

**ENHANCEMENTS IN SAFETY RESULTING FROM  
PROBABILISTIC SAFETY ASSESSMENTS —  
A DESIGNER'S PERSPECTIVE**

**DONALD F. RENNICK**  
Business Development Manager,  
Power Plant Services

**VICTOR G. SNELL**  
Manager, Safety, CANDU-300

**PHILLIP GUMLEY**  
Risk Assessment Team, CANDU-300

and

**P.S. NARAYANAN**  
Risk Assessment Team, CANDU-300

Atomic Energy of Canada Limited  
CANDU Operations  
Mississauga, Ontario, Canada

Presented to  
American Nuclear Society  
Topical Meeting on Nuclear Power Plant Operations  
Chicago, Illinois  
September 1, 1987



## A. INTRODUCTION

This paper describes our perspective on the preparation and use of Probabilistic Safety Assessments (PSAs) in enhancing the safety and operability of the CANDU reactor system, particularly from the design viewpoint. We outline the history of their development and use, and describe our present usage for design of the CANDU-300 reactor, based on lessons learned from previous applications to other CANDU plants.

PSAs are a method of systematic review of the safety and operation of any complex process system or mechanism. Our emphasis centers on predicting the frequency of possible failures and analyzing the associated consequences so reliability and safety can be achieved in a cost-effective manner. While the focus of this paper is on design aspects, we also document how the PSA foundation is useful in defining and implementing operational strategies.

Like any major project, nuclear reactors are designed in modules by teams of engineering staff, frequently supplied by different organizations. Design requirements usually specify the interfaces between systems and make implicit assumptions on the availability of support systems. Even if these requirements and interfaces were perfect, one could not determine, a priori, all the demands on the integrated plant under abnormal conditions. The global picture is obtained only by a systematic review. Further, the most effective time in the lifetime of a reactor to initiate these systematic studies is at the conceptual stage, yielding a structured and organized reactor design.

In section B, we give a summary of the long history of risk and safety analysis at Atomic Energy of Canada Limited (AECL). In section C, we describe our ongoing PSA analysis program, and the methods used; section D summarizes the results of those studies. Section E discusses how AECL is applying the lessons learned during the design, construction, commissioning, and licensing phases of the existing CANDU reactors to the innovative CANDU-300 design process.

## B. HISTORY OF RISK ANALYSIS AT AECL

AECL, the designer of the CANDU reactor, pioneered reliability and risk assessments as an integral element of the CANDU design. Together with prudent operation, these have been major contributors to the high performance records consistently achieved by CANDU reactors. Typically, CANDUs occupy four or five of the top ten positions for capacity factor, for all reactors world-wide with electrical output greater than 500 MW(e).

In the early 1950s, the Canadian nuclear industry set design targets for safety such that the risk from nuclear generation accidents

was to be less than 1/50 of the risk from accidents in comparable manufacturing or other electrical generation industries. This was achieved by reducing the risk of a catastrophic failure to very low values. To prove these values were achievable, separate reliability targets were derived for the process systems which run the plant, and the safety systems which protect it. These targets had to be demonstrated by test during operation, and the two classes of systems had to be physically and functionally separate to reduce the chance of common failure modes. This approach has evolved (1) into the single/dual failure approach used in the safety design and licensing of CANDU power reactors. The result is a two-level system of radiological public dose limits -- a low dose for the failure of a single process system (the frequency must be shown to be less than one per three years) and a somewhat higher value for a "dual failure" consisting of the process failure plus the assumed unavailability of any one of the safety systems designed to mitigate the consequences of that process system failure (There is an overall inferred frequency target for this circumstance of less than one per 3000 years). Thus, loosely speaking, the regulatory dose limits are frequency-based.

The demonstration that the design meets these dose/frequency targets is the analysis found in the Safety Report. The approach is still evolving: within the last four years, the Canadian regulatory, in consultation with the nuclear industry, has introduced a number of approaches which place even more emphasis on doses related to frequency of failure (1).

