detail was adequate for the material presented in Section 6 and Appendices F and G. The review found inconsistencies in the values used in the event tree shown in Figure G-2. These inconsistencies also caused the sequence results for this event tree to be inconsistent with an informal calculation.

Results for the "Fire Scenario Event Tree for FT174(1)" (see Figure G-2) were examined, and errors and inconsistencies were noticed. The values of 0.38 and 0.43 used for "Late Manual Fire Suppression" (LMFS) top event were not consistent with the documented value of 0.3 provided on page F-15 of Appendix F. In addition, the "Conditional Core Damage Probability" value of 1.54×10^{-6} used for FDS4 was not consistent with the documented value of 1.56×10^{-6} provided on page F-16 of Appendix F. The corresponding sequence probabilities for these two series were informally calculated to be 5.839 × 10^{-5} (instead of 5.77 × 10^{-4} as shown in Figure G-2) and 9.11 × 10^{-11} (instead of 8.88 × 10^{-10} as shown in Figure G-2). Further informal calculations were not performed. These inconsistencies represent a weakness in attention to details.

With the exception of the methodology comments mentioned in Section 4.6.1 of this report, this section and its associated appendices were of high quality, and the documentation was excellent.

The errors and inconsistencies noted in the Fire Scenario event trees questions the viability of the sensitivity study concerning fire retardant electrical cables and use of the deaerator as an alternate source of water.

A more comprehensive review of this section and its associated appendices should be performed when all references are collected and reviewed and NUREG-1805[74] is available in final form. The values used in all three event trees presented in Appendix G should be verified, and the resultant sequence values recalculated and verified. This represents a weakness in the review of the GC PSA analysis report.

5.6 Section 7, "CANDU 6 Flood Events Analysis;" Appendix H, "CANDU 6 Flood Events Analysis—Supporting Information;" and Appendix I, "CANDU 6 Flood Events Analysis—Event Trees"

Section 7 (CANDU 6 Flood Events Analysis) contains a preliminary assessment of the generic CANDU 6 response to flood events. Appendix H identifies the flood zones of a generic CANDU 6 plant and estimates the core damage frequency for those flood zones that are considered to be safety-significant. Appendix H also discusses the three flood scenario event trees provided in Appendix I. Appendix I provides an event tree for each of the three flooding areas that were deemed more significant and that contribute to the total core damage frequency of 8.96 × 10^{-7}/year. Fault trees were not developed for any of the flood scenario event tree top events.

The most significant flooding area identified in the report is FL-T02 [Recirculating Cooling Water (RCW) heat exchanger room], which contributes approximately 62% of the total CDF. The reported next most significant flooding area is FL-T06 (inverter room), which the report indicates contributes about 23% of the total CDF. These two flooding areas are reported to account for about 95% of the total CDF attributed to floods.

The flood area FL-T02 is located at the lowest elevation in the turbine building. This area contains four RCW heat exchangers, associated isolation valves, vacuum pumps, and other equipment. The flooding sources in this area are raw service water (RSW) and fire protection systems. The RCW system itself can also be a flood source, but is not considered because it does not affect the other safety systems.

The flood area FL-T06 (inverter room) contains Group 1, Class I and Class II electrical cabinets and other Group 1, Class III motor control centers (MCCs). The major flooding source is water from the fire hose cabinet.

5.6.1 Methodology

The methodology for the flood events analysis is consistent with the methodology described in Section 9 of *GC PSA—Methodology*[6] (see Section 4.7 of this report). However, the data source[65] for estimating flood frequencies was not reviewed and use of data from WASH-1400[64] does not reflect the availability of more up-to-date data. The use of data circa 1975 is considered to be a weakness.

5.6.2 Strengths and Weaknesses

The level of detail was not adequate for the material presented in Section 7 and Appendices H and I because it was difficult to associate the top events in the event tree with the unavailability values provided for those top events. This is considered to be a weakness in reporting.

Results for the "Flood Scenario Event Tree for FL-T02" (see Figure I-1 in the GC PSA reference analysis document) were examined and no errors were noticed. However, difficulties were encountered when trying to confirm the unavailability values used for the event tree top events. Specifically:

- the IE frequency was difficult to verify consistency with documentation because the value was "buried" in the text of Appendix H,
- the unavailability for the top event "Category of Flood" was moderately difficult to verify consistency because it was in Section 7, and
- the unavailability for the remaining top events could not be verified consistent with the documentation because the values could not be found.

Flood scenario event tree top events could not be associated with a single area, section, or subsection of Section 7 or Appendix H because they were not discussed by top event name in the section or appendix. This is considered to be a weakness in reporting.

The sequence probability of 1.26×10^{-3} for the dominant sequence was verified by an informal calculation. The associated sister sequence probability of 3.11×10^{-7} was also verified by a hand calculation based on the event tree branch probabilities provided. Both of these hand calculations used the unverified values provided in the event tree for IE frequencies and unavailabilities.

Section 7 and particularly Appendix H are not well-organized and, as such, difficult to associate with the top events in the figures provided in Appendix I. This represents an important weakness for reviewing the PRA.

Not using the analysis of more recent source data for flood IE frequencies is considered to be a weakness. Rewriting Section 7 and Appendices H and I to improve the organization to make any inconsistencies apparent would be beneficial.

5.7 Section 9, "CANDU 9 Internal Events Analysis;" Appendix L, "CANDU 9 Internal Events Analysis—Supporting Information;" and Appendix M, "CANDU 9 Containment Ventilation Isolation System Reliability (CVIS) Analysis"

Section 9 (CANDU 9 Internal Events Analysis) presents IE analysis and event tree development for the CANDU 9 NPP. The IEs are listed as are the dominant accident sequences.

Appendix L (CANDU 9 Internal Events Analysis—Supporting Information) describes the mitigating functions and their assigned vulnerabilities. The various mitigating systems are also described.

Appendix M (CANDU 9 Containment Ventilation Isolation System (CVIS) Reliability Analysis) completely describes the CVIS and how its reliability is determined. The predicted unavailability, 8.0×10^{-7}, of the CVIS (calculated via the event tree at the end of the appendix) is also developed.

5.7.1 Methodology

The PRA is performed in two stages. The preproject PRA (first phase) confirms the design concept. The second phase - identifying the IEs - is discussed in Section 9.2. This involves identifying the mechanisms by which radioactive materials can be displaced, thereby possibly impacting public safety. A list of all possible internal IEs can then be developed from this identification process. This section further explains how a review of all the possible internal IEs can reduce the list of potential IEs to only those IEs that require evaluation. A logic process is then used to review the plant systems and develop the initial list of IEs. The IEs are then grouped according to their respective effect on the plant. The IE frequencies were then determined based on plant operating histories at the CANDU NPPs and mathematical derivations.

Section 9.3 (Event Tree Development) describes the event tree development for each of the IEs. The event trees are used to quantitatively assess the IE accident sequences.

Appendix M describes the methodology for the CVIS reliability analysis.

5.7.2 Strengths and Weaknesses

Section 9 (CANDU 9 Internal Events Analysis) is very detailed for the material that is presented. The IE definitions are clear, concise, and complete.

Tables 9-2 and 9-3 in the GC PSA reference analysis document[7] list the dominant accident sequences for the plant damage states PDS1 and PDS2 respectively. However, this is considered to be a weakness because these frequencies are presented without supporting documentation or references.

The level of detail in Appendix L (CANDU 9 Internal Events Analysis—Supporting Information) is good; however, more information is necessary to assess the information presented in the appendix.

The supporting information in Appendix L is presented without reference documentation, nor are any calculations listed for verification. In almost all cases the reference CANDU PSAs are needed to duplicate or verify the unavailabilities. The large LOCA event tree is legible, clear, and appears to be complete; however, a more detailed review of this tree is needed.

While the system information presented is excellent, the UPM values presented in the section for the system's reliability and unavailability were not independently confirmed.

GC PSA References 20 and 38 were not reviewed in the performance of this task; consequently, the results of Appendix M could not be verified. More time and effort would be needed to properly evaluate the CCF analysis for CVIS and its associated unavailability.

A more comprehensive review would determine whether the process used for generating IEs and their frequency of occurrence is consistent with NRC, NRC-sponsored, and industry results. The grouping of the IEs, Tables 9-2, 9-3, and all the tables of Appendix L require review. There is a good deal of detailed information on the CVIS in Appendix M.

With the exception of the above comments in the methodology, level of detail, and results portions of this review, the appendices were of high quality and the documentation was good.

5.8 Section 10, "CANDU 9 Seismic Events Analysis;" Appendix N, "CANDU 9 Seismic Event Analysis—Supporting Information;" and Appendix O, "CANDU 9 Seismic Events Analysis—Event Trees"

Section 10 (CANDU 9 Seismic Events Analysis) conducts a preliminary evaluation of the generic CANDU 9 design's response and vulnerability to seismic events. The results from a hazard 1 curve (DBE level of 0.25 g) are compared to the results from a hazard 2 curve (DBE level of 0.2 g). The preliminary analysis indicated that the dominant contributors to the severe seismic core damage frequency for hazard curve 1 is about 1.7×10^{-6}/year and for hazard curve 2 is about 1.4×10^{-5}/year.

Appendix N (CANDU 9 Seismic Events Analysis—Supporting Information) describes and lists all the top event labels from the seismic event trees found in Appendix O. Also, different level event trees are described as well as their respective sequence quantification. System reliability and human error estimation are also detailed.

5.8.1 Methodology

The methodology for the seismic events analysis is consistent with the methodology described in Section 7 of *GC PSA—Methodology*[6] (see Section 4.5 of this report). This methodology, for the most part, is consistent with standard techniques and is easy to follow. The analysis did not include a derivation of the seismic hazard analysis. Instead, the site seismic information was used for seismic hazards. The mean seismic hazard curve was also used because it was judged by AECL to be sufficiently accurate. The sequence quantification was performed using the EQESRA computer code.[71] In Section 10.4 it was indicated, "The seismic design for the CANDU 9 structures and equipment is not yet finished."

Appendix N presents a description and quantification for various level 1–4 event trees. The top events from the event tree depicted in Appendix O are discussed in detail.

Appendix O (CANDU 9—Seismic Events Analysis—Event Trees) contains three event trees: one depicting the main seismic Level 1 event tree and two that illustrate the secondary seismic event trees (one level 2 and one level 3).

However, Section 9 and Appendices N and O all need to be more thoroughly reviewed.

5.8.2 Strengths and Weaknesses

The level of detail for the material presented in Section 10, Appendices N and O, is very good. However, the reporting of Section 10 is considered to be a weakness because Section 10 appears to be incomplete insofar as adequate documentation and explanation of the material presented (it appears as though many things were either left out or were overlooked in Section 10).

The review found no inconsistencies and only two minor typographical errors on page 10-4.

The results of Section 10 and Appendix N are clear, concise, and appear to be complete.

The information presented in Tables 10-1 through 10-5 needs to be verified or confirmed.

Section N.1.3.2.1.4 appears to be a repeat of Section N.1.3.2.1.3. There are inconsistencies between the event trees (Appendix O), their descriptions (Appendix N), and the figures in Appendix O. For example, Figures O-2, O-3, and O-4 all show a top event labeled SL. Appendix N (in Section N.1.3.1.1.1) indicates there is only one SL. However, Sl on Figure O-2 has no value, on Figure O-3 its value is 0.13 (0.87), and on Figure O-4 its value is 0.27 (0.73). It is not clear which value Figure O-2 uses. Also, the first level event tree (Figure O-1) appears to be acceptable, but it is not consistent with the level 2 and level 3 event trees. Any differences or similarities are not discussed. Inconsistencies between event trees without any explanation is considered to be a significant weakness on control and documentation.

The third-level seismic event trees (T1, T2, T3, T4, and T5) discussed in Appendix N are not presented in Appendix O as indicated. This is considered to be a significant weakness on control and documentation.

The calculations for human error estimates presented in Appendix N appear to be consistent (indirectly) with the standard techniques and methods of NUREG/CR-1278.[42] The sample calculations presented in Appendix N are not verifiable, nor are the human error probabilities assessments, which is a weakness.

The event trees of Appendix O could only be partially verified. Some sequences could be quantitatively verified by informal calculations; however, most of the sequences in Appendix O could not. The inability to verify sequence probabilities is considered to be a weakness. These event trees should be reviewed again following the resolution of the other comments concerning Appendix O.

5.9 Section 12, "Severe Accident Consequences Analysis for Level II PSA"

The computer code used to analyze severe accidents was MAAP4 CANDU;[69] however, the code was a beta version. Only the CANDU 6 was modeled for the analysis. It was not discussed why the CANDU 9 was not modeled, nor how the current reference analysis represents a generic application. The assumptions used are presumably derived from CANDU 6 references, but this was not stated directly. The inputs and results for two accidents were presented in sufficient detail to analyze if needed. AECL believes the results are "consistent with prior engineering judgement for the scenarios analyzed." Therefore, the use of the code and its current adaptation is viewed by AECL to "demonstrate the capability of the code for Level II PSA applications."

5.9.1 Methodology

The methodology is derived or adapted from five references.[69, 75-78] Because these references were not reviewed against the GC PSA, it was not possible to wholly verify the methodology reviewed.

5.9.2 Strengths and Weaknesses

The level of detail in this section was good for the material presented.

The MAAP CANDU code has not been reviewed by NRC and its acceptability has not been determined.

The figures used in this section to profile the two scenarios were too small to allow a detailed review of the results.

This section would need a more thorough review before any assessment of its overall adequacy could be made. There needs to be more information concerning how this preliminary analysis represents a generic application and why it can be done without applying the method or analysis to a CANDU 9 design. It would have been helpful in the review to have included some CETs with underlying fault trees to enhance the description of the accident scenarios in the analysis report; this is viewed as a weakness.

A more comprehensive review would determine whether this process used for generating the Level II PSAs would be viable or not. The methodology needs a thorough review to determine if this process is consistent with accepted PRA practices. This represents a major weakness in the review of the AECL PRA documents.

5.10 Summary

The reporting and methodology strengths and weaknesses noted from the review of the GC PSA reference analysis document are summarized in Tables 7–10.

Table 7. Summary of Reporting Strengths Identified in Review of GC PSA Reference Analysis

Topic	Observations
Shutdown Events Analysis (CANDU 9)	The shutdown events section in the GC PSA provides a preliminary shutdown state analysis to demonstrate the adequacy of the single-unit CANDU 9 plant design to events that occur during reactor shutdown. The IEs analyzed included loss-of-offsite power, loss of service water, loss of shutdown cooling, and leaks from the heat transport system.
Internal Events Analysis (CANDU 9)	There is a good deal of detailed information on the CVIS in Appendix M.
PSA Analysis Overview	The analyses performed for internal and external events follows that described in the GC PSA methodology report.

Table 8. Summary of Reporting Weaknesses Identified in Review of GC PSA Reference Analysis

Topic	Observations
Description (CANDU 6)	The description of CANDU 6 Reactor is detailed enough to understand only the simplest structure and functions of the CANDU 6 reactor. No detailed description of front-line systems or associated plant diagrams were given.
Flood Events Analysis (CANDU 6)	The level of detail was not adequate for the material presented in Section 7 and Appendices H and I because it was difficult to associate the top events in the event tree with the unavailability values provided for those top events.
Flood Events Analysis (CANDU 6)	Difficulties were encountered when trying to confirm the unavailability values used for the event tree top events for the "Flood Scenario Event Tree for FL-T02." Specifically, • the IE frequency was "buried" in the text of Appendix H, • the unavailability for the top event "Category of Flood" was in Section 7, and • the unavailability for the remaining top events could not be found.
Flood Events Analysis (CANDU 6)	Flood scenario event tree top events could not be associated with a single area or section because they were not discussed by top event name.
Flood Events Analysis (CANDU 6)	The flood events analysis sections are not well-organized and, as such, difficult to associate with the top events in the figures provided in Appendix I.
Flood Events Analysis (CANDU 6)	Errors and inconsistencies noted in the Flood Scenario Event trees questions the viability of sensitivity studies. A reorganization may be beneficial.
Internal Events Analysis (CANDU 9)	Tables 9-2 and 9-3 in the GC PSA reference analysis document list the dominant accident sequences for the plant damage states PDS1 and PDS2 respectively. However, these frequencies are presented without supporting documentation or references.
Internal Events Analysis (CANDU 9)	The level of detail in Appendix L (CANDU 9 Internal Events Analysis—Supporting Information) is good; however, more information is necessary to assess the information presented in the appendix.
Internal Events Analysis (CANDU 9)	The supporting information in Appendix L is presented without reference documentation, nor are any calculations listed for verification.
Seismic Event Analysis (CANDU 9)	The seismic event analysis provided in Section 10 appears to be incomplete insofar as adequate documentation and explanation of the material presented (it appears as though many things were either left out or were overlooked in Section 10).
Seismic Event Analysis (CANDU 9)	Section N.1.3.2.1.4 appears to be a repeat of Section N.1.3.2.1.3. There are inconsistencies between the event trees (Appendix O), their descriptions (Appendix N), and the figures in Appendix O.

Table 8. Summary of Reporting Weaknesses Identified in Review of GC PSA Reference Analysis (Continued)

Topic	Observations
Seismic Event Analysis (CANDU 9)	The third-level seismic event trees (T1, T2, T3, T4, and T5) discussed in Appendix N are not presented in Appendix O as indicated.
Seismic Event Analysis (CANDU 9)	The event trees of Appendix O could only be partially verified based on the event tree branch probabilities provided. Some sequences could be quantitatively verified by informal calculations; however, most of the sequences in Appendix O could not.
Level II PRA	The assumptions used are presumably derived from CANDU 6 references, but this was not stated directly.
Level II PRA	The figures used in this section to profile the two scenarios were too small to allow a review of the results.
Level II PRA	The Level II PRA section lacks information concerning how this preliminary analysis represents a generic application and why it can be done without applying the method or analysis to a CANDU 9 design.

Table 9. Summary of Methodology Strengths Identified in the Review of the GC PSA Reference Analysis Report

Topic	Observations
Fire Events Analysis (CANDU 6)	The data sources for estimating fire frequencies were not reviewed; however, data from U.S. LWRs from approximately January 1, 1964 through January 26, 1994, and from the COG from commercial operation of each CANDU plant through December 1997 was used.
Internal Events Analysis (CANDU 9)	The PRA is performed in two stages. The preproject PRA (first phase) confirms the design concept. The second phase - identifying the IEs - involves identifying the mechanisms by which radioactive materials can be displaced, thereby possibly impacting public safety. Thus, PRA is used early in the design.