The unavailability requirements for each of the dormant special safety systems ( $10^{-3}$  for shutdown, emergency core cooling, and containment) must be demonstrated during operation. If the system is normally dormant, the reliability must be shown by test. Fault trees for these mitigating systems provide the perfect vehicle for establishing the test interval. For active systems, such as process systems, the unsafe failure rate must likewise meet regulatory and economic targets. While this can be established from experience, to avoid expensive backfitting, fault trees are used to give some assurance that the reliability target is achievable in practice.

The single/dual failure approach did not explicitly treat support systems in a logical fashion. Thus in 1975, AECL initiated, as a design tool, probabilistic analysis of the service water systems of Ontario Hydro's Bruce A multi-unit nuclear generating station(2). The benefits from this study were:

- a) a comprehensive identification of crosslinks (service water has interfaces with many systems),
- b) identification of which support functions needed backup cooling water, and
- c) definition of the necessary operator actions to mitigate the consequences of a loss of service water.

After this, four more Bruce A support systems were studied: Instrument Air, Electrical Power Supplies, Maintenance Cooling (Residual Heat Removal), and Moderator and End Shield Cooling Systems.

### C. PROBABILISTIC SAFETY ASSESSMENT OF CANDU-600 REACTORS

Following the successful Bruce A studies, AECL and the CANDU utilities decided to undertake more comprehensive probabilistic studies, including Balance of Plant (BOP) systems, of the CANDU 600 MW stations and the multi-unit stations in Ontario (Table I).

TABLE I  
REACTORS STUDIED

Station	Utility
Gentilly Unit 2	Hydro Quebec
Point Lepreau Unit 1	New Brunswick Power
Wolsung Unit 1	Korea Electric Power Company
Pickering B	Ontario Hydro
Bruce B	Ontario Hydro

At the time, these were called Safety Design Matrix (SDM) studies; similar studies with refined methods are now called Probabilistic Safety Assessments. The differences between SDM's and PSA's are discussed in Reference 3. For simplicity, we will use SDM and PSA interchangeably.

This program produced 15 studies for each reactor, listed in Table II.

TABLE II  
SAFETY DESIGN MATRIX STUDIES FOR CANDU REACTORS

1. Failure of Station Electrical Power Supplies
2. Service Water System Failures
3. Instrument Air System Failures
4. Moderator and End Shield Cooling System Failures
5. Dual Computer Failures
6. Loss of Steam Generators as a Heat Sink
7. Reactor Building Flooding
8. Turbine and Service Building Flooding
9. Operation after an Earthquake
10. Inadvertent Addition of Positive Reactivity
11. Large Loss of Coolant and Emergency Core Cooling Operation
12. Small Loss of Coolant and Emergency Core Cooling Operation
13. Shutdown Cooling System Operation
14. Use of Moderator as an Emergency Heat Sink
15. Containment Operation

These studies went beyond the analysis of support systems. They covered all major initiating events, and were used to systematically identify and quantify scenarios which had the potential to release radioactivity from the plant at credible event frequencies. The overall benefits from the studies are independent of the specific reactor. We will focus on the lessons learned and their application to design and operation in the remainder of this paper.

The bases for choosing the 15 studies in Table II were as follows:

- a) Support systems such as electrical power, instrument air, and service water are common to many plant systems and can lead to complex interactions and plant-wide consequences.
- b) Failure of control, notably of the dual computers, had not been analyzed probabilistically.
- c) There had to be assurance of long term heat sinks for all credible scenarios.
- d) There had to be assurance that flooding from internal pipe breaks, both in the reactor building and in the service buildings, would not disable essential systems.
- e) Earthquakes had not been analyzed from a plant-wide viewpoint.

#### METHODS—TECHNICAL

AECL uses standard fault tree/event tree methods, and adds unique and powerful treatments of event sequences. A brief outline of the process AECL uses is given in Reference 3:

- 1) Initiating events are chosen based primarily on their potential for core damage or severe economic loss.
- 2) Fault trees for initiating events are prepared to determine the event frequency.
- 3) Descriptive event sequences are written to identify the consequences of the initiating event on other process systems; to evaluate the pattern of alarms in the main control room during the transient and recovery period; and to identify the mitigating systems required, and their mission times. In cases where additional analysis is required, design centre or best estimate assumptions are used.
- 4) Event trees are transcribed from the descriptive event sequences, and show the paths the plant can follow up to and including the establishment of a long-term heat sink.
- 5) Fault trees are prepared for the mitigating systems (dormant or active) to establish their reliability.
- 6) Surveys are done for crosslinks between the initiating event and the mitigating systems, and between the mitigating systems themselves.
- 7) Fault trees for the selected scenarios are merged and analyzed to determine the frequency of the scenario.
- 8) The final scenario frequency is judged against an acceptance criterion (see below). If the frequency or extent of core damage is unacceptable, then equipment or procedural changes are made.
- 9) Utility operations and engineering staff review all stages of the analysis and their comments are incorporated where appropriate.

- 10) Designers and/or operations staff prepare normal and abnormal operating procedures (which are also valuable for operator training).

Fault trees are used to model the failure logic of a system based on its components. The use of fault trees yields two important advantages over other methods used for nuclear plant failure assessments:

- a) It ensures that possible common-cause events between initiating events and mitigating systems are accounted for in the analysis of the scenario.
- b) It gives a more realistic and defensible estimate of the frequency of rare initiating events than trying to estimate them from statistically sparse historical data.

AECL is unique in its development of event sequences/event trees because a time line is added to highlight the chronology of events. This enables the analyst to confirm that the mitigating equipment is available and capable in the time window and to calculate what its mission time must be. Because alarms and operator actions are shown explicitly, the human role can be included realistically.

#### ACCEPTANCE CRITERION

Very rare events should not require design changes. Since the PSA<sub>7</sub> is a design/operational tool, events with a frequency less than  $10^{-7}$  events per year (once in ten million reactor-years) do not need further mitigation, and hence are not developed further. This is in line with international practice. For values between  $10^{-6}$  and  $10^{-7}$ , engineering judgement is used, depending on the situation and the possible severity of consequences. Thus, the acceptance criterion used by AECL is either that the plant would reach a stable operating state or an event frequency of less than  $10^{-7}$  ( $10^{-6}$  in a few cases involving judgement) has been reached.

#### OPERATOR MODEL

The operator model used by AECL takes credit for operator action as a function of the stress of the situation, the time from the first clear indication of the initiating event, and the clarity (unambiguity) of alarms available. The actual numbers used for this logically simple model are given in Reference 3.

By including operator actions in the event trees, and by retaining a time-line in them, the event trees are firmly tied to the actual phenomena of the incident, and hence the operator response can be evaluated in the context of alarms present, time-scale of required

actions, etc. --- all of which are also apparent from the tree (4). In practice, our post-event operator model gives similar numerical results to those of Swain and Guttman (5).

#### **METHODS—MANAGERIAL**

A criticism often leveled at fault tree methods is the dependence of the outcome on the particular analyst constructing the tree. This can be minimized by having personnel intimately familiar with process design prepare the trees. This is the strategy which AECL has used--a core of people expert in the rigorous mathematical aspects of reliability methods plus a larger group of process designers. Since AECL has a large staff of process designers who already have some familiarity through detailed reliability assessments of individual systems, this permits rapid expansion of the safety assessment team as needs arise.

#### **CHANGES AND CHANGE CONTROL**

There is a need to maintain safety while protecting against unnecessary changes. This is especially acute when plants are in the late stages of construction. To control this aspect, AECL set up a Board of senior engineers and managers to review all proposed changes to the plant. Participants represented Safety and Licensing, Engineering (design) and Project (economic interests). The mandate was to review all changes for generic application and to ensure that the safety objective would be attained in the most cost-effective manner. The decisions of this Board were then communicated to the owners/operators for their concurrence.

### **D. SUMMARY OF RESULTS/INSIGHTS**

#### **ROLE OF SUPPORT SYSTEMS**

The most important benefit of these studies was that they provided a systematic examination of the integrated plant. They showed that plant utility systems were responsible for a number of potential crosslink failures, which resulted in design changes as discussed below.

#### **DESIGN CHANGES**

The PSA studies described so far were done, mostly, while the stations were in the mid-to-late stages of design and construction.

Table IV reflects the number of design changes approved for each reactor.

**TABLE IV  
DESIGN CHANGES RESULTING FROM PSA STUDIES**

Station	Number of Design Changes
Gentilly Unit 2	92
Point Lepreau Unit 1	66
Wolsung Unit 1	37
Pickering B	22
Bruce B	17

The reactors are listed chronologically in order of their design, with Gentilly-2 being the lead plant. While the first three are of the generic CANDU-600 type with site-related differences, the latter two are multi-unit stations with significant differences in overall design. Note that as the design proceeded, the generic changes were automatically incorporated (fed forward) so no design change request was needed.

Many changes were as small as modifying the failure mode of valves or adding additional overpressure relief; others were as complex as adding a steam-driven auxiliary feed pump as a backup for loss of offsite power. Table V shows some typical equipment changes.

**TABLE V  
SOME OF THE MORE SIGNIFICANT DESIGN CHANGES**

CHANGE	REASON
1. Provision of Second Auxiliary Boiler Feed Pump or Auto-depressurization of Steam Generators	Long term heat sink
2. Dousing Tank Water Inventory Reduction	Reactor Building Flooding
3. Backup Cooling to Air Compressors	Crosslink between Service Water and Instrument Air
4. Auto Isolation of Hot Degasser Condenser	D <sub>2</sub> O Feed/Small Leak Protection
5. Valve Failure Mode Change	Instrument Air/Shutdown System #2 Crosslink
6. Emergency Water Supply to Steam Generators	Long Term Heat Sink
7. Valve Interlocks	Recirculating Service Water/ Emergency Water Crosslink

- |   |  |
|---|--|
| 8. Add Local Air Tanks  | Liquid Relief Valve/<br>Instrument Air Crosslink   |
| 9. Add Alarm on Loss of<br>Instrument Air (Loss of<br>High dp Indication and<br>Travelling Screen Trip) | Gain Credit for<br>Operator Action to<br>Increase Frequency of Screen<br>Wash to Prevent Carryover of<br>Debris to Service Water Systems |

#### INPUT TO ABNORMAL OPERATING PROCEDURES AND ACCIDENT DIAGNOSIS

A major benefit was the insight gained into the sequence of events which is **most likely** to occur after an accident or a process upset transient. In co-operation with utility operating staff, AECL prepared Operational Documents (OPDOCS) for all the support systems (air, water, power, etc.) to guide the operators in the event of a failure. For instance, OPDOCS can indicate the most probable cause of a particular set of alarms.

In one case, the PSA analysts discovered that an emergency support system would be completely disabled by an incorrect sequence of valve opening. This resulted in item 7 of Table V. In another case, routine surveillance of expansion joints in large service water pipes was initiated at Point Lepreau when the PSAs showed the consequences of failure and contribution to system unavailability of such pipes were unacceptable.

New Brunswick Electric Power Corporation (NBEPCC), the owner of the CANDU-600 at Point Lepreau, used the SDMs to do a review of all operator actions from a utility perspective (6), including such factors as:

- \* how much action time do they realistically have?
- \* can they do the required actions in that time?
- \* do they have the necessary information in understandable form to make the correct decisions?

#### MAINTENANCE PLANNING

The PSA studies have been used to establish procedures for maintenance outages. For example, during maintenance of the steam generators, the shutdown cooling (residual heat removal) system is the heat sink. This system relies on electrical power. It was determined from the electrical power supply fault trees that a major contributor to unavailability of electric power supply to the shutdown cooling system was the failure of the standby diesel generator(s) to start following a loss of offsite power. Thus the utility decided a prudent measure would be to run the diesel generators continuously while repairing the steam generators.

## REGULATORY USAGE

The SDMs were undertaken at AECL initiative with the primary aim of increasing production effectiveness and safety. However, they have proven so useful in their secondary purpose of making regulatory submissions that they have become de facto Licensing Support Documents. While there is still no formal acceptance criterion for them by the Canadian regulatory agency, it is doubtful that any reactor could be licensed in Canada without a probabilistic study of the generic design.