Table 10. Summary of Methodology Weaknesses Identified in the Review of the GC PSA Reference Analysis Report

Topic	Observations
Fire Events Analysis (CANDU 6)	The review found inconsistencies in the values used in the event tree shown in Figure G-2. These inconsistencies also caused the sequence results for this event tree to be inconsistent with an informal calculation.
Fire Events Analysis (CANDU 6)	Results for the "Fire Scenario Event Tree for FT174(1)" (see Figure G-2) were examined, and errors and inconsistencies were noticed. The values of 0.38 and 0.43 used for the "Late Manual Fire Suppression" (LMFS) top event were not consistent with the documented value of 0.3 provided on page F-15 of Appendix F. In addition, the "Conditional Core Damage Probability" value of 1.54×10^{-6} used for FDS4 was not consistent with the documented value of 1.56×10^{-6} provided on page F-16 of Appendix F. The corresponding sequence probabilities for these two series were informally calculated to be 5.839×10^{-5} (instead of 5.77×10^{-4} as shown in Figure G-2) and 9.11×10^{-11} (instead of 8.88×10^{-10} as shown in Figure G-2).
Fire Events Analysis (CANDU 6)	The errors and inconsistencies noted in the Fire Scenario Event trees questions the viability of the sensitivity study concerning fire retardant electrical cables and use of the deaerator as an alternate source of water.
Flood Events Analysis (CANDU 6)	The using data from WASH-1400 (circa 1975) does not reflect the availability of more up-to-date data.
Seismic Event Analysis (CANDU 9)	Inconsistencies between event trees are not explained and there is no discussion of the differences and similarities between event trees.
Level II PRA	The computer code used to analyze severe accidents was MAAP4 CANDU; however, the code was a beta version. Only the CANDU 6 was modeled for the analysis. It was not discussed why the CANDU 9 was not modeled nor how the current reference analysis represents a generic application.
Level II PRA	The MAAP CANDU code has not been reviewed by NRC and its acceptability has not been determined.

6. PSA METHODOLOGY, ACR

Because the PRA methodology and analysis reports cover the same information and rely on the same methodology, the comparison to two PRA standards -NUREG/CR-2300 and ASME R-SA-2002 - are made in the review of the GC PSA methodology document (see Section 4 of this report).

6.1 Section 1, "Introduction;" Section 2, "Description of CANDU Design;" Section 3, "PSA Methodology—General;" and Appendix E, "General CANDU Single Unit Design Description"

An initial comparison with the *Generic CANDU Probabilistic Safety Assessment—Methodology*[6] report was made because of the similar nature of the two documents and repetitious descriptions used in each. As before, the generic CANDU PSA methodology document will be referred to as the GC PSA and the subject methodology document (*Probabilistic Safety Assessment Methodology, ACR*[8]) will be referred to as the ACR PSA.

Section comparisons

Section 1 of the ACR PSA is comparable to Section 3 of the GC PSA document. However, there are some differences and one similarity, as noted in the following table.

Table 11. Similarities and Differences Between ACR and GC PSA Methodology

Category	ACR PSA, Section 1	GC PSA, Section 3
Definitions	More	Less
Standard	Conforms to ASME RA-S-2002 Cat. I PRA	Conforms to NUREG/CR-2300
	Level I/II PRA	Level I/II PRA
Shutdown analysis	Included	Not included
Figure 2-1 in NUREG/CR-2300	Figure 1-1	Figure 3-1

General comparisons

The ACR PSA document is more thorough in its description of what is intended for the PRA compared to the GC PSA. The extensive lexicon of definitions of terms is far more comprehensive and thorough, and the program description is more detailed than the GC PSA document. In addition, the ACR PSA clearly states that the current PRA effort will be in accordance with the licensing basis document (LBD) for ACR.[79] This was not explicitly stated in the GC PSA documents.

6.2 Section 1, "Introduction;" Section 2, "Description of CANDU Design"

Section 1 describes the Level I and Level II PRA for the ACR design regarding internal events, seismic concerns, internal fire issues, and internal flooding issues. The introductory section also indicates that a shutdown PRA would be performed; however, no Level III PRA will be performed. The scope of the PRA is clearly defined, and the LBD[79] that is used to define the safety goals and design targets was not reviewed under this task. Many specific PRA terms, such as limited core damage and severe core damage accidents, are defined in Section 1.2. The LBD's safety goals of 1×10^{-5}/year for the ACR design is to be demonstrated via the PRA. Finally, the remaining chapters and the areas of study are introduced.

6.2.1 Methodology

The methodology follows typical practices because it follows the PRA process given in Figure 2-1 of NUREG/CR-2300. However, the ACR PSA is judged (by AECL) to be an ASME RA-S-2002 Category I PRA. However, the ACR PSA also states that

> 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 guidelines in developing the PSA methodology for the ACR program.

Thus, it is unclear what guidance the various tasks follow.

6.2.2 Strengths and Weaknesses

The presentation of Section 1 is consistent with standard techniques and is easy to follow. It is detailed enough to follow the methodology that will be presented in the following sections. However, not reviewing the references (because of time limitations) serves to limit the extent of this review, and the concerns regarding the information presented in Section 1.1 on Page 1-2 (discussed below) of the document need to be addressed before this section of the report can be considered complete.

Section 1.1, page 1-2, fourth paragraph, states that "The ACR™[*] design is intended to satisfy current licensing basis of the USNRC." It is unclear is this statement refers to the Standard Review Plan or some other NRC document. Also, the statement should specify what LBD is to be used as a standard or reference because the NRC does not have a "licensing basis" *per se.*

When reading the statement "Considering these, the appropriate capability category for satisfying the purpose of the ACR-700 PSA is judged to be Category I," it is not clear how the Category I classification was arrived at without more explanation. Many requirements for a Category II or III PRA are identical to a Category I PRA (i.e., only specific areas need additional work to meet the higher category requirements). Section 1.3 of the ASME Standard indicates "The required category of PRA capabilities may vary over different elements of the PRA." Further, "When a comparison is made between the capabilities of any given PRA and the supporting requirements (SRs) of this Standard, it is expected that the capabilities of a PRA's elements or parts of the PRA within each of the elements will not necessarily all fall within the same Capability Category, but rather will be distributed among all three Capability Categories." Moreover, the ASME Standard indicates in Section 3.1, "For a specific application, PRA capabilities are evaluated to determine the appropriate SRs rather than by specifying a single Capability Category for the whole PRA." The ACR PSA objectives are not requirements. Thus, while an objective may be acceptable, if the PRA falls short. The PRA technical adequacy is not based solely on the achievement of a specific capability category for each SR.

It is stated in Section 1.3 that a Level II PRA will be performed for the shutdown state; however, in Section 1.2 (on page 1-2, second paragraph) it is indicated that a shutdown state PRA standard is still under development with no delivery date specified. It is unclear how the shutdown PRA is to be conducted if a standard is not available. This comment also applies to Section 1.5.1 on page 1-8 and Section 1.5.1 on page 1-9 Item (a) at the bottom of the page.

6.3 Section 3, "Familiarization With ACR Design"

Section 3 describes the process by which the technical analysts of the PRA team are to become familiar with the plant design. The collection of information from various sources is described, and several references are specified for the necessary background information. Design change control is also described.

6.3.1 Methodology

The methodology for the process is clear and distinct. However, several of the references that were cited were not reviewed to verify the steps taken in the process.[20, 79–88]

6.3.2 Strengths and Weaknesses

The presentation of Section 3 in the ACR PSA methodology document is consistent with standard techniques and is easy to follow. It is also detailed enough to follow the methodology that will be presented in the following sections. However, not reviewing the references limits the extent of this review.

The material presented in Section 3 is complete and very detailed.

6.4 Section 4, "Internal Events PSA"

If Sections 4, 10, 12, and 13 of the ACR PSA are reviewed as a group, they are comparable to Section 4 of the GC PSA methodology document (see Section 4.2 of this report). However, there are some differences.

Section comparisons

Section 4 of the ACR PSA is essentially the same as Section 4 of the GC PSA methodology document. The ACR PSA leaves out or does not address the following sections that appeared in the GC PSA: assumptions and limitations, Sections 4.2.3.1–4.2.3.5.2, Sections 4.2.6.4, 4.4.7.3, 4.4.8.2–4.4.8.4, 4.7.3.6, and 4.9.2.5–4.9.2.7. These sections do not detract from the overall completeness or quality of the ACR PSA. Some of the items that were left out pertained to a CANDU 6 or CANDU 9 plant and are not necessary for the ACR PSA; other items were viewed as not being germane to the ACR design. The plant damage states described in the GC PSA are also not directly applicable to the ACR design, so information regarding damage states was rewritten with slightly different headers. All these differences were deemed to be of little consequence.

Section 10 of the ACR PSA is almost identical to Sections 4.10 and 4.11 of the GC PSA with some minor exceptions. Section 4.10.4 refers to an older version of the UNCERT computer program than the ACR PSA (Version 2.0 vs Version 5.0). Two small sections of the GC PSA (4.11.2.2 and 4.11.2.3) had no comparable section in the ACR PSA; however, this information was general in nature and could be left out with little consequence.

Section 12 of the ACR PSA is essentially the same as Section 4.12 of the GC PSA, except that the GC PSA refers to an older version (2.3) of CAFTA than the ACR PSA (CAFTA 5.0). The ACR PSA is far more detailed and better explained than the GC PSA. In addition, the ACR PSA follows NRC guidelines specifically, whereas, the GC PSA provides only general description and directions. The ACR PSA also refers to a licensee quality assurance (QA) manual, while the GC PSA does not. Several sections of both documents were identical. For example, Sections 4.12.1 and 4.12.3 are, respectively, identical to Sections 12.5 and 12.7 of the ACR PSA.

Section 13 of the ACR PSA is essentially the same as Section 4.13 of the GC PSA with no pronounced differences.

General comparisons

The ACR PSA methodology document is more thorough than the GC PSA methodology document in its description of what is intended for the internal events PRA. Also, the ACR PSA gives better and more comprehensive explanations than the GC PSA, and the program description is more detailed than in the GC PSA. In addition, the ACR PSA clearly indicates, by placing in separate sections, that the uncertainty/sensitivity analysis, the reporting of results, and QA of the PRA are applicable to the entire PRA. The GC PSA methodology document had this type of information in Section 4, and it could have conceivably been construed as only applying to the internal events PRA and not the whole PRA. Further, the ACR PSA explicitly states what documents, procedures, or other regulations will govern the process.

The methodology is similar to that found in NUREG/CR-2300. Internal events are introduced in Section 4.1. Events that disrupt normal conditions and possibly lead to the need for reactor subcriticality or the use of decay heat removal are called accident sequence IEs. These are defined in Section 4.2. Event tree development, system reliability analysis, and dependent failure analysis are treated in subsequent sections. HRA and database development are then addressed in later sections. The methodology for quantifying accident sequences is introduced in Section 4.8, and plant damage states are examined in Section 4.9.

6.4.1 Methodology

Most of the methodology for performing an internal events analysis is addressed in Section 4.2.1 of this report.

The two types of IEs are internal and external events. Internal events occur within the plant boundaries, and external events occur outside the plant. External events may cause internal events. The IEs are listed in the CNSC requirements for the safety analysis of CANDU NPPs;[20] selected applicable IEs are chosen from these lists. After the IEs are identified, the safety functions necessary to prevent core damage are developed.

Sections 4.2.5.1, 4.2.5.2, 4.2.5.4, and 4.2.5.5 cover rare events and error factors. The IEs with 10 or more occurrences are classified as commonly occurring events. Rare events are IEs that occur one to ten times over the operating history or analyzed time frame.

Section 4.7.2 states that data for component reliability is obtained from operating CANDU plants, in particular OPG’s generating stations, and References 18–19. However, because References 18–19 provide 20-year old data, the adequacy of the data could be questioned.

The modularization process given in Section 4.8.2.6 is said to reduce the time spent reviewing the cut sets, but this process is not presented. For example, "By implementing the modularization technique, the analyst can greatly reduce the number of cut sets that require review." However, that is the extent of the information regarding the technique. So, the concept is explained, but the technique is not presented. Therefore, an assessment of how to employ the process (or even more importantly, how to analyze the process) is not possible.

6.4.2 Strengths and Weaknesses

The strengths and weaknesses identified in Section 4.2.2 of this report are applicable to Section 6.4.2.

Section 4 of the ACR PSA methodology document is very detailed for the material that is presented. However, many times a representative example or calculation would have enhanced the reader’s understanding of the methodology.

The methodology is essentially consistent with that used in NUREG/CR-2300. A more comprehensive review could better determine the extent of conformance and/or any subtle inconsistencies with NRC, NRC-sponsored, and industry results. The proposed comprehensive review would require a review of all the references listed in Section 14.

The modularization process as it is applied to accident sequence quantification needs examples and a more thorough explanation of how it works. The lack of information provided in the ACR PSA on the modularization process is considered to be a significant weakness for the review of a PRA.

6.5 Section 5, "Dependent Failure Analysis"

The dependent failure analysis proposes to explicitly model:

1. functional dependencies,
2. physical interactions, and
3. human interactions.

The common cause failures (CCFs) will be implicitly modeled "...in the sense that a single fault tree basic event is used to capture all of the possible causes." The Unified Partial Method (UPM) will be used to quantify the CCFs. The CCFs can be quantified in one of two ways. First, the CCFs can be evaluated at the system level by estimating a system cut-off probability, or another method is to estimate a beta-factor for sets of similar components. The analyst is then tasked to examine the system vulnerabilities or the sets of similar components and determine a quantitative estimate for the probability of CCF.

6.5.1 Methodology

A detailed review of the methodology for performing a dependent failure analysis is given in Section 4.3.1 of this report.

The UPM method described in Sections 5.1–5.5.3 is described in detail in the "UPM Workbook,"[38] a company proprietary document. There is no CANDU-specific data for CCF. The analyst will assign beta-factors based on generic CCF data obtained from other sources such as PWRs and BWRs. AECL thinks the UPM is "...preferable to using published data for parameters of other CCF models, such as the Multiple Greek Letter (MGL) technique." The UPM is a refinement of the partial beta-factor method;

however, instead of decomposing the judgements into 19 groups, they are decomposed into 8 causal groups, with 5 system definitions to choose from. AECL will follow NUREG/CR-4780[28] for selecting the appropriate CCF component groups. However, in applying a refined partial beta-factor method, some second order cut sets may be lost. The MGL and other methods do not have this problem, but AECL thinks that "...this can lead to a proliferation of cut sets, without significantly altering the calculated system reliability."

The generic beta factors given in Section 5.5.4 (Component Types and Boundaries) are obtained from References 30–33, 64, 67, and 89. This data may still be outdated because it nominally covers information from 1972 through 1981.

AECL indicates in Section 5.5.5.2 that "Since the UPM is designed for CCF analysis at both the system level and the component level, certain explanations in the manual are ambiguous." As such, a document containing ambiguous reference information leaves little room for further discourse or analysis. Given the nature of the quoted comment and the ensuing expanded problems, it can only be concluded that an adequate review cannot be performed, which is considered to be a weakness.

Section 5.5.5.4 indicates that staggered testing is not addressed in the UPM method. Staggered testing should be accounted for; without it, the method has an inherent weakness in this regard.

6.5.2 Strengths and Weaknesses

The strengths and weaknesses identified in Section 4.3.2 of this report are applicable to Section 6.5.2.

Section 5 of the ACR PSA methodology document is very detailed for the material that is presented. However, there are too many generalizations to perform an adequate review. Also, there is a lack of examples using the UPM in estimating CCF.

Not accounting for staggered testing is a weakness.

6.6 Section 6, "Human Reliability Analysis"

The HRA for the ACR PSA generally follows NUREG/CR-1278, which is the standard for HRA. Five basic types of human actions in NPPs are classified into three categories:

1. preaccident,
2. initiators, and
3. postaccident.

The last category is further broken down into three types:

1. procedural safety actions,
2. aggravating actions, and
3. recovery actions.

Procedural safety actions are usually explicitly modeled and generally include diagnosis and execution of tasks. Aggravating actions are not always modeled and are considered errors of commission. Recovery actions are modeled. In accordance with the Accident Sequence Evaluation Program (ASEP) for HRA (NUREG/CR-4772), three different behaviors are modeled for human actions:

1. skill-based,
2. rule-based, and
3. knowledge-based.

NUREG/CR-4772 is a simplified version of NUREG/CR-1278.

6.6.1 Methodology

A detailed review of the methodology for performing a human reliability analysis is given in Section 4.4.1 of this report.

Dependence effects development follows NUREG/CR-1278, but uses four levels of dependence. This contrasts with the five levels found in NUREG/CR-1278 and the two levels found in the ASEP.

Postaccident HRA divides human actions into diagnosis and postdiagnosis tasks, and it develops coping times to determine the diagnosis and allowable execution time tasks.

Sections describing HRA for external events such as fire or earthquakes were included. These sections followed accepted practices as demonstrated in various NPP IPEEEs. The main control room was assumed to be habitable after an earthquake.

The methodology follows accepted practices outlined in NUREG/CR-1278,[40] NUREG/CR-4772,[41] NUREG/CR-4550[43] (the contractor report that formed the basis for NUREG-1150[46]), and NUREG/CR-3688.[44]

6.6.2 Strengths and Weaknesses

The strengths and weaknesses identified in Section 4.4.2 of this report are applicable to Section 6.6.2.

The HRA process is consistent with standard HRA techniques and is easy to follow. No weaknesses were identified.

Section 6 of the ACR PSA methodology document is very detailed for the material that is presented. There are many examples, and the review found no inconsistencies or errors.

The HRA methodology to be used for the ACR PSA HRA follows accepted practices given in NUREG/CR-2300[3] and NUREG/CR-4772.[41] No errors or omissions were noticed.

6.7 Section 7, "Seismic Events PSA"

The ACR PSA intends to use a seismic margin PRA as opposed to the more traditional seismic PRA. The latter uses well-developed and accepted fragility analysis methods, whereas the former uses a new method coupled with generic fragilities to calculate probabilities. The ACR PSA "...expects to satisfy all current criteria of the U.S. NRC Standard Review Plan." The ACR PSA for seismic analysis intends to follow the recommendations of U.S. NRC Policy Issue, SECY-93-087.[90] This method is similar to the traditional method except that the development of seismic hazards and integration of the hazard curve with the rest of the seismic analysis will not be done. This eliminates the need to deal with the uncertainty of the hazard curves. This appears to be slightly different from the method used for the GC PSA.

There are three methods for calculating the high-confidence of low-probability of failure (HCLPF) for structures, systems, and components (SSCs)─the traditional fragility analysis methodology; the conservative deterministic failure margin (CDFM); and, finally, using generic fragilities. Because the ACR is still in the design stage, there is not enough detail to perform the traditional fragility analysis method; rather, data from EPRI and other sources will be used along with NUREG/CR-3558 to perform the CDFM. The CDFM will be supplemented with generic fragilities where applicable or necessary. Relay chatter is not a concern because the ACR design will use solid state devices that are immune to this phenomenon.

6.7.1 Methodology

A detailed review of the methodology for performing a seismic events PRA is given in Section 4.5.1 of this report.

The plant HCLPF capacity for each seismic-induced accident sequence will be determined following the methods of NUREG/CR-4482.[91] The CDFM estimates the seismic capacities based on the review level earthquake and certain exceedence probabilities. These are to be coupled with the generic fragilities obtained from various sources to calculate and estimate the HCLPF for the SSCs.

6.7.2 Strengths and Weaknesses

The strengths and weaknesses identified in Section 4.5.2 of this report are applicable to Section 6.7.2.

The level of detail is adequate for the material presented, and the methodology to be used for the ACR PSA seismic margin assessment follows typical assessments. Several references were not reviewed during the assessment of the ACR PSA methodology[20, 50, 89, 92-96] (ACR PSA References 1, 33–36, 39, 40, and 69). Not reviewing these references means that this section’s methods and findings cannot be properly verified; this represents a significant weakness in this report’s review of the ACR PSA.

The external events analyses and subsequent PSA-based seismic margin assessment process were consistent with standard techniques and fairly easy to follow. However, the weaknesses identified earlier still apply.

6.8 Section 8, "Fire PSA"

This section describes the methodology in general terms and identifies the basic assumptions that are incorporated in a fire PRA. It states that the assumptions will be confirmed during the detailed design for the ACR.

6.8.1 Methodology

A detailed review of the methodology for performing a fire PRA is given in Section 4.6.1 of this report.

Similar to the GC PSA, the ACR PSA fire methodology follows the outline provided in IAEA Safety Series No. 50-P-4[52] (referenced by Standard Review Plan at bottom of page SRP 19-A24[53]). The IEs frequencies (fire ignition frequencies) are developed in "Development of Probabilistic Safety Assessment Methodology for Fire Events in CANDU Plants" by G. How Pak Hing and A. Stretch [presented at the International Workshop on Fire Risk Assessment Organization for Economic Cooperation and Development’s (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 1, 1999].[97] Although based on fire experience in CANDU and U.S. LWR power plants, this information source for estimating fire ignition frequencies was not reviewed and, thus, it was not possible to tell how current or inclusive the fire experience data is reported.

Qualitative screening is used to eliminate from further analysis areas that are believed to have a low impact on plant safety.

Similar to the GC PSA, the ACR PSA uses the COMPBRN IIIe computer code to calculate fire propagation and to determine the time interval between fire initiation and damage to critical equipment.

6.8.2 Strengths and Weaknesses

The strengths and weaknesses identified in Section 4.6.2 of this report are applicable to Section 6.8.2.

The level of detail was adequate.

This section has minor differences from the GC PSA methodology report's Section 8, "Fire Events PSA." The only noticed differences were the reference used for historical fire ignition frequencies and the method used to quantify fire ignition frequencies is not explicitly identified as "Bayesian." However, the term "Bayesian" may be used in reference "IAEA Safety Series No. 50-P-4."[52]

When spurious actuation of equipment is a concern, the probability of a hot short due to the fires is assumed to be 0.1. No discussion of this assumption was provided. It is not known if 0.1 is conservative and what the potential pitfalls of assuming 0.1 are. This lack of information is deemed a weakness in the report.

It is assumed that fire events in various areas in the plant will not influence operator performance in the control room. For the case of fire in the control room, a factor of 5 is applied to human factor failure probabilities to account for the increased stress. No discussion of this assumption was provided. It is unknown if assuming a factor of 5 is conservative and what the potential pitfalls of assuming a factor of 5 are. This lack of information is deemed a weakness in the report.

6.9 Section 9, "Flood PSA"

This section describes the methodology in general terms and identifies the basic assumptions that are incorporated in a flood PRA. Only the method for assessing the consequences of internal floods is described.

6.9.1 Methodology

A detailed review of the methodology for performing a flood PRA is given in Section 4.7.1 of this report.

The basic components of the internal flood PRA methodology are as follows:

- determine potential flood areas,
- identify flood sources and location of safety-related equipment,
- qualitatively screen analysis to eliminate flood areas from further analysis,

- conservatively quantify analysis to eliminate flood areas from further analysis (only those flood areas not rejected by the "qualitative screening" analysis are considered),
- refine of results for some scenarios to eliminate conservatisms,
- detail analysis of the remaining scenarios. Any local operator recovery actions are credited during this analysis, and
- perform a sensitivity analyses for the detailed analyses.

The flood protection barrier failure probabilities for watertight doors, nonwatertight doors, drain line check valves, and sealed cable penetrations are based on judgment. In addition, flood frequencies are reduced by the application of several empirical factors (location, direction, propagation, severity, and operator). If these factors are empirical, the methodology fails to reference a source for the data for deriving these empirical factors. The methods used to develop these empirical factors are not discussed.

Pipe break frequencies are based on WASH-1400 (circa 1975). Expansion joint rupture frequencies are based on the frequencies presented in the Oconee PRA by EPRI (NSAC-60, 1984[98]) rather than the Calvert Cliffs PRA for the GC PSA. The frequency for ruptures of tanks was taken as the minimum of the feedwater storage tank and refueling water storage tank rupture frequencies for PWRs obtained from (IAEA-TECDOC-478, 1988[67]). No justification or discussion was provided to support selection of the minimum value.

6.9.2 Strengths and Weaknesses

The strengths and weaknesses identified in Section 4.7.2 of this report are applicable to Section 6.9.2.

The level of detail is incomplete.

This section differs slightly from and is a little different from the GC PSA methodology report's Section 9, "Flood Events PSA."

Data should be available to estimate failure probabilities for doors, check valves, and penetrations, thus eliminating the use of "judgment" for estimating these values. The references used to estimate pipe breaks, tank ruptures, and expansion joint ruptures are at least 20 years old—more recent data should be available to estimate these frequencies. In particular, the use of WASH-1400 (which includes many "Delphi" generated values) pipe break frequencies should be reconsidered.

With the exception of the potential data issues identified above, the methodology described in this section follows the guidelines in NUREG/CR-2300, Section 11.4.

More recent data sources for estimating rupture frequencies should be used. Data sources for estimating door, drain check valve, and penetration failure estimates should be researched and identified. In addition, data sources for estimating the empirical factors of location, direction, propagation, severity, and operator action should be identified, and the method(s) used to generate these empirical factors should also be documented. These items represent a significant weakness in the PRA methodology.

6.10 Section 10, "Uncertainty and Sensitivity Analysis"

Section 10 describes the process for determining the uncertainty, or "how well the prediction will match the actual situation," for the PRA. Various sources of uncertainty are described along with the methodology for calculating them. The techniques used to determine the sensitivity of the PRA results are also described.

6.10.1 Methodology

The methodology for the process is clear and distinct and follows standard methods. However, the program used to perform the uncertainty analysis[23] was not reviewed or tested.

6.10.2 Strengths and Weaknesses

The presentation of Section 10 is consistent with standard techniques and is easy to follow. The section also presents a clear example of uncertainty fundamentals. Including the review of Reference 23 in the review of the ACR PSA would enhance the review process.

6.11 Section 11, "Level II PSA"

The object of the Level II PRA is to confirm that the severe core damage frequency (SCDF) is $\leq 1 \times 10^{-5}$/year, and LERF $\leq 1 \times 10^{-6}$.

6.11.1 Methodology

The PDSs define the broad accident sequence categories that define the starting conditions for the long-term accident progression. PDS0 (failure to shutdown) is screened out of the ACR-700 PRA based on low frequency. No similar screening is identified in the GC PSA.

There are two other differences between the ACR and GC PSAs: (1) the PDSs for the ACR are binned into core damage states, and (2) different terminology is used—the term "large release" for the ACR is the same as a "large early release" for the GC. It is not clear that they are or are not the same quantity.

6.11.2 Strengths and Weaknesses

The Level II PRA identifies PDSs for internal, fire, and flood events. These are binned into core damage states after accounting for long-term interventions. Deterministic analyses enumerate the radiation source terms outside containment via open paths. A profile of source terms as a function of frequency is derived, and these source terms are screened out against the large release criterion. The lack of detail is considered a weaknesses of the methodology.

6.12 Section 12, "Quality Assurance"

Section 12 describes the process for ensuring the quality of the PRA. The QA manual[99] is followed, and the documentation required such as Reference 100 is described. The design verification and subsequent review processes are also described. All pertinent AECL documents are listed.

6.12.1 Methodology

The methodology for the process is very thorough, clear, and distinct and follows standard methods. However, most of the references cited were not reviewed during the review of the ACR PSA.

6.12.2 Strengths and Weaknesses

The presentation of Section 12 is consistent with standard techniques and is easy to follow. Section 12 is very detailed, complete, and the methodology is easy to follow. The lack of review of the various references probably is of little consequence.

6.13 Section 13, "Reporting of Results"

Section 13 describes how the results from the PRA will be provided and what form they will take. The U.S. NRC PRA Procedures Guide[47] will be followed and adjusted where necessary to account for CANDU practices.

6.13.1 Methodology

The structure for the reporting of results is very thorough, clear, and distinct, and it follows standard methods.

6.13.2 Strengths and Weaknesses

The presentation of Section 13 is consistent with standard techniques and is easy to follow. Section 13 is very detailed, and the structuring of the results reporting is easy to follow.

The previous review documents, GC PSA Methodology and GC PSA Reference Analysis, each had their references listed for and within each individual section, whereas the ACR PSA Methodology document lists all the references in Section 14. In some cases, this made it easy to recognize a serious problem with the overall scope of reference material cited—that is, many references were proprietary. Although proprietary references would be made available to the NRC, they are not available to the general public. Relying on proprietary documents is considered to be a weakness.

6.14 Section 14, "References"

All of the references for the ACR PSA were provided in one section. Conversely, the two GC PSA documents provided references at the end of each individual section.

6.15 Appendix A, "Internal Events PSA Supporting Information"

Data is collected and analyzed. A failure rate is derived from the raw data called "mean time between failure." The data is described as exponentially distributed consistent with data gathered from

1. highly reliable components,
2. small population,
3. low number of failures, and
4. short time spans.

Confidence limits are calculated using the Chi-square distribution. Tables are presented detailing plant success states and mission times. Component types and boundary descriptions for the grouping, along with component failure modes and mechanisms, are presented.

6.15.1 Methodology

The use of the Chi-square distribution calculations has been covered in Section 4.2.1.

6.15.2 Strengths and Weaknesses

The section presents the data very well and is easy to follow.

6.16 Summary

The reporting and methodology strengths and weaknesses noted from the review of the ACR PSA methodology document are summarized in Tables 12–15.

Table 12. Summary of Reporting Strengths Identified in the Review of the ACR Methodology

Topic	Observations
Description	The ACR PSA document is more thorough in its description of what is intended for the PSA compared to the GC PSA. The extensive lexicon of definitions of terms is far more comprehensive and thorough, and the program description is more detailed than the GC PSA document. In addition, the ACR PSA clearly states that the current PSA effort will be in accordance with the licensing basis document (LBD) for ACR. This was not explicitly stated in the GC PSA documents.
Introduction	Section 1 describes the Level I and Level II PRA for the ACR design regarding internal events, seismic concerns, internal fire issues, and internal flooding issues. The introductory section also indicates that a shutdown PRA would be performed. The scope of the PRA is clearly defined.
Internal Events PRA	The ACR PSA is far more detailed and better explained than the GC PSA.
Internal Events PRA	The ACR PSA methodology document is more thorough than the GC PSA methodology document in its description of what is intended for the internal events PRA. Also, the ACR PSA gives better and more comprehensive explanations than the GC PSA, and the program description is more detailed than in the GC PSA. In addition, the ACR PSA clearly indicates, by placing in separate sections, that the uncertainty/sensitivity analysis, the reporting of results, and QA of the PRA are applicable to the entire PRA. The GC PSA methodology document had this type of information in Section 4, and it could have conceivably been construed as only applying to the internal events PRA and not the whole PRA. Further, the ACR PSA explicitly states what documents, procedures, or other regulations will govern the process.

Table 13. Summary of Reporting Weaknesses Identified in the Review of the ACR Methodology

Topic	Observations
Introduction	The ACR PSA states that "The ACR™[*] design is intended to satisfy current licensing basis of the USNRC." It is unclear if this statement refers to the Standard Review Plan or some other NRC document. Also, the statement should specify what LBD is to be used as a standard or reference.
Internal Events PRA	The modularization process is said to reduce the time spent reviewing the cut sets, but this process is not presented. Thus, the modularization process as it is applied to accident sequence quantification needs examples and a more thorough explanation of how it works.
Internal Events PRA	Section 4 of the ACR PSA methodology document is very detailed for the material that is presented. However, many times a representative example or calculation would have enhanced the reader's understanding of the methodology.
Dependent Failure Analysis	The dependent failure analysis section of the ACR PSA methodology document is very detailed for the material that is presented. However, there are too many generalizations to perform an adequate review. Also, there is a lack of examples using the UPM in estimating CCF.
Fire Events Analysis	When spurious actuation of equipment is a concern, the probability of a hot short due to the fires is assumed to be 0.1. No discussion of assumptions was provided. It is not known if 0.1 is conservative and what the potential pitfalls of assuming 0.1 are.
Fire Events Analysis	It is assumed that fire events in various areas in the plant do not influence operator performance in the control room. For the case of fire in the control room, a factor of 5 is applied to human factor failure probabilities to account for the increased stress. No discussion of this assumption was provided. It is unknown if assuming a factor of 5 is conservative and what the potential pitfalls of assuming a factor of 5 are.
Flood Events Analysis	Flood frequencies are reduced by the application of several empirical factors (location, direction, propagation, severity, and operator). If these factors are empirical, the methodology fails to reference a source for the data for deriving these empirical factors. The methods used to develop these empirical factors are not discussed.
Flood Events Analysis	The frequency for ruptures of tanks was taken as the minimum of the feedwater storage tank and refueling water storage tank rupture frequencies for PWRs obtained. No justification or discussion was provided to support selection of the minimum value.
Flood Events Analysis	Data sources for estimating door, drain check valve, and penetration failure estimates should be researched and identified. In addition, data sources for estimating the empirical factors of location, direction, propagation, severity, and operator action should be identified, and the method(s) used to generate these empirical factors should also be documented.

Table 13. Summary of Reporting Weaknesses Identified in the Review of the ACR Methodology Report (Continued)

Topic	Observations
Level II PRA	There are two other differences between the ACR and GC PSAs: (1) the PDSs for the ACR are binned into core damage states, and (2) different terminology is used—the term "large release" is used in the ACR and "large early release" is used in the GC. It is not clear that they are or are not the same quality.
Level II PRA	The Level II PRA identifies PDSs for internal, fire, and flood events. These are binned into core damage states after accounting for long-term interventions. Deterministic analyses enumerate the radiation source terms outside containment via open paths. A profile of source terms as a function of frequency is derived, and these source terms are screened out against the large release criterion. There is a lack of detail when discussing the methodology.
Reporting of Results	The previous review documents, GC PSA Methodology and GC PSA Reference Analysis, each had their references listed for and within each individual section, whereas the ACR PSA Methodology document lists all the references in Section 14. In some cases, this made it easy to recognize a serious problem with the overall scope of reference material cited—that is, many references were proprietary. Although proprietary references would be made available to the NRC, they are not available to the general public.

Table 14. Summary of Methodology Strengths Identified in the Review of ACR Methodology

Topic	Observations
Internal Events PRA	The ACR PSA follows NRC guidelines specifically, whereas, the GC PSA provides only general description and directions. The ACR PSA also refers to a licensee quality assurance (QA) manual while the GC PSA does not.
Human Reliability Analysis	Sections describing HRA for external events such as fire or earthquakes were included. These sections followed accepted practices as demonstrated in various NPP IPEEEs.

Table 15. Summary of Methodology Weaknesses Identified in the Review of the ACR Methodology

Topic	Observations
Introduction	The ACR PSA is judged (by AECL) to be an ASME RA-S-2002 Category I PRA. At the same time, the ACR PSA states that 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 guidelines in developing the PRA methodology for the ACR program. Thus, it is unclear what guidance the various tasks follow.
Introduction	When reading the statement "Considering these, the appropriate capability category for satisfying the purpose of the ACR-700 PRA is judged to be Category I," it is not clear how the Category I classification was arrived at without more explanation. Many requirements for a Category II or III PRA are identical to a Category I PRA (i.e., only specific areas need additional work to meet the higher category requirements). The PRA technical adequacy is not based solely on the achievement of a specific capability category for each SR.
Introduction	The ACR PSA states that a Level II PRA will be performed for the shutdown state; however, it is indicated that a shutdown state PRA standard is still under development. It is unclear how the shutdown PRA is to be conducted if no standard is available.
Internal Events PRA	The ACR PSA states that data for component reliability is obtained from operating CANDU plants, in particular OPG's generating stations; and IEEE Standard Number 500; and the NPRDS database. However, because the IEEE standard and the NPRDS database provide 20-year old data, the adequacy of the data is questioned.
Dependent Failure Analysis	The data used to obtain generic beta factors may be outdated because they rely on 20–30 year old sources for information.
Dependent Failure Analysis	The ACR PSA indicates that staggered testing is not addressed in the UPM method. Staggered testing should be accounted for.
Seismic Events Analysis	The ACR PSA intends to use a seismic margin PRA as opposed to the more traditional seismic PRA. The latter uses well-developed and accepted fragility analysis methods whereas the former uses a new method coupled with generic fragilities to calculate probabilities. This method is similar to the traditional method except that the development of seismic hazards and integration of the hazard curve with the rest of the seismic analysis will not be done.
Flood Events Analysis	The flood protection barrier failure probabilities for watertight doors, nonwatertight doors, drain line check valves, and sealed cable penetrations are based on judgment.

Table 15. Summary of Methodology Weaknesses Identified in the Review of the ACR Methodology Report (Continued)

Topic	Observations
Flood Events Analysis	Pipe break frequencies are based on WASH-1400 (circa 1975). Expansion joint rupture frequencies are based on the frequencies presented in the Oconee PRA by EPRI (NSAC-60, 1984) rather than the Calvert Cliffs PRA for the GC PSA.
Flood Events Analysis	Data should be available to estimate failure probabilities for doors, check valves, and penetrations, thus, eliminating the use of "judgment" for estimating these values.
Flood Events Analysis	The references used to estimate pipe breaks, tank ruptures, and expansion joint ruptures are at least 20 years old—more recent data should be available to estimate these frequencies. In particular, the use of WASH-1400 (which includes many "Delphi" generated values) pipe break frequencies should be reconsidered.
Flood Events Analysis	More recent data sources for estimating rupture frequencies should be used.

Page Intentionally Blank

7.0 DESIGN ASSIST ROLE OF ACR PROBABILISTIC SAFETY ASSESSMENT

The PSA assessment document, *Design Assist Role of ACR Probabilistic Safety Assessment (PSA)*[9] presents an overview of the role that probabilistic safety―or risk―assessments (PSAs or PRAs) have played in the design of the Canada Deuterium Uranium (CANDU) reactors. The PSA assessment document also explains how PSAs are to be used in the design of the latest CANDU, the Advanced CANDU Reactor (ACR-700). Four broad areas of information and study are discussed:

1. the history of the application of risk assessment used throughout the Canadian nuclear industry,
2. the use of PSAs in the design of the ACR-700,
3. a review of the preliminary results from the ACR-700 PSA, and
4. a discussion of how these preliminary results from the ACR-700 PSA are being used to finalize the design.