## E. CANDU-300 DESIGN PROCESS AND PSA

As noted in the preceding sections, AECL has used probabilistic safety assessment as a design tool as well as for licensing. AECL is using a logical extension of these techniques in the design of the CANDU-300, a new-generation CANDU aimed at the emerging market for smaller size nuclear units, and designed from the beginning to be competitive with coal. In order to achieve low capital costs, the design and construction schedule has been dramatically shortened compared to previous Canadian experience --- from Construction Start to In-Service will be less than 42 months. To achieve this schedule, innovative approaches are being taken in the way we perform the design processes.

A large contributor to schedule delays in the past, all over the world, has been late changes to the design arising either from the detailed design process, or, as we have discussed, from safety analysis and probabilistic safety assessment late in the design and construction process. These delays have been driven either by the designer or in response to evolving interpretations of regulatory requirements. Two of the innovations to reduce the risk of such delays are:

- 1) up-front licensing, in which the safety design groundrules, scope of safety work, detailed acceptance criteria, and key aspects of the design are agreed in detail with the regulatory body (the Canadian Atomic Energy Control Board, or AECB) before the detailed design work begins. This process is described more completely in References 7,8.
- 2) up-front safety analysis and probabilistic safety assessment, which evolve along with, and influence, both the conceptual and the detailed design, as well as providing a vehicle for keeping the AECB informed and therefore early highlighting of any potential concerns.

The probabilistic safety assessment programme has four logical phases:

- PHASE 1: Reliability Targets Programme,
- PHASE 2: Event sequence/event tree analysis with preliminary supporting fault trees,
- PHASE 3: Probabilistic Safety Assessment, and
- PHASE 4: Review of dominant accident sequences to include operator errors of commission and any late changes in design.

Phase 1, currently underway, is a fast review of those areas which are expected, based on past experience, to have the most potential for design changes. The eight reviews are:

- 1) electrical power failures,
- 2) loss of coolant,
- 3) service water system failures,
- 4) moderator/shield cooling failures,
- 5) instrument air failures,
- 6) distributed computer control and multiplexer failures,
- 7) feedwater/condensate system failures, and
- 8) fuelling machine failures (The CANDU reactor is refuelled on-line and while generating full power.)

The studies identify, for each initiating event, all the mitigating systems required to achieve a post-accident stable plant state. The event sequences are converted to event trees and conservative target system unreliabilities are assigned based on a reasonable apportionment. Known dependencies (such as on safety support systems like air and cooling water) are allowed for, but at this stage only block-type fault trees are prepared.

The power of this approach is that major deficiencies can be identified very early in the conceptual design, when changes are less expensive and moreover when they can be integrated in a holistic manner into the design as opposed to being add-ons constrained by a frozen design. It is also very cost-effective --- each review takes between two and four weeks, and probably captures 80% of the required changes. Finally, if needed, the results can be used in the early stages of licensing to inform the regulatory of the safety characteristics of the design and to obtain their comments on potential issues.

Figure 1 shows an example of an event tree for loss of electrical power. An analysis was done to predict the failure rate of the two Group 2 standby diesel generators as a function of the duration of the power outage. Where outage durations exceeded the mean repair times, the effect of repair was included using a Markov state analysis. It can be seen that several events lead to fuel damage above the target frequency we have chosen of  $10^{-6}$  events/year. As a result, a small local diesel has been proposed (instead of an electric motor) to drive a Group 2 feedwater pump, and local diesel generators will be added to charge the emergency batteries independent of the standby diesel-generators. Finally the reliability of heat transport system bottle-up following a loss of power has been increased to reduce the consequential small Loss Of Coolant Accident (LOCA) frequency. These changes were made with insignificant penalty to the cost or schedule, and therefore were approved quickly.

Phase 2 - sufficiently complete event sequence/event tree analysis --- will begin at the early stages after project commitment, when most of the nuclear steam plant process design will be available, although control and instrumentation and balance of plant details may not be complete. Detailed event sequence/event tree

diagrams will be prepared and supporting consequence analysis identified and performed. Preliminary supporting fault trees will be constructed to a sufficient level of component detail. The event sequences include a detailed expansion of the eight described in Phase 1, plus:

- 9) Very small loss-of-coolant,
- 10) Flooding in the reactor building,
- 11) Flooding in other buildings,
- 12) Fuel handling system failures, and
- 13) Failures during reactor shutdown.