Section 1 of the PSA assessment document indicates that the PSA assessment document will review the history of PSA in the Canadian nuclear industry, and then its use in the latest CANDU and ACR designs. Section 2 details the historical evolution of Canadian PSAs from the Siting Guide first used for the Pickering A reactor in the early 1970s. This guide establishes the rules for licensing power reactors by categorizing plant systems as being either "process" systems or "protective" systems. The purpose of the current program is to establish a standard "state-of-the-art PSA . . . based on commonly-accepted scope and methodologies."

In the early designs of the CANDU reactors, the risk assessment efforts were focused on applying target frequencies for various process systems to the reactor design. Examples include the 1975 Pickering A and 1979 Bruce A PSA studies. Later reactor designs integrated reliability assessments using fault tree techniques into the designs resulting in "PSA techniques becoming embedded into the system design process." This was followed by the development of a three-time frame safety design matrix that evolved into a tabular Safety Design Matrix (SDM). Throughout the 1980s, the SDM evolved into a more comprehensive PSA that was extended to included accident sequences that resulted in releases of radioactivity. As a result, Fuel Damage Categories (FDCs) and Ex-Plant Release Categories (EPRCs) were defined, and the frequencies for severe core damage (SCD) and large early releases were determined.

AECL Technologies, Inc. and a Dutch utility support organization, N.V. Tot Keuring van Elekrotechnische Materialen (KEMA), extended the PSA analyses to include sequences beyond previous frequency cutoff limits. Pickering A was the first operating plant to use PSA to provide a means to assist the safety-related decision-making process throughout the lifetime of the station. Core damage progression was defined in terms of six core damage states (CDSs), and the EPRCs were divided into seven release categories. As a result of this PSA, several design changes were developed that reduced the overall plant risk for severe core damage by an order-of-magnitude.

The Korea Atomic Energy Research Institute and Atomic Energy of Canada, Ltd. (AECL) applied this acquired knowledge and insights from Pickering A risk assessment to the PSA for the three CANDU 6 units at Wolsong in Korea. Those insights led to the number of CDSs being extended to 11 plant damage states (PDSs), and common-cause failures (CCFs) and human reliability analysis being included in the PSA. From the PSA analyses, it was determined that pipe breaks were an insignificant risk; however, transients and postaccident operator actions were dominant contributors to SCD. Therefore, based on these PSA reviews, the emergency operating procedures were enhanced, and several automatic actuations were included in the emergency cooling recovery systems along with the use of redundant valving.

The design of the next product line, the CANDU 9, included many risk-based improvements such as two auxiliary feedwater (AFW) pumps, four emergency core cooling recovery pumps, four emergency diesel generators, relocated service water pumps, and a reserve water tank supplying gravity-feed makeup water. The current PSA effort establishes a generic PSA for all reactors in the product line (i.e., CANDU 6 and CANDU 9). The generic PSAs model CCFs using a method called the Unified Partial Method (UPM).[101] As noted in the PSA assessment document, "The UPM method permits a qualitative evaluation of the vulnerabilities of redundant components to CCF, while providing a reasonable quantitative estimate of the effects of these failures on the eventual in-service reliability of the systems." Also, the Accident Sequence Evaluation Program (ASEP) is used to evaluate human reliability analysis (HRA) procedures.[41]

Section 3 of the PSA assessment document provides a brief description of the ACR-700 design features. Section 4 provides "salient aspects of the preliminary Event Tree Analysis" extracted from *Preliminary Design Assist PSA Level 1—Selected Full Power Event Trees*[10] (see Section 8 of this report).

7.1 Methodology

Section 3 of the PSA assessment document describes several safety features that were incorporated into the design of the ACR-700. These features include:

- solid reactivity control devices for spatial power control instead of the injection of water into zone compartments,
- a negative void reactivity coefficient,
- one-way rupture discs in the emergency coolant injection (ECI) to provide makeup to the heat transport system (HTS) following a loss of coolant accident (LOCA),
- higher strength calandria tubes to withstand the loading from a pressure tube failure for a considerable time,
- large quantities of water located in the reserve water tank (RWT),
- passive autocatalytic recombiners for post-accident hydrogen control,
- vault and dome local air coolers for steam pressure control, and
- automated safety system responses so that no operator action is needed for a minimum of 8 h following most design basis accidents.

The ACR-700 also departs from the following previously standard features of the CANDU design:

- standby electrical power and water systems themselves are qualified for common mode events and, as such a separate set of "emergency" systems is not necessary, and
- the same set of pumps and heat exchangers used for the shutdown cooling function, or residual heat removal, as well as for ECC recovery is now located outside containment.

According to AECL, "The apparent reduction in redundancy [for the emergency electric power and water systems] for other initiating events is minimized by configuring key mitigating systems in the form of multiple redundant ‘divisions’, analogous to the ‘train’ concept of LWRs." Although AECL states that this "actually provides more reliable mitigation of common mode events because of reduced reliance of the surviving system on operator action," this arrangement should be noted and evaluated in detail.

Section 4 of the PSA assessment document details how the ACR-700 PSA will be performed and examines preliminary results that have already been used to identify vulnerabilities that will be reviewed by the designers. AECL states that designers will make design modifications to eliminate the vulnerabilities if the changes are practicable.

The ACR-700 PSA will be complete Level 1 and Level 2 risk assessments following the methods of NUREG/CR-2300[3] and NUREG/CR-4550.[43] The Level 1 PSA will include an assessment of risk from IEs, internal floods, internal fire, and operators in a shutdown state. A seismic margin assessment will also be conducted. The Level 2 assessment will include a containment performance analysis and an analysis of physical processes associated with key severe core damage accidents. AECL has already developed a list of IEs.[102] A mandatory requirement by AECL is that the safety design adequacy will be within the safety goals (acceptance criteria) of the ACR-700 licensing basis.[79]

According to AECL, external events such as high winds and tornadoes are not expected to be safety significant and therefore will not be studied. However, site-specific events will be examined in accordance with the screening criteria established in NUREG-1407.[45]

As stated in the PSA assessment document, "[T]he PSA is being conducted iteratively as the design progresses." Several assessments have already been conducted for the design. These are called "design-assist" assessments, and three such assessments are the subject of the rest of the PSA assessment document. The three design-assist assessments discussed in the last portion of the PSA assessment document concern event tree analysis for selected IEs,[10] fault tree analysis including CCF modeling using the UPM for the emergency feedwater system (EFW),[101] and a design configuration assessment. Although the PSA assessment document discusses three design-assist assessments, the document focuses on the event tree analysis for selecting initiating events.

The event tree design-assist assessments provide input to the design teams concerning accident mitigation systems and their respective reliabilities. This event tree analysis is used as a screening tool that credits such things as the reserve water system (RWS) as an example of a passive mitigation feature. Credit is taken only "for those sequences which would otherwise have a higher than target frequency." The PSA assessment document copies and presents information on the 11 IEs selected for further analysis from *Preliminary Design Assist PSA Level 1—Selected Full Power Event Trees*.[10] The 11 IEs selected for further analysis in *Preliminary Design Assist PSA Level 1—Selected Full Power Event Trees*[10] using event trees were divided into 6 groups:

1. small breaks,
2. loss of Division 2 service water,
3. loss of power to one of two units at a two-unit site,
4. loss of shield water,
5. secondary side breaks, and
6. power excursions.

Ten event tree end states were grouped into three broad categories of PDSs. PDS 0, PDS 1, and PDS 2 are classified as SCD states; PDS 3, PDS 4, and PDS 6 are classified as limited core damage (LCDs) states; while PDS 5, PDS 7, PDS 8, and PDS 9 have no classification. Each accident sequence is assigned to a PDS, and the sequence ends in one of three conditions:

1. no significant damage or S,
2. some damage or a PDS in accordance with the core damage states given above, and
3. no further development of the sequence or NDF because its (the sequence) frequency is below a predetermined cutoff value of 1.0×10^{-9}/year.

As the process unfolds, the ACR-700 PSA AECL expects to include operator errors of diagnosis and execution. All but two of the IEs for the early design work employed a simplified human error analysis. The event trees for a pressure tube break with a subsequent calandria tube rupture and the asymmetric feedwater line break downstream of a steam generator (SG) check valve each have a more extensive HRA associated with their respective trees because the operator actions in these scenarios have a greater impact on the severe core damage frequency (SCDF) than in the other event trees.

The PSA assessment document also examines and discusses the feeder break event tree and analyzed the results. With respect to the feeder breaks, the document indicates, "that for almost all accident sequences resulting in core damage the frequency is small enough that the summed frequency would be well within the SCDF targets." The document concludes its section on the preliminary event tree analysis by listing the following key assumptions made as part of the PSA:

- A connection from the reserve feedwater tank (in the turbine building) to the auxiliary feedwater pump suction header is important because this allows the auxiliary feedwater pumps to maintain supply to the SGs in the event of a loss of the auxiliary condensate pump.
- A reliable, automatic closure of the auxiliary feedwater level control valves exists when a discrepancy between the two SG levels is sensed.
- The assigned 1.5×10^{-2} probability of calandria tube failure following a pressure tube rupture requires demonstration that the calandria tube will survive all relevant loading conditions, and that the calandria tube has a high creep rupture resistance. (To afford high reliability credit for the operator action, the calandria tube needs to survive for about 2 h or longer. This appears to be the exception to no operator action for 8 h for most design basis accidents.)
- Eight hours is available before the HTS pressure boundary, or any other boundary that holds water, could be threatened following a loss of shield water inventory.
- Although the HTS pumps are not formally environmentally qualified, it is assumed (as a best estimate) that at least one pump can run for up to 60 min after a secondary side line break in the reactor building (asymmetric feedline break event).

AECL states that "As part of the ACR-700 detailed design development process, these assumptions are required to be supported by analysis and/or equipment suppliers' test records as appropriate."

The fault tree analysis of the EFW supply for two cases were analyzed and are briefly discussed:

1. both SGs are required for a heat sink following a loss of Class IV (offsite) power; thermosyphoning is credited for decay heat removal, and
2. either SG is sufficient for a heat sink following a loss of Class IV (offsite) power.

The first case, where both SGs are required, is the most limiting by at least an order-of-magnitude. The results indicate that the EFW system is sensitive to the CCF of motorized valves in the system.

The following design changes to the ACR-700 have resulted from the preliminary work of the PSA:[9]

1. All systems were analyzed qualitatively to ensure that they meet the single failure criterion.
2. The optimal number of Class III diesel generators was determined by assessing the impact of various proposed configurations on the accident sequences involving loss of Class III power (DGs).

3. Similar to item 2 above, the required number of main and auxiliary feedwater pumps and the configuration of the backup source of water for the auxiliary feedwater supply were established using a similar methodology as in item 2.
4. The recirculated cooling water (RCW) system and the raw service water (RSW) system were reviewed by examining selected accident sequences involving these systems and by simplified fault tree modeling. A configuration was selected that provided the highest reliability, taking into account the major failure modes to which these systems and their components were subjected, such as expansion joints failures, screen-wash system failure, and pump failures,
5. PSA staff also provided input to the system designers to remove potential sources of unreliability in their systems. For example, in an early configuration of the ECI system, it was identified to the designers that the one-way rupture disks could inadvertently burst while reactor power maneuvers were underway. Provision for additional operating procedures was identified to remove this possibility.

The PSA assessment document stresses in its concluding section that "the conduct of the PSA for the ACR-700 is an integral part of the design process. As such AECL has made mandatory the review of PSA event trees and fault trees by the relevant design staff and the formal dispositioning of comments and issues raised." Moreover, the PSA "will also be subjected to a formal independent peer review to confirm it possesses attributes generally considered essential for a quality PRA, e.g., those outline in" Chapter 19.1 of NUREG-0800.[53]

7.2 Strengths and Weaknesses

The methodology used for the PSA for the ACR-700 is "generally" in accordance with NUREG/CR-2300[3] and NUREG/CR-4550[43] (NUREG/CR-4550 is the foundation for NUREG-1150[46]). Thus, AECL’s methodology "generally" follows typical practices for the industry. Because the PSA assessment document is an overview of the PSA process applied by AECL, detailed reasoning behind the selection or analysis of IEs is not expected.

The level of detail in the PSA assessment document is comprehensive. In addition, Sections 3 and 4 of the PSA assessment document provide a complete description of the enhanced design features incorporated into the ACR-700 design as well as the structure, philosophy, and implementation of the integrated-design PSA. This document is an excellent introductory synopsis of the Canadian nuclear industry’s risk assessment history and provides insights into other AECL documents (specifically, Refs. 7–8, 10 and 102).

According to AECL, external events such as high winds and tornadoes are not expected to be safety significant and therefore will not be studied. However, site-specific events will be examined in accordance with the screening criteria established in NUREG-1407.[45] The exclusion of the effects of high winds and tornados may be unreasonable and is considered to be a weakness. For example, the CDF at McGuire[103] resulting from tornados impacting the plant is ~1.9 × 10^{-5}/year. Considering that the CDF at McGuire[103] from transients is 2.2 × 10^{-5}/year and from LOCAs is 1.5 × 10^{-5}/year, tornados are a significant contributor to plant risk.

The results presented in the appendixes of the PSA assessment document are duplications of those provided in *Preliminary Design Assist PSA Level 1—Selected Full Power Event Trees*[10] (see Section 8 of this report). The PSA assessment document in this review is an overview of the process, and, as such, it does not provide the detailed reasoning behind the selection or analysis of the IEs. For example, *Preliminary Design Assist PSA Level 1—Selected Full Power Event Trees*[10] presents a detailed comprehensive discussion of how the 11 IEs were selected for event tree analysis from the list of 87 grouped IEs given in *Systematic Review of Plant Design for Identification of Initiating Events*.[102] A spot-check of the results in this document with the selected full power event trees[10] did not indicate any inconsistencies or errors.

The design-assist assessments provide a significant and principal link to the overall ACR-700 integrated-design PSA. It is important to understand the process of how the PSA has evolved into its current state. In order to do this, it becomes essential to follow the process from its inception to the present so that when a design modification or system logic change takes place, it is clear how and why that happened. The clarification of the purpose and thought behind the development of *Preliminary Design Assist PSA Level 1—Selected Full Power Event Trees*[10] explained in Section 4 of the PSA assessment document ties together the historical evolution of the PSA and the concept of design-integration. Without this connection, it would seem that the selection of 11 initiating events was arbitrary and without foundation; subsequently, any resulting design modifications that were made would also be viewed as arbitrary and lead to the false conclusion that the design change was either unnecessary or unsubstantiated. Thus, it is a strength that the logic, process, and thought behind using PSA to make design modifications is detailed.

According to AECL, several key assumptions made in Section 4.2.8 of the PSA assessment document (and listed previously) require either verification or substantiation:

1. The probability of calandria tube failure following a pressure tube rupture of 1.5×10^{-2} not only needs justification, but, as indicated by AECL, it also "requires demonstration." Moreover, it is indicated that operator action concerning this accident is considered highly reliable, and the calandria tube will "survive for about 2 hours or longer." AECL indicates that these latter assumptions will be justified. It is expected that the demonstration noted will also support the 2-h assumption. (To afford high reliability credit for the operator action, the calandria tube needs to survive for about 2 h or longer. This appears to be the exception to no operator action for 8 h for most design basis accidents.)
2. "The operator plays a crucial role following shield cooling accidents." There is a corollary assumption that 8 h is available before any pressure boundary is breached. It is further indicated that "Analyses need to ascertain that long times are available for the ACR-700 as well." Thus, AECL indicates that the 8-h availability should be justified, and the analyses supporting long times should also be made available.
3. Because the HTS pumps are not environmentally qualified, and "the layout of the piping needs to minimize a harsh environment around the HT[S] pumps," then it appears that the HTS pumps could be in a harsh environment and should be qualified for the potentially harsh environment.
4. The PSA assessment document notes "the HTS pumps are credited in the short term in conjunction with auxiliary feedwater (AFW) which acts as the heat sink until long-term cooling (LTC) in shutdown cooling mode is valved in. During detailed PSA, this conservative assumption will be assessed and the event trees will be revised appropriately." This issue ties in with the third issue, because the ability of the HTS pumps to provide a heat sink (in conjunction with AFW) is dependent on the results of the pumps' qualification. These assumptions should be supported with analyses or demonstration to claim credit during some accident sequences.
5. During the discussion regarding the fault tree analysis of EFW (Section 4.3 of the PSA assessment document), it was indicated that "the EFW unavailability result is almost an order of magnitude better in the case where either steam generator is sufficient, attesting to the need to analytically confirm the assumption related to steam generator capability." AECL recognizes that the support

analysis should be performed and made available to confirm this statement in addition to claiming credit in the PSA.

6. The PSA assessment document indicates in Section 4.3 that an analysis has been initiated to demonstrate or support the assumption that feedwater flow to any SG is sufficient for decay heat removal via thermosyphoning. This analysis is necessary to confirm results in the PSA and its fault trees.

Although the statement by AECL that "As part of the ACR-700 detailed design development process, these assumptions are required to be supported by analysis and/or equipment suppliers' test records as appropriate" could be viewed as a weakness, it is recognized that this is a normal part of the design process.

7.3 Summary

The PSA assessment document ties together the historical evolution of the PSA and the concept of design-integration. Without this connection, it would seem that the selection of 11 IEs for detailed review was arbitrary and without foundation; subsequently, any resulting design modifications that were made would also be viewed as arbitrary and lead to the false conclusion that the design change was either unnecessary or unsubstantiated. Thus, it is a strength that the logic, process, and thought behind using PSA to make design modifications is detailed.

The reporting and methodology strengths and weaknesses noted from the review of the design-assist role of the ACR-700 PSA PSA assessment document are summarized in Tables 16–17.

Table 16. Summary of Reporting Strengths Identified in the Review of the Design-Assist Role of the ACR-700 PSA

The PSA assessment document is an excellent introductory document that provides insights into other AECL documents.
A spot-check of the results in the PSA assessment document with the selected full power event tree did not indicate any inconsistencies or errors.
The logic, process, and thought behind using PSA to make design modifications is sufficiently detailed to provide readers an understanding on how design modifications are made.

Table 17. Summary of Reporting Weaknesses Identified in the Review of the Design-Assist Role of the ACR-700 PSA

Because the HTS pumps are not environmentally qualified, and "the layout of the piping needs to minimize a harsh environment around the HT[S] pumps," it appears that the HTS pumps could be in a harsh environment and should be qualified for the potentially harsh environment.
The ability of the HTS pumps to provide a heat sink (in conjunction with AFW) is dependent on the results of the pumps' qualification.

The exclusion of the effects of high winds and tornados may be unreasonable. For example, the CDF at McGuire resulting from tornados impacting the plant is ~1.9 × 10^{-5}/year, almost 1/3 of the total CDF.

Page Intentionally Blank

8.0 PRELIMINARY DESIGN ASSIST PSA, LEVEL 1─SELECTED FULL-POWER EVENT TREES

Section 4 of AECL's assessment document *Design Assist Role of ACR Probabilistic Safety Assessment (PSA)*[9] provides "salient aspects of the preliminary Event Tree Analysis" extracted from its design-assist document *Preliminary Design Assist PSA Level 1─Selected Full Power Event Trees*[10] (the document under review in this section).

Even though the ACR-700 shares some similarity with previous CANDU reactors, several improvements in the reactor design require some preliminary assessment to determine their effectiveness. This design-assist analysis report[10] uses event trees to perform that analysis. Moreover,

> This preliminary event tree (ET) analysis report examines the responses of Advanced CANDU Reactor™ (ACR™) to selected internal initiating events (IEs) that significantly impact Severe Core Damage Frequency (SCDF) in existing CANDU® reactors. Design targets for SCDF values in the ACR are $< 10^{-7}$ per year for an individual sequence, $< 10^{-6}$ per year for summed internal events, and $< 10^{-5}$ per year for summed internal and external events to be evaluated for a mission time of 24 hours. The first two targets are guides, which are expected to yield the summed SCDF for internal and external events prescribed by Reference 1 [*Licensing Basis for ACR*[79]].

Because the design-assist analysis document is a preliminary "design-assist" analysis, several features planned for the ACR-700 design were not included in the event trees. For example, not all of the supplied process volumes from the reserve water system (RWS) were modeled, such as the RWS supply to the end shield tanks. Therefore, the implicit screening assessment objective is that "the preliminary analyses in this document should be viewed as 'screening assessments' that identify accident sequences leading to Severe Core Damage (SCD) and the features that contribute most to these sequences (e.g., hardware failures, system cross-link failure or post-accident human error)."

AECL uses the preliminary design-assist document to identify those internal event sequences for the ACR-700 that contribute the most to and/or dominate the SCDF based on CANDU 6 and CANDU 9 reactor designs. Eleven IEs were picked from the comprehensive list of 87 grouped IEs developed in *Systematic Review of Plant Design for Identification of Initiating Events*.[102] The 11 IEs that were analyzed are listed in Table 18.

Based on AECL's previous experience with other CANDU designs, the 11 IEs selected for detailed review were expected to produce the highest individual accident sequences in terms of SCDF. Also, these IEs were expected to be major contributors to the sum of the SCDF. To meet the screening assessment objective of identifying accident sequences that lead to SCD and the features that contribute most to those sequences, the design-assist document "progressively expands the event tree models to identify and characterize the dominant sequences." Of the 11 selected IEs, 8 include the typical pipe breaks─4 primary side (e.g., pressure tube rupture, feeder break, etc.) and 4 secondary side (e.g., feedwater line break, small steam line break, etc.). The remaining three IEs comprise a loss of one service water division, a loss of Class IV (offsite) power to one ACR-700 unit at a dual-unit site (i.e., loss of offsite power to 1 of 2 reactors at a site), and a loss of reactivity control.

Table 18. Initiating Events Selected for Detailed Review

No.	IE identification	Definition	IE Frequency (/year)
1	IE-PTR	Pressure tube rupture with a calandria tube remaining intact (small loss of coolant accident, LOCA)	4.0×10^{-3}
2	IE-PCTR	Rupture of a pressure tube and calandria tube (small LOCA)	6.0×10^{-5}
3	IE-FBIO	Feeder break	2.0×10^{-3}
4	IE-FSB	Feeder stagnation break (with consequential channel rupture)	2.0×10^{-4}
5	IE-SWD2	Total loss of one service water division (division 2)	5.0×10^{-2}
6	IE-LCL4	Total loss of Class IV (offsite) power supply to one ACR-700 unit	3.0×10^{-1}
7	IE-SCB	Loss of inventory in shield cooling system	4.0×10^{-4}
8	IE-MSL3	Small steam discharge causing low deaerator level	1.0×10^{-1}
9	IE-FWBS	Symmetric feedwater line break upstream of feedwater level control valves	2.2×10^{-3}
10	IE-FWBA	Asymmetric feedwater line break downstream of steam generator (SG) check valve	5.8×10^{-5}
11	IE-LOR	Loss of reactivity control leading to uncontrolled power increase	4.2×10^{-2}

Each end state of the analyzed event tree sequences is assigned one of three general conditions:

1. success [S] (i.e., no releases for the entire duration of the mission time),
2. not developed further [NDF] (i.e., the sequence is terminated because the estimated sequence frequency is less than 1.0×10^{-9}/year), or
3. plant damage state [PDS] (i.e., some degree of damage is expected).

There are ten PDSs listed in the design-assist analysis document. Although *Probabilistic Safety Assessment Methodology, ACR*[8] lists 11 PDSs, for the purposes of the design-assist document only 10 PDSs were deemed necessary. The 10 PDSs are grouped into 3 broad categories signifying the severity of core damage. PDS 0–PDS 2 are considered to be severe core damage (SCD) states, PDS 3–PDS 6 are considered to be limited core damage (LCD) states, and PDS 7–PDS 9 have some potential for fuel damage and/or fission product release (Table 19). Section 4 of *Probabilistic Safety Assessment Methodology, ACR*[8] provides a thorough description and assessment of each of these plant damage states.

Table 19. Plant Damage States
(*Source: Preliminary Design Assist PSA Level 1—Selected Full Power Event Trees*[10])

PDS	Definition	Description	Category
PDS 0	Early loss of core integrity at high power and pressure as a result of a failure to shutdown when required	This PDS is assigned to end states resulting from failure of all shutdown functions when the shutdown is required to mitigate a power-cooling mismatch. The reactor core disassembles at high internal pressure.	SCD
PDS 1	Late loss of core integrity at decay power starting from high HTS pressure caused by a loss of all primary and backup heat sinks	Loss of primary heat sinks at HTS high pressure (e.g., loss of feedwater + service water + RWS make-up to SGs). A small number of channels fail to relieve HTS pressure, but ECC and moderator heat sinks are unavailable. The reactor core disassembles at low internal pressure. The core debris can be retained in the calandria if the shield water heat sink is available.	
PDS 2	Late loss of core integrity at decay power starting from low HTS pressure caused by a loss of all primary and backup heat sinks	LOCA + loss of emergency core cooling (LOECC) + loss of moderator heat sink. The reactor core disassembles at low internal pressure. The core debris can be retained in the calandria if the shield water heat sink is available.	
PDS 3	Early, widespread fuel and channel damage at decay power starting from low HTS pressure caused by a loss of primary heat sinks and a failure of emergency core cooling system (ECCS)	LOCA + LOECC cause rapid core voiding; e.g., large LOCA + failure of emergency cooling injection system (ECIS) and long-term cooling system (LTCS). The moderator heat sink is available to maintain the fuel within the fuel channels, which are deformed but intact.	LCD
PDS 4	Late, widespread fuel and channel damage at decay power starting from low HTS pressure caused by a loss of primary heat sinks and a failure of ECCS	LOCA + LOECC cause slow core voiding (e.g., a small LOCA + failure of ECIS and LTCS or any size LOCA + failure of LTCS). Moderator heat sink is available to maintain the fuel within the fuel channels, which are deformed but intact.	
PDS 5	Early, limited fuel damage at decay power starting from low HTS pressure caused by a loss of primary heat sinks	LOCA with ECCS performing as intended. No temperature-induced fuel failures, but some incipient cladding defects open. All pressure tubes remain intact.	
PDS 6	Late, limited fuel and channel damage at decay power starting from low HTS pressure caused by a loss of primary heat sinks	A small LOCA (leak) + a loss of SG cooldown or a loss of all feedwater supplies. The HTS voids gradually at a high pressure. A small number of pressure tubes and bellows (or a few fuel channels) fail to depressurize the HTS. The ECIS activates while the fuel temperatures are moderate. The LTCS provides the long-term heat sink. The fuel damage is mainly mechanical.	
PDS 7	Early but limited fuel damage caused by a single-channel LOCA and containment pressurization	Inlet feeder or end-fitting breaks with ECCS performing as intended. Up to whole-channel fission product inventory could be released into the containment.	Potential fuel damage and/or fission product release
PDS 8	Early but limited fuel and channel damage caused by a single channel LOCA and no containment pressurization	In-core LOCAs (pressure tube rupture and calandria tube rupture) with ECCS + moderator system performing as intended (i.e., no significant steam discharge into containment, fission product release into moderator).	
PDS 9	Tritium release	Moderator spills or boiling, but no fuel damage.	

8.1 Methodology

This report reviews the methodology associated with the development of the 11 event trees. In addition, 2 of the 11 event trees were reviewed for their application of the methodology.

More than 20 systems are used in mitigating the accident sequences for the 11 IEs that AECL chose for further development. Each of these systems is assigned a reliability target value that is based on simple fault tree analyses, previous CANDU PSAs, and engineering judgement. Very simple operator error probabilities are also assigned. The human error probabilities (HEPs) are diagnostic errors only and are based on previous CANDU PSA results. These HEPs do not include execution actions by the operators.

Two general criteria are assigned for all the accident sequences:

1. the summed SCDF for all internal events occurring at power should be $< 1.0 \times 10^{-6}$/year, and
2. any sequence that has an end state of PDS 0, PDS 1, or PDS 2 should have a frequency $<1.0 \times 10^{-7}$/year.

To facilitate the design-integration process and usefulness of its study, AECL identified ~14 generic assumptions for developing all of its event trees (Table 20). These generic assumptions range from operating the reactor at 100% full power prior to an accident to all of the on-site diesel generators being capable of operating for 24 h without cooling.

Each of the 11 selected IEs for the event tree analyses were reviewed further by AECL to identify which assumptions were specifically related to each of the individual event trees. Because it is necessary to understand the expected plant responses to develop the accident sequences for the 11 IEs, the details were provided to the PSA analysts. The results for each event tree are presented and discussed.

The overall results from the design-assist analysis document indicate that the target value of 1.0×10^{-6}/year for the summed SCDF was not met without factoring in recovery actions. The estimated summed SCDF was 1.6×10^{-6}/year with 95% (i.e., 1.5×10^{-6}/year) of the SCDF occurring in PDS 2, "late loss of core integrity at decay power starting from low HTS pressure." Even if credit is taken for such things as a reduced pressure tube rupture frequency (by a factor of 4), reduced frequency for loss of Class IV (offsite) power (by a factor of 3), decay heat removal capability by one SG, and revising operator recovery action credit, the SCDF estimate is reduced to 1.3×10^{-6}/year, still above the target value.

Table 21 lists the top ten contributors to the summed SCDF. The three accident sequences that have slightly higher frequencies than the SCD target value of 1.0×10^{-7}/year without recovery are:

1. pressure tube and calandria tube rupture followed by loss of LTC,
2. pressure tube and calandria tube rupture followed by loss of Class IV (offsite) power and loss of auxiliary condensate supply to the deaerator, and
3. feeder stagnation break followed by loss of dormant ECC injection.

When recovery factors are applied, the two sequences that remain above the target frequency are:

1. pressure tube and calandria tube rupture followed by loss of LTC, and
2. feeder stagnation break followed by loss of dormant ECC injection.

Table 20. Generic Assumptions Used for Developing Event Trees
(*Source: Preliminary Design Assist PSA Level 1—Selected Full Power Event Trees*[10])

No.	Assumption
1	The reactor operates at 100% full power prior to the accident.
2	All on-site diesel generators (DGs), auxiliary condensate-extraction pump, auxiliary feedwater pumps, and instrument-air compressors are air-cooled or are capable of operating for 24 h without cooling.
3	Auxiliary feedwater pumps have sufficient head to supply the minimum required flow with the main steam safety valves (MSSVs) relieving steam by lifting against their spring load.
4	Auto depressurization of SG secondary side is performed by four MSSVs.
5	One Class III DG can run one raw service water (RSW) pump and one recirculating cooling water (RCW) pump plus other essential loads.
6	Moderator and LTC systems require cooling water to operate, which may be supplied from Division 1 or Division 2 RCW system.
7	A failure of instrument air system does not impact service water supplies when: a. all critical valves fail to their safe-state, and b. all valves that need to be opened after the IE have a backup gas supply (e.g., bottles)
8	The emergency feedwater supply from RWS to SGs is available for the mission time of 24 h when: • isolating valves can be actuated without any dependency of Class IV (offsite) and Class III power (DGs) for ~3 h, • the same valves can be manually operated on long term basis (beyond 3 h) in order to prevent spilling of water from the SGs, thereby ensuring that RWS inventory can last for the mission time of 24 h, and • the IE does not cause a discharge of HT coolant into the reactor building.
9	Moderator pony motors are automatically provided with Class III power (DGs) within a few minutes following a loss of Class IV (offsite) power.
10	For all events that involve a small LOCA as an IE or a consequential failure, it is presumed that the post-accident break discharge is not large enough to remove decay heat from the HTS as liquid is at saturation temperature or less. (The ECC function of the LTC is not sufficient to act as a heat sink; a SG heat sink is also required for these events.)
11	In the absence of forced HTS circulation, SGs provide effective heat sink only if both of them are available (i.e., it is presumed that thermosyphoning breaks down when only one SG is available).

Table 21. Significant Contributors to the Summed SCDF
(*Source: Preliminary Design Assist PSA Level 1—Selected Full Power Event Trees*[10])

No.	Initiating event	Sequence description[a]	Frequency without recovery (/year)	Frequency[b] with recovery (/year)
1	IE-PCTR	Pressure Tube and Calandria Tube Rupture Followed by Loss of LTC	2.85×10^{-7}	2.85×10^{-7}
2	IE-PCTR[c]	Pressure Tube and Calandria Tube Rupture Followed by Loss of Class IV (offsite) Power and Loss of Auxiliary Condensate Supply to the Deaerator	1.38×10^{-7}	1.38×10^{-8}
3	IE-FSB	Feeder Stagnation Break Followed by Loss of ECC Injection	1.33×10^{-7}	1.33×10^{-7}
4	IE-PTR[c]	Pressure Tube Rupture Followed by Loss of LTC and Loss of Moderator Cooling	9.49×10^{-8}	9.49×10^{-9}
5	IE-FSB	Feeder Stagnation Break Followed by Loss of Main and Auxiliary Feedwater Supply to SGs	9.45×10^{-8}	9.45×10^{-8}
6	IE-PTR[c]	Pressure Tube Rupture Followed by Loss of Class IV (offsite) Power, Loss of Auxiliary Condensate to Deaerator, and Loss of Moderator as a Heat Sink	7.35×10^{-8}	7.35×10^{-9}
7	IE-LCL4	Loss of Class IV (offsite) Power Supply and Failure to Start of all Standby DGs, Followed by Operator Failure to Actuate/Open the MSSVs	6.91×10^{-8}	6.91×10^{-8}
8	IE-FSB	Feeder Stagnation Break Followed by Loss of Class IV (offsite) Power and Loss of Auxiliary Feedwater Supply to SGs	5.55×10^{-8}	5.51×10^{-8}
9	IE-FWBA	Asymmetric Feedwater Line Break Followed by Loss of Dormant ECC Injection	5.51×10^{-8}	5.51×10^{-8}
10	IE-FBIO[c]	Feeder Break followed by Loss of LTC and Loss of Moderator Cooling	4.75×10^{-8}	4.75×10^{-9}

[a] All event sequences end in plant damage state PDS2.
[b] No details of recovery actions were provided in the design-assist analysis document.

[c] The frequency of sequences 2, 4, 6, and 10 were reduced by an order of magnitude by crediting the moderator makeup or reserve feedwater tank as a supply of water.

AECL reduced the frequencies of sequences 2, 4, 6, and 10 by an order-of-magnitude by crediting the moderator make-up or reserve feedwater tank as a supply of water.

The summed frequencies for the limited core damage sequences indicate that the summed frequency for PDS 4 satisfies the regulatory guidelines in *Safety Analysis of CANDU Nuclear Power Plants* (CNSC Regulatory Guide C-006[20]). The summed frequencies for PDS 6 were almost all (~90%) from one event─an asymmetric feedwater line break. (An asymmetric line break is a break in 1 of 2 divisions in a system. A symmetric line break is a break that affects the entire system.) A review of the 11 event trees did not identify any accident sequences in PDS 3 or 5.

The design-assist document concludes that this design-assist assessment has "provided insights into the adequacy of the safety design" and that internal event sequences were identified that "will likely dominate the SCDF."

8.2 Strengths and Weaknesses

Overall, the level of detail in the design-assist analysis document is comprehensive but not complete. The methodology suffers from the lack of definition because the source referenced for the methodology[8] only indicates that it "generally" follows NUREG/CR-2300.[3] The breadth and extent of what is followed in NUREG/CR-2300 should be listed. It is considered to be a weakness that what is followed in NUREG/CR-2300 (and what exceptions were taken) is not explicitly provided or referenced in the document.

The "loss of Class 3 Power" subevent-tree were specifically reviewed as part of this technical review. The loss of Class 3 power subevent tree is duplicated in 9 of the 11 selected IEs contained in the appendixes of the design-assist analysis document (e.g., FBIO-A and LCL4-B). Only "asymmetric feedwater line break downstream of SG check valves" and "loss of reactor control leading to core power excursion" events did not challenge the DGs.

Feeder Break IE

The sequence of the event progresses from the initiating event to reactor shutdown followed by a challenge of the support systems─the four DGs, crash cooldown of the SGs, and service water divisions. Injection of the ECI accumulator tanks refills the HTS. The HTS pumps are tripped before the ECI accumulators inventory depletes and the LTC-ECC starts. The SGs continue to serve as heat sinks in conjunction with the LTC heat exchangers. These sequences are typical for a "small break LOCA-like" rupture, that requires water for cooling the core along with a successful scram and available electrical power. If water is not available, then some heat sink is needed to avoid severe core damage.

The frequency for the Feeder Break IE (IE-FBIO) given in the design-assist analysis document was compared with the feeder break IE given in *Systematic Review of Plant Design for Identification of Initiating Events, ACR*.[102] The IE frequency for the feeder break given in this document ($f = 2 \times 10^{-3}$/year) is higher than that used in *Systematic Review of Plant Design for Identification of Initiating Events, ACR*[102] (GE-05, $f = 8.04 \times 10^{-4}$/year). The difference between frequencies of the IEs for the feeder break is unknown but it is considered to be a weakness that documents published within 2 weeks of each other (1/14/2004 and 1/28/2004) by the same author have different IE frequencies.