Phase 3 is the main probabilistic safety assessment which merges the fault trees (now with more detail as the design firms up) and the event trees in a systematic identification of crosslinks. Because we will be using fully computerized fault-tree/event-tree construction and calculation, the trees from the earlier phases can simply be extended rather than being re-analysed, a necessary saving in cost. The Phase 3 studies include a review of the most dominant event sequences and an analysis of control components. The studies are scheduled to be available if required to support an application for an operating licence.

Phase 4 incorporates more realistic details of the operator response into the most dominant sequences. It is scheduled between the application for an operating licence and six months before first criticality, so that it will be able to include information from commissioning activities and preliminary operating procedures. Any late changes in control logic which influence the PSAs can also be examined in this phase.

## F. DISCUSSION

The above program gets the most "effect for the dollar" in the design of a new plant. It is cheap, very effective at identifying plant weaknesses and in forcing real issues to be addressed, and can be used either as a screening model or as a basis for a regulatory submission. The phased series of studies placed as early as possible in the design cycle, ensure that:

- reliability targets (from a safety point of view) can be agreed with designers during the conceptual design phase, so they can affect the choice of equipment and the system design itself,
- any changes can be identified early enough to avoid cost/schedule penalties,
- the regulatory is kept familiar with the design as it develops,
- the later phases give regulatory, designer, and customer assurance that the details are correct, and provide a basis for examining the effect of key as-built changes.

Technically the operator model is simple enough to be applied by non-experts in human factors, yet stands up well in comparison with established models of human behaviour.

Retention of the time-scale in event sequences forces a realistic view of plant behaviour and interaction with the operator. The PSA studies are used effectively in operations in developing advanced training manuals for licensed operators and shift supervisors, and in simulator training where possible. The fault trees identify sensitive areas which may lead to a modification of operating practice or initiate a design change.

Faults during operation at other than normal full power conditions and partial failure modes are routinely examined, and ensure that the more likely accidents are catered for.

In short, the PSA techniques provide a cost-effective understanding of a plant that can lead to real improvements in safety and economics, and provide a framework for evaluating design options.

#### G. REFERENCES

1. Snell, V.G., "Probabilistic Safety Assessment Goals in Canada", Presented to the IAEA Technical Committee on Prospects for the Development of Probabilistic Safety Criteria, Vienna, January 1986. (Also Atomic Energy of Canada Limited Publication AECL-8761.)
2. Gumley, P., "Use of Fault Tree/Event Sequence Analysis in a Safety Review of CANDU Plants", International Atomic Energy Agency Publication IAEA-CN-39/7, Vienna 1981. (Also Atomic Energy of Canada Limited Publication AECL-7373.)
3. Rennick, D.F., and Snell, V.G., Enhancements in Safety Resulting From Probabilistic Safety Assessments, Proceedings of the American Power Conference, Chicago, April 1987.
4. Gumley, P., Narayanan, P.S. and Smith, J.E., "CANDU Alarm Sequence Analysis Following Abnormal Conditions", International Atomic Energy Agency Specialist Meeting on Systems and Methods for Aiding Nuclear Power Plant Operators During Normal and Abnormal Conditions, Hungary, October 1983.
5. Swain, A.D. and Guttman, H.E. "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications", United States Nuclear Regulatory Commission publication NUREG/CR-1278, August 1983.
6. Alikhan, S., "Probabilistic Safety Assessment --- Role in Operations", International Atomic Energy Agency/Argonne National Laboratory Course in Probabilistic Safety Analysis Methods in Nuclear Power Plant Operation, Toronto, March, 1986.
7. Natalizio, A., (AECL) "Up-front Licensing --- A New Approach", Canadian Nuclear Association Annual Meeting, June 1985.

8. Marchildon, P., (AECEB) "Recent Developments in Canadian Nuclear Power Plant Licensing Practices", Canadian Nuclear Association Annual Meeting, June 1985.

#### H. ACKNOWLEDGEMENTS

The work described in this paper was done by analysts in the Risk Assessment and Safety Design Branch, some of which was under contract to, and in association with, the CANDU utilities: Ontario Hydro, New Brunswick Electric Power Commission, Hydro Quebec, and the Korea Electric Power Company.