A check was performed on the sequences in the feeder break event tree to verify that the sequence frequencies were consistent and calculated correctly based on the event tree branch probabilities given in the event tree. The sequence frequencies were consistent with the event tree branch probabilities multiplied by the initiating event frequency. Further, the sequences ending in PDS 0, PDS 1, PDS 2, and PDS 7 were all summed and verified consistent with the results tabulated in Section 8 of the design-assist analysis document.

A review of the event tree indicated that to avoid a SCD state (i.e., PDS 0, PDS 1, or PDS 2) after a feeder break, the plant must scram and Class IV (offsite) power or at least one diesel generator (DG) should be available. If Class IV (offsite) power or at least one DG is not available, at least one division of the service water system and one of three heat sinks must be available (long-term cooling, HTS make-up, or the moderator acting as a heat sink) to prevent SDC. A failure to scram results in PDS 0, the most severe plant damage state. If the plant scrams and ac power is unavailable (Class IV (offsite) power is lost or three DGs are unavailable for the 24-h mission time) or there is a failure to crash cooldown the SGs or both the divisions of service water are unavailable, the plant will be in PDS 1.

All of the accident sequences for Feeder Break IE appear to be reasonable and there were no unusual sequences identified.

The top events for the feeder break event tree were assessed against the system reliability/unavailability target values (with and without DG availability) listed in Tables 5-1 and 5-2 in the design-assist analysis document. The branch point probabilities were verified for all the top events except for DG-AV=4, DG-AV=3, DG-AV=2, and DG-AV=1 because these values are not given in the design-assist analysis document.

Section 5 of the design-assist analysis document indicates that "The reliability targets of Tables 5-1 and 5-2 are currently being verified by detailed fault tree analysis." The document may be considered to be lacking in substance without some verification of these values. For the purposes of the current review, it was assumed that the entries in these two tables were correct.

A summary of the consequences for the feeder break accident sequences by plant damage state was tabulated for this review and are presented in Table 22.

Table 23 provides a list of several branch point probabilities that appear to be nonconservative. Although no number was found for comparison to the crash cooldown of the SGs, the 1.0×10^{-5} probability, based on engineering judgment, seemed low. The service water system for the ACR-700 supplies cooling to the gland seals and bearings of the HTS pumps. The failure probability for the loss of both service water divisions is 1.0×10^{-5} . The total loss of nuclear service water that provides cooling to the RCS pump motors at Catawba 1[104] is 1.8×10^{-4}. Based on this simple comparison, the loss of service water at an ACR-700 appears to be nonconservative.

The accident sequences that lead to SCD for the Feeder Break IE are given in Table 24. There is 1 event in PDS 0, 3 events are in PDS 1, and 17 events are in PDS 2.

These sequences are characterized by:

- If the moderator is available as a heat sink, then there is minimal core damage; however, if the moderator is not, then severe core damage results.

Table 22. Summary of Consequences for the Feeder Break

Sequence consequence	Sequence frequency (/year)	Number of cutsets contributing to sequence
Reactor disassembles at high internal pressure (PDS 0)	2.00×10^{-9}	1
Late loss of core integrity at decay power starting from high HTS pressure caused by a loss of all primary and backup heat sinks (PDS 1)	3.10×10^{-8}	3
Late loss of core integrity at decay power starting from low HTS pressure caused by loss of all primary and backup heat sinks (PDS 2)	9.48×10^{-8}	17
Late, widespread fuel and channel damage at decay power starting from low HTS pressure caused by a loss of primary heat sinks and a failure of ECCS (PDS 4)	1.30×10^{-5}	15
Early but limited fuel damage caused by a single-channel LOCA and containment pressurization (PDS 7)	1.99×10^{-3}	5
Not developed further (NDF)	1.41×10^{-8}	6

Table 23. Nonconservative Branch Point Failure Probabilities

Event	Probability	Comparable U.S. failure probability
Crash cooldown of the SGs (CC)*	1.00×10^{-5}	9.9×10^{-5} (Ref. 105)
Service water system divisions 1 and 2 (SWD1&D2)	1.00×10^{-5}	1.8×10^{-4} (Ref. 104)

*The crash cooldown function for the ACR-700 is similar to AFW and secondary side heat removal using the atmospheric discharge valves at a generic CE plant.

Table 24. Dominant Accident Sequences That Lead to SCD for Feeder Break Events

Accident Sequence	**Plant damage state**	**Frequency (/year)**
Feeder break, failure to shutdown the reactor	PDS 0	2.00×10^{-9}
Feeder break, reactor shutdown, power available from switchyard, crash cooldown of steam generators fails	PDS 1	1.90×10^{-8}
Feeder break, reactor shutdown, power available from switchyard, crash cooldown of steam generators is successful, service water system divisions 1 and 2 (SWD1&D2) fail	PDS 1	1.90×10^{-8}
Feeder break, reactor shutdown, power available from switchyard is unavailable, all 4 DGs fail	PDS 1	5.76×10^{-9}
There are 17 events in PDS 2 that lead to severe core damage. These sequences are mostly characterized by: successful scram, Class IV (offsite) electrical power or at least three DGs are available, and crash cooldown of the SGs is successful. Severe core damage results if any of the following failures occur: crash cooldown fails, both divisions of SW fail, ECI is successful but the moderator fails as a heat sink, or both ECI and the moderator as a heat sink fail.	PDS 2	9.48×10^{-8}

LOOP IE

The event tree for the "complete loss of Class IV (offsite) power at one ACR unit at a dual-unit site" (IE-LCL4) was replicated with the branch probabilities from the event tree of Appendix F and Tables 5-1 and 5-2 inserted into the duplicate event tree. All sequence frequencies were calculated and were verified to be calculated correctly based on the event tree branch probabilities provided. When the duplicated event tree was analyzed for those sequences ending in NDF, it was determined that the summed frequency exceeded 1.0×10^{-8}/year.

The frequency for the LOOP IE (IE-LCL4) given in the design-assist analysis document was compared with the loss of offsite power (LOOP) IE (loss of Class IV power) given in *Systematic Review of Plant Design for Identification of Initiating Events, ACR*.[102] The IE frequency for the LOOP given in this document ($f = 3 \times 10^{-1}$/year) is larger than that used in *Systematic Review of Plant Design for Identification of Initiating Events, ACR*[102] (GE-58, $f = 2.17 \times 10^{-1}$/year). The difference between frequencies of the IEs for the loss of offsite power events is unknown but it is considered to be a weakness that documents published within 2 weeks of each other (1/14/2004 and 1/28/2004) by the same author have different IE frequencies.

A summary of the consequences for the loss of Class IV (offsite) power accident sequences was tabulated for this review and are presented in Table 25.

Table 25. Summary of Consequences for the Loss of Class IV (Offsite) Power (LOOP)

Sequence consequence	Sequence frequency (/year)	Number of cutsets contributing to sequence
Reactor disassembles at high internal pressure (PDS 0)	3.00×10^{-9}	1
Late loss of core integrity at decay power starting from low HTS pressure caused by loss of all primary and backup heat sinks (PDS 2)	7.39×10^{-8}	2
Late, limited fuel and channel damage (PDS 6)	2.21×10^{-5}	21
Main steam line break (MSLB)	1.8×10^{-6}	1
Main steam line break and loss of Class IV (offsite) power (MSLB/CL4)	1.2×10^{-6}	1
Not developed further	1.41×10^{-8}	59

Table 26 provides a list of several branch point probabilities that appear to be nonconservative.

The LOOP event tree has a reactor trip failure probability of 1.0×10^{-8}. The event tree for total loss of one service water division has a failure probability to shutdown of 3.0×10^{-8}. All of the other event trees in the design-assist analysis document have a probability of failure to shutdown by shutdown system

(SDS) 1 and SDS 2 (event RS is reactor shutdown by SDS1 and SDS2) as 1.00 × 10^{-6}. Without an explanation, the differences in shutdown probabilities appears to be a weakness in quality control.

The dominant accident sequences that lead to SCD are given in Table 27.

Table 26. Nonconservative Branch Point Failure Probabilities

Event	Probability	Comparable U.S. failure probability
Reactor shutdown (RS) by SDS1 and SDS2 and reactor regulating system (RRS)	1.00 × 10^{-8}	2.0 × 10^{-6} (Refs. 106–107)
Steam generator pressure relief via spring-loaded MSSVs (SGPR)	1.00 × 10^{-5}	3.0 × 10^{-4} (Ref. 108–109)
HTS inventory loss via liquid relief valves (CLPRV)	4.00 × 10^{-6}	Not applicable
Service water system divisions 1 and 2 (SWD1&D2)	1.00 × 10^{-5}	1.8 × 10^{-4} (Ref. 104)

Because of the low failure probability to trip the reactor, the frequency for the LOOP sequence with a failure to trip (3.0 × 10^{-9}/year) appears to be too low. As an example, the comparable event at Catawba[104] is 3.99 × 10^{-7}/year.

The two MSLB sequences are not classified into any of the 10 plant damage states.

The LOOP event tree, just like the other IEs, evaluates the availability of the service water systems to provide cooling water to non-safety related systems to support unit power generation, and to safety related systems to mitigate and/or prevent the effects of accident conditions. The service water systems include the two systems named the RSW and the RCW systems.

System heat loads under normal and abnormal operating conditions (with and without Class IV (offsite) or III (DG) electric power supplies available) form the basis for the service water systems design. Other systems, including the RWS, provide makeup cooling water when the RSW and/or RCW systems are unavailable.

The RWS provides an emergency source of water to the containment sumps for recovery by the long term cooling system in the event of a LOCA to ensure net positive suction head for the long term cooling pumps. The RWT, located at a high elevation in the reactor building, is a key component of the RWS. The RWT is connected to the various systems by means of piping fitted with remotely controlled isolation valves. In addition, the RWT can provide emergency make-up water by gravity to the steam generators (emergency feedwater), moderator system, shield cooling system, pressure and inventory system, and the HTS if required.[80]

Table 27. Dominant Accident Sequences That Lead to SCD for LOOP Events

Accident Sequence	Plant damage state	Frequency (/year)
LOOP, failure to trip reactor	PDS 0	3.00×10^{-9}
LOOP, reactor trips, failure to relieve steam generator pressure, offsite power recovered within 60 min	MSLB	1.80×10^{-8}
LOOP, reactor trips, failure to relieve steam generator pressure, failure to recover offsite power within 60 min	MSLB/CL4	1.20×10^{-8}
LOOP, reactor trips, steam generator pressure relieved, no LOCA via D_2O storage tank (liquid relief valves (LRVs) fail to reclose), failure to recover offsite power within 60 min, all DGs fail, operator opens MSSVs, and failure of emergency feedwater supply from RWS to SG	PDS 2	4.79×10^{-9}
LOOP, reactor trips, steam generator pressure relieved, no LOCA via D_2O storage tank (LRVs fail to reclose), failure to recover offsite power within 60 min, all DGs fail, operator fails to open MSSVs, and failure of emergency feedwater supply from RWS to SG	PDS 2	6.91×10^{-8}

When a LOCA occurs, the RWT is emptied onto the containment floor to ensure sufficient water and suction head for recirculating water in the HTS. There does appear to be the potential for three different scenarios:

1. A LOCA occurs early in a sequence of events resulting in no or insufficient RWS water being available for emergency feedwater, moderator system, shield cooling system and pressure and inventory system.
2. A LOCA occurs late in a sequence of events resulting in no or insufficient RWS water being available for recirculation flow in the HTS.

3. One or more isolation valves spuriously open and divert water to other systems leaving no or insufficient RWS water available for recirculation flow in the HTS system or other systems requiring makeup water.

It seems possible that a LOOP with offsite power restored and a resulting LOCA via the HTS liquid relief valves could drain the RWT (LCL4-C, p. F-10). The associated accident sequences challenge the RWS/RCW and EFW systems. If the water in the RWT is emptied onto the containment floor, there may be insufficient water available for the RWS and EFW systems.

The fourth paragraph of Section 1 on Page 1-1 of the design-assist analysis document states in part,

> ...the passive water supplies from the RWS to process systems other than steam generators were not finalized. As a result, the passive accident mitigation features of the ACR are not treated systematically and comprehensively in this report. The Emergency Feed Water (EFW) supply from the RWS is modeled, but the gravity water supplies to the other process volumes (i.e., to Heat Transport System (HTS), Calandria Vessel, End Shield Tanks, and Shield Tank) are not credited unless an ‘individual-sequence’ SCDF is close to its acceptance value. In two of the event trees, the event trees were expanded to include the gravity water supply to the HTS. Models of all passive water supplies from the RWS will be included in the future.

Section 6.2.4.7 of the design-assist analysis document indicates

> Should the ECC make-up fail, water can be supplied from the RWS into the HTS for the duration of mission time at a sufficient rate to maintain the fuel channels flooded with water. This assumption implies that the HTS remains depressurized for the gravity make-up to work. It may not be consistent with earlier assumption (Item 5 in Section 6.2.4 of the design-assist analysis document). Future analysis will explore and confirm this assumption.

This latter IE is a "feeder stagnation break with consequential channel rupture" and was not analyzed or reviewed in depth in this report.

The loss of Class IV (offsite) power supply IE indicates in Section 6.2.6.5.c of the design-assist analysis document that RWS will be available for the SGs for the 24 hour mission. The "loss of inventory in shield cooling system" IE assumes (Section 6.2.7.3) that RWS is available for emergency feedwater (EFW) to the SGs; however, it would be manually stopped once the SDC function of LTC is operational, and RWS make-up for the shield tank or end shields is not credited. Similarly, RWS is not credited in the small steam discharge causing low deaerator level IE as a feedwater supply for auxiliary feedwater (AFW) (Section 6.2.8). However, the design-assist analysis document also indicates (Section 6.2.8) that EFW can be supplied manually to the SGs within three hours. The assumptions for the "asymmetric feed water line break downstream of SG check valve" IE indicate that RWS supply for EFW is not available in the early stages of the accident because high pressure in the reactor building will inhibit the automatic opening of the supply valves. Later, after the operator has verified the integrity of the HTS boundaries, the valves may be manually opened. It is expected that this will take place 15 minutes into the accident.

Event tree LCL4-A (p. F-3) represents a LOOP with the recovery of offsite power. Although offsite power has been recovered, the first branch point indicates that the probability of SWD1&2 being unavailable given offsite power is *unavailable* is 1.0 × 10^{-5}. The other event trees in the design-assist analysis document indicate that the probability of SWD1&2 being unavailable given offsite power is *available* is also 1.0 × 10^{-5}. There are two questions:

1. if offsite power has been recovered, how come it is still modeled as being unavailable, and
2. how can the probabilities of SWD1&2 failing be the same for offsite power being unavailable and offsite power being available?

Some accident sequences with the end state NDF could easily be assigned a plant damage state. For example, consider the following accident sequences that begin with a

- LOOP,
- reactor successfully shut down,
- successful pressure relief through an SG,
- HTS integrity remains intact (i.e., no inventory loss via the LRVs),
- power in switchyard not restored within 60 min, and
- service water divisions 1 and 2 provide cooling.

In the sequences that follow, if the operator fails to successfully start the LTC-SDC, the sequence is not developed further. However, if the operator successfully starts the LTC-SDC but the system fails, the plant damage state is PDS 6. For these sequences, the results are the same—the LTC-SDC failed to run—and the plant damage states are the same—PDS 6. Thus, although similar event sequences are not developed further because their frequency is < 1.0 × 10^{-9}/year, they could be placed into PDS 6 without much effort (Table 28).

Table 28. Example of Accident Sequences Leading to Limited Core Damage for LOOP Events That Could be Assigned a Plant Damage State (Successful Depression)

Accident Sequence	Plant damage state	Frequency (/year)
AFW supply to SGs fails, auto depressurization system is successful, EFW supply to SGs fails, operator successfully starts the LTC-SDC, and LTC-SDC fails	PDS 6	2.59 × 10^{-9}
AFW supply to SGs fails, auto depressurization system is successful, EFW supply to SGs fails, and operator fails to start LTC-SDC	NDF	5.23 × 10^{-10}

According to the design-assist document, if the estimated frequency of a sequence is less than 1.0 × 10^{-9}/year, the sequence is terminated and assigned the end state NDF. However, several accident sequences with frequencies < 1.0 × 10^{-9}/year are developed further. For example, consider the same LOOP sequence given above:

- LOOP,
- reactor successfully shut down,
- successful pressure relief through an SG,
- HTS integrity remains intact (i.e., no inventory loss via the LRVs),
- power in switchyard not restored within 60 min, and
- service water divisions 1 and 2 provide cooling.

The sequence proceeds to the operator successfully starting the LTC-SDC and the LTC-SDC fails or the operator fails to start the SDC (Table 29). Similar to those events in Table 28, the result is that the LTC-SDC failed to run. The plant damage state is PDS 6. In this instance however, the frequency of the each event is below the 1.0 × 10^{-9}/year cutoff but a plant damage state is assigned to one of the events. Again, many sequences labeled NDF could be placed into a PDS category with minimal effort.

Table 29. Example of Accident Sequences Leading to Limited Core Damage for LOOP Events That Could be Assigned a Plant Damage State (Depressurization Fails)

Accident Sequence	Plant damage state	Frequency (/year)
AFW supply to SGs fails, auto depressurization system fails, operator opens MSSVs to depressurize the SGs, operator successfully starts the LTC-SDC, and LTC-SDC fails	PDS 6	3.66 × 10^{-10}
AFW supply to SGs fails, auto depressurization system fails, operator opens MSSVs to depressurize the SGs, and operator fails to start the LTC-SDC	NDF	7.40 × 10^{-11}

According to Section 8.7 of *ACR-700 Technical Description*,[80] the DGs are either air-cooled or are capable of operating for 24 hours without cooling (see generic assumption 2 in Table 3). It is questionable that the DGs can operate 24 h without cooling. Moreover, the *ACR-700 Technical Description*,[80] indicates that each DG "has an indoor day tank with a capacity for a minimum four hours of operation." Thus, although the day tank has a 4 hour fuel supply, credit is taken for 24 h of continuous operation of the DG. The assumption that the DGs can operate for 24 h without cooling on a 4-h fuel supply in its day tank with out any discussion of providing a longer-term fuel supply is considered to be a weakness.

Section 6.1 of the design-assist analysis document assumes that "the auxiliary feedwater (AFW) pumps have sufficient head to supply the minimum required flow with the MSSVs relieving steam by lifting against their spring load." This assumption needs clarification and more supporting information to be considered valid. For example, does this assumption mean that the AFW pumps provide sufficient head to supply the minimum flow and lift the MSSVs? Does it mean that when steam pressure is high enough (i.e., the steam pressure exceeds the MSSV spring load), the MSSVs will open and remain open as long as the steam pressure remains high? In this case the AFW pumps are expected to supply sufficient cooling water to account for the losses through the open MSSVs and any additional heat loads. Section 5.2.5 of the *ACR-700 Technical Description*[80] indicates in the design basis for the steam and feedwater systems that the AFW pumps are 4% capacity operating on Class III power (DGs). The design-assist analysis document further indicates that the MSSVs have the capacity to relieve 120% of the steam flow from each SG. Therefore, it is not clear that the assumption that the AFW pumps have sufficient head to provide the minimum required flow with the MSSVs relieving steam is a valid assumption. Specific information or analyses should be provided to support this assumption; otherwise, it is considered to be a weakness.

The HEP values listed in Table 30 (Table 4-1 of the design-assist document) seem both nonconservative (HEPs for limited action time) and overly conservative (HEPs for long action time) for HEP values for diagnostic errors. It is expected that when NUREG/CR-4772 (as indicated in Section 4 of the design-assist analysis document) is applied, the values at the lower end of allowed time (0 –15 min) and the upper end (2–4 h and 4–8 h) will change.

Table 30. HEPs Associated with Operator Action Times

Action time	HEP
0–15 min	1 (no credit)
15–30 min	1.0×10^{-1}
30–60 min	1.0×10^{-2}
1–2 h	1.0×10^{-3}
2–4 h	1.0×10^{-4}
4–8 h	1.0×10^{-5}

When evaluating generic safety issue (GSI) B-56, AECL indicates that "There are two onsite standby diesel-generator sets for each unit of the two-unit ACR-700 plant, with all four being available to supply the safety functions for each unit."[110] This means that the medium voltage distribution system with the "four Class III DGs common for the two units"[111] "includes inter-unit connections allowing sharing of the standby diesel generators" between units.[112] The crediting all four DGs being available for one unit assumes that the LOOP only affects the one unit at a two unit site. This may be an unrealistic (nonconservative) assumption.

On numerous occasions, the design-assist analysis document indicates that the ACR-700 is to be "a two unit integrated plant with each unit having a nominal gross output of 731 MWe." Several figures (Figs. 1-1, 1-2, 2.3-1, and 8-1 in the design-assist document) indicate a two unit plant with a total of four DGs. However, Table 13.2-1 lists four DGs under the equipment list for one unit. This is inconsistent with other documents and this inconsistency between documents is considered to be a weakness.

As noted above, a DG may supply any of the safety buses at either unit at a dual-unit site. The subevent trees (FBIO-A, LCL4-B, FSB-A, etc.) show that four DGs are credited for use following a LOOP to one unit at a two-unit site (complex).

According to *Regulatory Guide 1.6*,[113]

> Each a-c load group should have a connection to the preferred (offsite) power source and to a standby (onsite) power source (usually a single diesel generator). The standby power source should have no automatic connection to any other redundant load group. At multiple nuclear unit sites, the standby power source for one load group may have an automatic connection to a load group of a different unit. A preferred power source bus, however, may serve redundant load groups.

Thus, the sharing of DGs between units and between load groups is allowed given that there are no automatic connections. It appears that the ACR-700 has automatic connections between electrical load groups.

To correctly model the DGs, dependencies between the DGs must be reflected. Typically, failures or unavailability of events appearing in the fault tree must be statistically independent.[113] That is, the probabality of an event occurring is not affected by the occurrence of any other event. In the case of the DGs, both random failure and maintenance of the DGs are coupled among the DGs. The random failure model for the DGs needs to account for all the potential combinations of operating states of the DGs. Thus, the conditional probability of failure for all combinations of events is known. The conditional failure probability equations develop the conditional probabilities for each DG failure as a function of all possible combinations of other DG states. For example, one DG can fail when another DG is in a failed state or in an operating state.

The probabilities of three DGs available for 24 h having a better chance of success than four DGs available for the same time period appears to be counter-intuitive because the probabilities are not monotonic. For the ACR-700, the probabilities for 4, 3, 2, and 1 DG being available for 24 h are 0.07, 0.11, 0.086, and 0.087, respectively.[10] In comparison, the conditional DG failure probabilities for 1, 2, 3, or 4 DGs failed at Limerick are 0.017, 0.0068, 0.0054, and 0.0035, respectively.[114] It is considered to be a weakness that the event tree does not provide an explanation for unexpected, unusual, or calculated failure probabilities.

The LOOP event tree with all 4 DGs unavailable (e.g., SBO) event tree branch (IE-LCL4-B5, p. F-15) requires the operator to open the MSSVs within 60 min and the EFW to supply water to the SGs. The EFW is a safety system without motor- or turbine-driven pumps (i.e., it is a gravity-drain system). However, electricity is required to open the isolating valves so that the system can be actuated. These isolation valves can be actuated without any dependency on offsite power or the DGs for ~3 h because they are supplied with Class II power (uninterruptible ac power supply) power. The event tree is modeled correctly but this accident sequence is described because of the subtle dependence on Class II power (uninterruptible ac power supply).

IE frequencies

The scope of the *Preliminary Design Assist PSA Level 1—Selected Full Power Event Trees*[10] report was to develop and analyze event trees for selected IEs that "are judged to produce high values of 'individual-sequence' SCDF [severe core damage frequency] and/or be major contributors to 'summed' SCDF." Eleven IEs are judged to be of importance to the risk profile of the ACR-700 were selected for evaluation. Annual frequency of occurrence for each are provided in Table 31. The estimated frequencies for these 11 events are compared to the IE frequencies given in AECL's *Preliminary Design Assist PSA Level 1—Selected Full Power Event Trees ACR-700*. Of the 11 IEs compared, frequencies were not provided for 4 of the 11 IEs, 3 had comparable IE frequencies, and 4 had frequencies that differed by up to an order-of-magnitude. The reason for these differences is unknown but these reports were published by the same author within two weeks of each other.

8.3 Summary

The reporting and methodology strengths and weaknesses noted from the review of the selected full-power event trees summarized in Tables 32–33.

Table 31. Comparison of IE Frequencies from ACR-700 Preliminary PSA Studies

IE description	IEs from AECL Analysis Report, 10810-03660-AR-001[a]	IEs from AECL Assessment Document, 108-03660-ASD-001[b]	
	Frequency (/year)	ACR-700 group designator	Frequency (/year)
Small LOCA - pressure tube rupture (with calandria tube remaining intact	4.0×10^{-3}	GE-15	4.18×10^{-3}
Small LOCA - pressure tube and calandria rupture	6.0×10^{-5}	GE-13	4.18×10^{-4}
Feeder break	2.0×10^{-3}	GE-05	8.04×10^{-3}
Feeder stagnation break (with consequential channel rupture)	2.0×10^{-4}	GE-12	TBD
Total loss of one service water division (division 2)	5.0×10^{-2}	GE-56	TBD
Total loss of Class IV power supply to one ACR unit	3.0×10^{-1}	GE-58	2.17×10^{-1}
Loss of inventory in shield cooling system	4.0×10^{-4}	GE-76	TBD
Small steam discharge causing low deaerator level	1.0×10^{-1}	GE-40	3.24×10^{-2}
Symmetric feed water line break upstream of feed water level control valves	2.2×10^{-3}	GE-39	2.17×10^{-4}
Asymmetric feed water line break downstream of steam generator check valve	5.8×10^{-5}	GE-38	5.8×10^{-5}
Loss of reactivity control leading to uncontrolled power increase	4.24×10^{-2}	GE-06 GE-07	TBD

[a] *Preliminary Design Assist PSA Level 1—Selected Full Power Event Trees ACR-700* (Ref. 10)
[b] *Systematic Review of Plant Design for Identification of Initiating Events, ACR* (Ref. 9)

Table 32. Summary of Reporting Strengths Identified in the Review of the Selected Full-Power Event Trees

A check was performed on the sequences in the feeder break event tree to verify that the sequence frequencies were consistent and calculated correctly based on the event tree branch probabilities given in the event tree. The sequence frequencies were consistent with the event tree branch probabilities multiplied by the initiating event frequency. Further, the sequences ending in PDS 0, PDS 1, PDS 2, and PDS 7 were all summed and verified consistent with the results tabulated in Section 8 of the design-assist analysis document.
The top events for the feeder break event tree were assessed against the system reliability/unavailability target values (with and without DG availability) listed in Tables 5-1 and 5-2 in the design-assist analysis document. The values were consistent.
All of the accident sequences for Feeder Break IE appear to be reasonable and there were no unusual sequences identified.
All LOOP accident sequence frequencies were calculated and were verified to be calculated correctly based on the event tree branch probabilities provided.

Table 33. Summary of Reporting Weaknesses Identified in the Review of the Selected Full-Power Event Trees

All system availability values used in the event trees were not listed or discussed in the body of the design-assist analysis document.
Probabilities for the event sequences were based on simple fault tree analysis, previous CANDU experience, and engineering judgment. No indication is given on what method was used to determine the event sequence probabilities.
What is followed in NUREG/CR-2300 (and what exceptions were taken) is not explicitly provided or referenced in the design-assist analysis document.
The difference between frequencies of the IEs for the feeder break is unknown but it is considered to be a weakness that documents published within 2 weeks of each other (1/14/2004 and 1/28/2004) by the same author have different frequencies for the same IE.
The branch point probabilities were verified for all the top events except for DG-AV=4, DG-AV=3, DG-AV=2, and DG-AV=1 because these values are not given in the design-assist analysis document.
The criteria for terminating the development of a sequence is not followed. That is, some sequences below the cut-off frequency are assigned a PDS category. Some sequences labeled NDF can be placed into a PDS category with minimal effort.
The assumption that the DGs can operate for 24 h without cooling on a 4-h fuel supply in its day tank without any discussion of providing a longer-term fuel supply is not a valid assumption.
It is not clear that the assumption that the AFW pumps have sufficient head to provide the minimum required flow with the MSSVs relieving steam is a valid assumption.
The HEP values listed seem both nonconservative (HEPs for limited action time) and overly conservative (HEPs for long action time) for HEP values for diagnostic errors.
There are inconsistencies between the document under review with some of its references (e.g., inconsistencies between the number of DGs per unit or per site).
Several branch point probabilities appear to be nonconservative (e.g., crash cooldown of SGs, loss of service water divisions, reactor trip, SG pressure relief, loss of water through liquid relief valves).
Several event trees used a different probability of failing to shutdown the reactor without any explanation.
MSLB sequences are not classified into any of the 10 plant damage states.
The crediting of all four DGs being available for one unit assumes that the LOOP only affects the one unit at a two unit site. This may be an unrealistic (nonconservative) assumption.
It seems possible that a LOOP with offsite power restored and a resulting LOCA via the HTS liquid relief valves could drain the RWT (LCL4-C, p. F-10).

Table 33. Summary of Reporting Weaknesses Identified in the Review of the Selected Full-Power Event Trees (continued)

The assumptions for the "asymmetric feed water line break downstream of SG check valve" IE indicate that RWS supply for EFW is not available in the early stages of the accident because high pressure in the reactor building will inhibit the automatic opening of the supply valves. Later, after the operator has verified the integrity of the HTS boundaries, the valves may be manually opened. It is expected that this will take place 15 minutes into the accident.
Event tree LCL4-A (p. F-3) represents a LOOP with the recovery of offsite power. Although offsite power has been recovered, the first branch point indicates that the probability of SWD1&2 being unavailable given offsite power is *unavailable* is 1.0×10^{-5}. The other event trees in the design-assist analysis document indicate that the probability of SWD1&2 being unavailable given offsite power is *available* is also 1.0×10^{-5}.
It appears that the ACR-700 has automatic connections between electrical load groups.
The design-assist analysis document should provide an explanation for unexpected, unusual, or calculated failure probabilities.
The estimated frequencies for the 11 events given in *Preliminary Design Assist PSA Level 1—Selected Full Power Event Trees ACR-700* were compared to the IE frequencies given in AECL's *Preliminary Design Assist PSA Level 1—Selected Full Power Event Trees ACR-700*. Of the 11 IEs compared, frequencies were not provided for 4 of the 11 IEs, 3 had comparable IE frequencies, and 4 had frequencies that differed by up to an order-of-magnitude. The reason for these differences is unknown, but these reports were published by the same author within two weeks of each other.
Although the statement by AECL that "As part of the ACR detailed design development process, these assumptions are required to be supported by analysis and/or equipment suppliers' test records as appropriate" could be viewed as a weakness, it is recognized that this is a normal part of the design process.

Page Intentionally Blank

9. SUMMARY

This report documents the review of several GC and ACR PSA documents to provide insights into the strengths and weaknesses of the PRA methodology and analysis supporting the ACR-700 design. Any review of methodology and analysis documents can only yield insights into how the PRA will be performed; it is not a substitute for—nor can it be—an actual PRA review.

Because the GC PSA and ACR PSA are recently published documents (published in 2002), it would be questionable if the references or methods given in NUREG/CR-2300 (published in 1983) were used verbatim. Similarly, the newness of ASME RA-S-2002 (published in 2002) precludes the GC and ACR PSAs from following its guidance closely. Thus, as expected, AECL followed the guidance of NUREG/CR-2300 where appropriate and used updated data and methods when available. However, this practice was not always followed and, occasionally, out-of-date methods and data are used.

Because the ACR-700 incorporates unique features and design characteristics, the guidance provided by PRA guidance documents written for LWRs may not completely cover the safety basis for an ACR. For example, compared to LWRs the use of heavy water for a moderator makes tritium production a unique concern applicable to the CANDU and ACR NPPs. The passive decay heat removal systems on advanced reactors further complicate the transference of guidance from PRA guidance documents written for current-generation LWRs. Thus, to thoroughly evaluate the strengths and weaknesses of the ACR PSA methodology, the CANDU and ACR methodology and reference analysis documents need to provide more detailed information. The benefit of reviewing the documents is that they provide a good overview of the PRA methodology. This overview can then be used to identify (1) differences from LWR-specific techniques, (2) where LWR-specific technology may not be appropriate for heavy-water moderated and/or cooled NPPs, and (3) deficiencies in current methods being applied to advanced NPPs.

From the review performed, general observations about the relative strengths and weaknesses (when compared to NUREG/CR-2300 and ASME RA-S-2002) of the GC and ACR PSA methodology were documented in the various sections. Regarding the use of the ASME standard, this review did not incorporate NRC staff positions on implementation of that standard given in DG-1122.[100]

The peer review processes described in NEI 00-02, Appendix B of DG-1122, and Chap. 6 of the ASME standard were not used for this reviews of the ACR-700 methodology or analysis documents. A peer review based on the guidance given in these documents should be performed and documented by AECL.

The observations and/or questions concerning the AECL PSA information (methodology, assumptions, and results) are summarized in Sections 4.11, 5.10, 6.16, 7.3, and 8.3 of this report. The major observations from reviewing all six documents are provided below.

<u>Reporting Strengths</u>

- The GC PSA process appeared to be generally consistent with typical PRAs,
- the information provided is generally complete and easily understood, and
- the ACR PSA is more thorough than the GC PSA for what is provided.

Reporting Weaknesses

- There is a lack of sufficient details, supporting information, assumptions, or references in describing plant systems or methodology,
- although many sections provide sufficient detail on what is reported, at times information necessary to fully understand the methodology or analysis is not reported,
- errors or inconsistencies exist between tables and text, and
- some figures are too small to read.

The most significant reporting weakness is the use of proprietary documents as references. Although proprietary documents would be available to the NRC, they are not available to the general public.

Methodology Strengths

- PRA is used early in the design,
- occasionally, recent plant data is cited,
- PRAs are based on NUREG/CR-2300 but are updated with new methods when appropriate, and
- PRA uses 16-digit event identification nomenclature.

Methodology Weaknesses

- Calculational errors and inconsistencies questioned the calculation techniques, results, and sensitivity/uncertainty analyses,
- 20–30 year old data provides the basis for many failure probabilities,
- MAAP CANDU that has not been reviewed and accepted by NRC,
- the use of new standards or methods provides uncertainty in calculations and models,
- some probabilities are based on judgments,
- not all components or systems appear to be considered,
- not all assumptions appear to be appropriate,
- the numerous weaknesses in the fire methodology, taken together, represent an important weakness, and
- the ACR PSA is an ASME RA-S-2002 Category I PRA; in practice, however, the ASME category varies over different elements of the PRA and is not a global category assignment.

If AECL updates its UPM values with NUREG information, they would need to justify the use of this data. Regardless, AECL should fully document the implementation of the UPM in its PSA.

The peer review process described in NEI 00-02, Appendix B of DG-1122, and Chap. 6 of the ASME standard was not used for the review of the ACR-700 methodology or analysis documents. The peer review should be performed and documented by AECL.

In summary, the PRA methodology is in general conformance with the guidance in the PRA standards although there are a number of important short comings. These short comings, if not properly attended to, could have a significant adverse impact on the results and their credibility.

10. REFERENCES

1. U.S. Nuclear Regulatory Commission, "Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement," *Federal Register*, Vol. 60, p. 42622 (60 FR 42622), August 16, 1995.
2. K. N. Fleming, *Issues and Recommendations for Advancement of PRA Technology in Risk-Informed Decision Making*, NUREG/CR-6813, U.S. Nuclear Regulatory Commission, Washington, D.C., April 2003.
3. American Nuclear Society and The Institute of Electrical and Electronic Engineers, *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*, NUREG/CR-2300, Vols. 1 and 2, U.S. Nuclear Regulatory Commission, Washington, D.C., January 1983.
4. S. A. Bernsen, *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications*, ASME RA-S-2002, American Society of Mechanical Engineers, April 5, 2002.
5. Letter from P. Hessel to G. Rzentkowski,"Response to the U.S.-NRC Staff Request for Information on OPG PRAs," February 26, 2003.
6. P. Santamaura, A. Nainer, et al, *Generic CANDU Probabilistic Safety Assessment–Methodology*, AECL Analysis Report, 91-03660-AR-001, Rev. 0, Atomic Energy of Canada, Ltd., Ontario, Canada, July 3, 2002.
7. P. Santamaura, A. Nainer, et al, *Generic CANDU Probabilistic Safety Assessment - Reference Analysis*, AECL Analysis Report, 91-03660-AR-002, Rev. 0, Atomic Energy of Canada, Ltd., Ontario, Canada, July 5, 2002.
8. U. Menon, *Probabilistic Safety Assessment Methodology, ACR*, AECL Analysis Basis Document, 108-03660-AB-001, Rev. 1, Atomic Energy of Canada, Ltd., Ontario, Canada, July 23, 2003.
9. W. M. Raina, *Design Assist Role of ACR Probabilistic Safety Assessment (PSA)*, Assessment Document, 108-03660-ASD-008, Rev. 0, Atomic Energy of Canada, Ltd., Ontario, Canada, February 2004.
10. H. Shapiro and C. Blahnik, *Preliminary Design Assist PSA Level 1–Selected Full Power Event Trees*, ACR - 700 AECL Analysis Report, 10810-03660-AR-001, Rev. 1, Atomic Energy of Canada, Ltd., Ontario, Canada, January 28, 2004.
11. *Risk-Spectrum PSA Professional*, Ver. 1.1, RELCON AB, Sundbyberg, Sweden, 1998.
12. U.S. Nuclear Regulatory Commission, *Systems Analysis Program for Hands-on Integrated Reliability Evaluation*, SAPHIRE for Windows, Ver. 7.x, Washington, D.C., 2004.
13. CNSC, *Requirements for the Safety Analysis of CANDU Nuclear Power Plants*, CNSC Consultative Document, C-6, Rev. 0, 1980.
14. V.G. Snell, *Probabilistic Safety Assessment Goals in Canada.* Presented to the IAEA Technical Committee on Prospects for the Development of Probabilistic Safety Criteria, January 27 –31, 1987, Vienna, Austria. Also AECL Report, AECL-8761, 1987.
15. IAEA, *Basic Safety Principles for Nuclear Power Plants*. IAEA Safety Series Document, 75-INSAG 3, 1988.
16. CNSC, *The Use of Fault Trees in Licensing Submissions*, CNSC Consultative Document, C-70, 1983.
17. Vesely et al., *Fault Tree Handbook*, NUREG-0492, U.S. Nuclear Regulatory Commission, 1981.
18. IEEE Standard 500, *Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, Mechanical Equipment Reliability Data for Nuclear Power Generating Stations*, 1984.

19. SRI, *Nuclear Plant Reliability Data System 1982 Annual Reports of Cumulative System and Component Reliability*, Southwest Research Institute, San Antonio, Texas, 1983. Proprietary.
20. *Safety Analysis of CANDU Nuclear Power Plants*, Draft Regulatory Guide, C-006, Rev. 1 (E), Atomic Energy Control Board, Ottawa, Ontario, Canada, September 1999.
21. CNSC, *Requirements for Reliability Analysis of Safety-Related Systems in Nuclear Reactors*, CNSC Consultative Document, C-98, Rev. 0, 1987.
22. Data Systems & Solutions, *ETA-II Users. Manual for Version 2.1d*, Los Altos, California, 1993. Proprietary.
23. Data Systems & Solutions, *CAFTA User's Manual for Version 2.3*, Los Altos, California, 1993. Proprietary.
24. Data Systems & Solutions, *SAIPLOT User's Manual for Version 2*, Los Altos, California, 1990. Proprietary.
25. Data Systems & Solutions, *Accident Sequence Quantification Using PRAQUANT*, Los Altos, California, 1993. Proprietary.
26. Data Systems & Solutions, *UNCERT User's Manual Version 2.0*, Los Altos, California, 1992. Proprietary.
27. D.A. Meneley, C. Blahnik, J. T. Rogers, V.G. Snell, and S. Nijhawan, *Coolability of Severely Degraded CANDU Cores*, AECL Report, AECL-11110, Atomic Energy of Canada, Ltd., Ontario, Canada, 1995.
28. U.S. Nuclear Regulatory Commission, *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*, NUREG/CR-4780, Washington, D.C., 1989.
29. U.S. Nuclear Regulatory Commission, *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*, NUREG/CR-5485, Washington, D.C., Nov. 1998.
30. U.S. Nuclear Regulatory Commission, *Common Cause Fault Rates for Pumps: Estimates Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants, January 1,1972 through September 30, 1980*, NUREG/CR-2098, Washington, D.C., 1983.
31. U.S. Nuclear Regulatory Commission, *Common Cause Fault Rates for Valves: Estimated Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants, 1976-1980*, NUREG/CR-2770, Washington, D.C., 1983.
32. U.S. Nuclear Regulatory Commission, *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, Washington, D.C., 1983.
33. U.S. Nuclear Regulatory Commission, *A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants*, NUREG-0666, Washington, D.C., 1981.
34. R. Emrit et al., "Actions to Reduce Common Cause Failures," New Generic Issue No. 145, *A Prioritization of Generic Safety Issues*, NUREG-0933, Washington, D.C., Oct. 2003.
35. J. W. Rowe, "Availability of Common-Cause Failure Database," NRC Administrative Letter 98-04, U.S. Nuclear Regulatory Commission, Washington, D.C., July 30, 1998.
36. U.S. Nuclear Regulatory Commission, Vol. 1, *Common-Cause Failure Database and Analysis System: Overview*; Vol. 2, *Common-Cause Failure Database and Analysis System: Event Definition and Classification*; Vol. 3, *Common-Cause Database and Analysis System: Data Collection and Event Coding*; Vol. 4, *Common-Cause Failure Database and Analysis System: Software Reference Manual*, NUREG/CR-6268, Washington, D.C., June 1998.
37. U.S. Nuclear Regulatory Commission, *Common-Cause Failure Parameter Estimations*, NUREG/CR-5497, Washington, D.C., January 1989.

38. AEA Technology PLC. (Nuclear Division under Serco Assurance), *UPM 3.1: A Pragmatic Approach to Dependent Failures Assessment for Standard Systems*, SRD Association Report, SRDA-R13, AEA Technology PLC, Cheshire, UK, 1996. Proprietary.
39. W. D. Travers, Executive Director for Operations, U.S. Nuclear Regulatory Commission, to NRC Office of the Commission, "NRC's Advanced Reactor Research Program," SECY-03-0059, April 18, 2003.
40. A. D. Swain and H. E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, Draft, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, D.C., 1980.
41. A.D. Swain, *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*, NUREG/CR-4772, SAND86-1996, U.S. Nuclear Regulatory Commission, Washington, D.C., February 1987.
42. U.S. Nuclear Regulatory Commission, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (Final Report)*, NUREG/CR-1278, Washington, D.C., 1983.
43. D. M. Ericson, Jr., T. A. Wheeler, et al, *Analysis of Core Damage Frequency: Internal Events Methodology*, NUREG/CR-4550, SAND86-2084, Vol. 1, Rev. 1, U. S. Nuclear Regulatory Commission, Washington, D. C., January 1990.
44. M. K. Comer et al., *Generating Human Reliability Estimates Using Expert Judgement*, NUREG/CR-3688, U.S. Nuclear Regulatory Commission, Washington, D.C., 1984.
45. J. T. Chen, N. C. Chokshi, et al., *Procedural and Submittal Guidance for Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities*, NUREG-1407, U.S. Nuclear Regulatory Commission, Washington, D.C., 1991.
46. *Severe Accident Risks: An Assessment for Five U. S. Nuclear Power Plants, Final Summary Report*, NUREG-1150, U. S. Nuclear Regulatory Commission, Washington, D. C. December 1990.
47. R. Bari et al., *Probabilistic Safety Analysis Procedures Guide*, NUREG/CR-2815, Department of Nuclear Energy, Brookhaven National Laboratory Report, U.S. NRC, 1994.
48. R. J. Budnitz, G. Apostolakis, et al., *Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts*, NUREG/CR-6372, U.S. Nuclear Regulatory Commission, Washington, D.C., 1997.
49. L. E. Cover et al., *Handbook of Nuclear Power Plant Seismic Fragilities*, NUREG/CR-3558, U.S. Nuclear Regulatory Commission, Washington, D.C., 1985.
50. Canadian Standards Association, *Ground Motion Determination for Seismic Qualification of CANDU Nuclear Power Plants*, CAN3-N289.2-M81, R92, Rexdale, ON, 1992.
51. J. N. Ridgely, NRC, personal correspondence to R. J. Ellis, ORNL, "Additional comments on AECL 91-03660-AR-001, Revision 0," November 7, 2003.
52. IAEA, *Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants, Level 1*, IAEA Report, Safety Series No. 50-P-4, 1992.
53. U.S. Nuclear Regulatory Commission, "Determining Technical Adequacy of PRA Results for Risk Informed Activities," *Standard Review Plan*, NUREG-0800, Chap. 19, Washington, D.C., 2002.
54. R. W. Hackenbury and M. L. Yater, *Development and Testing of a Model for Fire Potential in Nuclear Power Plants*, NUREG/CR-1819, U.S. Nuclear Regulatory Commission, Washington, D.C., 1980.
55. K. N. Flemming, W. J. Houghton, and F. P. Scaletta, *A Methodology for Risk Assessment of Major Fires and Its Application to an HTGR Plant*, GA-A15401, General Atomics, Co., San Diego, California, 1979.

56. R. W. Hockenbury et al., "Occurrence Rates of Fire in Nuclear Power Plants," *Nuc. Eng. and Design*, 1981.
57. 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.
58. A. Tewarson et al., *Categorization of Cable Flammability Part 1: Laboratory Evaluation of Cable Flammability Parameters*, EPRI NP-1200, NUREG/CR-4840, October 1979.
59. S. P. Nowlen and V. Nicolette, "A Critical Look at Nuclear Qualified Electrical Cable Insulation Ignition and Damage Threshold," SAND88-2161C, *Conference Proceedings of the Operability on Nuclear Systems in Normal and Adverse Environment, September 1989.*
60. J. N. Ridgely, NRC, personal correspondence to R. J. Ellis, ORNL, "AECL―Fire Event PRA," August 1, 2003.
61. The Institute of Electrical and Electronic Engineers, Ins., "IEEE Standard for Type Test of Class IE Electric Cables, Field Splices, and Connections for Nuclear Power Generating Systems," IEEE Std. 383-1974, April 30, 1975.
62. U.S. Nuclear Regulatory Commission, *A Summary of the U.S. NRC Fire Protection Research Program at Sandia National Laboratories: 1975-1987*, NUREG/CR-5384, Washington, D.C., December 1989.
63. J. N. Ridgely, NRC, personal correspondence to R. J. Ellis, ORNL, "AECL―Flood Event PSA," August 5, 2003.
64. WASH-1400, *Reactor Safety Study . An Assessment of Accident Risks in US Commercial Nuclear Power Plants*, NUREG-75/014, U.S. Nuclear Regulatory Commission, Washington, D.C., 1975.
65. W. H. Hubble and C.F. Miller, *Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants*, NUREG/CR-1363, Vols. 1–3, U.S. Nuclear Regulatory Commission, Washington, D.C., 1980.
66. Baltimore Gas and Electric, *Calvert Cliffs Nuclear Power Plants Probabilistic Risk Assessment Individual Plant Examination, Summary Report*, 1993.
67. IAEA, *Component Reliability Data for Use in Probabilistic Safety Assessment*, IAEA Report, IAEA-TECDOC-478, 1988.
68. Electric Power Research Institute, *MAAP4―Modular Accident Analysis Program, Ver. 4.0.5*, May 2003.
69. Fauske and Associates, Inc., *MAAP4-CANDU―Modular Accident Analysis Program for CANDU Power Plant*, Vol. 1-3, April 1998.
70. J. N. Ridgely, NRC, personal correspondence to R. J. Ellis, ORNL, "AECL Methodology Report Sections 10 and 11," August 6, 2003.
71. EQE International, Inc., 1995, *EQESRA Users' Manual, Version 3.00*, EQE International, Inc., San Francisco, CA. Proprietary.
72. ABSG Consulting, Inc., *Fire Database*, PLG Proprietary Database, 1998.
73. CANDU Owner's Group, *COG OPEX Database*, 1998. Proprietary.
74. *Fire Dynamics Tools (FDTs) Quantitative Fire Hazard Analysis Methods for the U.S. Nuclear Regulatory Commission Fire Protection Inspection Program*, NUREG-1805, Draft, U.S. Nuclear Regulatory Commission, Washington, D.C., June 2003.
75. J. G. MacGregor, D. W. Murray, and S. H. Simmonds, *Behaviour of Prestressed Concrete Containment Structures: A Summary of Findings*, Atomic Energy Control Board Report, INFO-0031, May 1980.

76. H. Mochizuki, M. H. Koike, and T. Sakai, "Core Coolability of an ATR by Heavy Water Moderator in Situations Beyond Design Basis Accidents," *Nuc. Eng. and Design*, Vol. 144 (1993).
77. *Technical Basis for Estimating Fission Product Behavior During LWR Accidents*, NUREG-0772, U.S. Nuclear Regulatory Commission, Washington, D.C., June 1981.
78. M. Silberberg et al., *Reassessment of the Technical Bases for Estimating Source Terms*, NUREG-0956, Draft, U.S. Nuclear Regulatory Commission, Washington, D.C., July 1985.
79. AECL, *Licensing Basis for ACR*, Licensing Basis Document 108-00580-LBD-001, Rev. 0, Atomic Energy of Canada, Ltd., Ontario, Canada, July 2002.
80. K. Sapple, E. Y. H. Choy, et al, *ACR-700 Technical Description*, 10810-01371-TED-001, Rev. 0, Atomic Energy of Canada Limited, Ontario, Canada, June 27, 2003.
81. Atomic Energy of Canada, Ltd., *ACR Safety Design Guide—Safety Related System*, 108-03650-SDG-001, Rev. 2, Atomic Energy of Canada, Ltd., Ontario, Canada, January 2003.
82. Atomic Energy of Canada, Ltd., *ACR Safety Design Guide—Seismic Requirement*, 108-03650-SDG-002, Rev. 2, Atomic Energy of Canada, Ltd., Ontario, Canada, January 2003.
83. Atomic Energy of Canada, Ltd., *ACR Safety Design Guide—Environmental Qualification*, 108-03650-SDG-003, Rev. 2, Atomic Energy of Canada, Ltd., Ontario, Canada, January 2003.
84. Atomic Energy of Canada, Ltd., *ACR Safety Design Guide—Separation of Systems and Components*, 108-03650-SDG-004, Rev. 2, Atomic Energy of Canada, Ltd., Ontario, Canada, January 2003.
85. Atomic Energy of Canada, Ltd., *ACR Safety Design Guide—Fire Protection*, 108-03650-SDG-005, Rev. 2, Atomic Energy of Canada, Ltd., Ontario, Canada, January 2003.
86. Atomic Energy of Canada, Ltd., *ACR Safety Design Guide—Containment*, 108-03650-SDG-006, Rev. 2, Atomic Energy of Canada, Ltd., Ontario, Canada, January 2003.
87. Atomic Energy of Canada, Ltd., *Analysis Basis—Trip Coverage Methodology*, 10810-03550-AB-001, Rev. 0, Atomic Energy of Canada, Ltd., Ontario, Canada, December 2002.
88. Atomic Energy of Canada, Ltd., Change Control Procedure 00-681.1 , Atomic Energy of Canada, Ltd., Ontario, Canada.
89. IAEA, *Probabilistic Safety Assessment for Seismic Events*, IAEA Report, IAEA-TECDOC-724, Vienna, Austria, 1993.
90. U.S. Nuclear Regulatory Commission, *U.S. NRC Policy Issue,* SECY-93-087, April 1993.
91. U.S. Nuclear Regulatory Commission, *Recommendations to the Nuclear Regulatory Commission on Trial Guidelines for Seismic Margins Reviews of Nuclear Power Plants*, NUREG/CR-4482, Washington, D.C., March 1986.
92. Canadian Standards Association, *General Requirements for Seismic Qualification of CANDU Nuclear Power Plants*, CAN3-N289.1-M80, R92, Rexdale, ON, 1992.
93. Canadian Standards Association, *Design Procedures for Seismic Qualification of CANDU Nuclear Power Plants*, CAN3-N289.3-M81, R92, Rexdale, ON, 1992.
94. R. D. Campbell et al., *Compilation of Fragility Information from Available Probabilistic Risk Assessments*, LLNL Report, UCID-20571, Rev. 1, 1988.
95. Electric Power Research Institute, *A Methodology for Assessment of Nuclear Power Plant Seismic Margin*, EPRI NP-6041-M, Rev. 1, 1991. Proprietary.
96. Atomic Energy of Canada, Ltd., *Design Earthquakes*, 108-10170-DG-001, Rev. 0, Atomic Energy of Canada, Ltd., Ontario, Canada, December 2002.
97. G. How Pak Hing and A. Stretch, "Development of Probabilistic Safety Assessment Methodology for Fire Events in CANDU Plants," *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 1, 1999.

98. Electric Power Research Institute, *A Probabilistic Risk Assessment for Oconee Unit 3*, NSAC-60, EPRI, Palo Alto, California, 1984.
99. Atomic Energy of Canada, Ltd., *ACR Design Verification—Verification Plan*, 108-01920-DVP-001, Atomic Energy of Canada, Ltd., Ontario, Canada.
100. U.S. Nuclear Regulatory Commission, *An Approach for Determining the Technical Adequacy of PRA Results in Risk Informed Activities*, DG-1122, Washington, D.C., September 2002.
101. V. P. Brand, *The Unified Partial Method: Pragmatism and Expert Assistance in Dependent Failure Analysis*, European Safety and Reliability Conference, ESREL 95, Bournemouth, UK, June 1995.
102. P. Ilescu, *Systematic Review of Plant Design for Identification of Initiating Events*, ACR–AECL Assessment Document, 108-03660-ASD-001, Rev. 1, Atomic Energy of Canada, Ltd., Ontario, Canada, January 15, 2004.
103. Duke Power Company, *McGuire Nuclear Station IPE Submittal Report*, November 1991.
104. Duke Power Company, *Catawba Nuclear Sation Unit 1 Probabilistic Risk Assessment*, Sept. 1992.
105. J. W. Minarick et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab.; Science Applications International Corp.; and Professional Analysis, Inc., *Precursors to Potential Severe Core Damage Accidents: 1988, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232, Vols. 9 and 10), February 1990.
106. M. Stattison, et al, *Standard Plant Analysis Risk Model for Davis-Besse (ASP PWR D)*, Rev. 3i, Idaho National Environmental and Engineering Laboratory, Idaho Falls, ID, May 2000.
107. S. A. Eide, et al, *Reliability Study: Westinghouse Reactor Protection System, 1984–1995*, NUREG/CR-5500, Vol. 2, Idaho National Engineering and Environmental Laboratory, Idaho Falls, ID, April 1999.
108. *Vogtle Electric Generating Plant, Units 1 and 2, Individual Plant Examination Report in Response to Generic Letter 88-20*, Southern Nuclear Operating Company, Westinghouse Electric Corporation, Fauske and Associated, Inc., December 1992.
109. *Palo Verde Nuclear Generating Station Individual Plant Examination for Severe Accidents (Response to Generic Letter 88-20)*, Arizona Public Service Company, Phoenix, AZ, April 1992.
110. C. Xu, *Identification and Initial Assessment of US NRC Generic Safety Issues Applicable to ACR*, Assessment Document, 108US-01321-ASD-001, Rev. 0, Atomic Energy of Canada, Ltd., Ontario, Canada, April 2003.
111. S. Yu, AECL Technologies, "An Overview of the ACR Design," presented to U.S. Nuclear Regulatory Commission on September 25, 2002.
112. L. Bratu, *Initial Conditions and Standard Assumptions Safety Analysis Basis, ACR-700*, Analysis Basis, 10810-03510-AB-001, Rev. 0, Atomic Energy of Canada, Ltd., Ontario, Canada, Aug. 14, 2003.
113. U. S. Nuclear Regulatory Commission, "Independence Between Redundant Standby (Onsite) Power Sources and Between Their Distribution Systems," *Safety Guide 1.6*, August 10, 1971.
114. Philadelphia Electric Co., *Probabilistic Risk Assessment Limerick Generating Station*, Sept. 1982.