PROBABILISTIC SAFETY ASSESSMENT OF SUPPORT SYSTEMS FOR CANDU STATIONS

NUCLEAR REACTOR SAFETY

KEYWORDS: *CANDU, support systems, probabilistic safety analysis*

HYMIE S. SHAPIRO *Atomic Energy of Canada Limited*
CANDU Operations, Sheridan Park Research Community
2251 Speakman Drive, Mississauga, Ontario, Canada L5K 1B2

Received August 23, 1990
Accepted for Publication January 18, 1991

Atomic Energy of Canada Limited (AECL) has performed probabilistic safety assessments (PSAs) of Canada deuterium uranium (CANDU) reactor support systems since 1975. AECL's experience in the use of PSAs on support systems and the application of the PSA for the CANDU 3 are described. The PSA work reviews support system failures such as loss of service water and loss of instrument air as initiating events during full power and during plant shutdown conditions. The design changes resulting from this work, with respect to prevention of loss-of-coolant accidents and maintaining a long-term heat sink, are described.

The use of PSAs is being initiated early in the design of the next-generation CANDU reactor (CANDU 3) to avoid the possibility of design changes and backfits during the construction phase of the project.

I. INTRODUCTION

Atomic Energy of Canada Limited (AECL) has performed safety and reliability assessments, otherwise known as probabilistic safety assessments (PSAs), of Canada deuterium uranium (CANDU) reactor support systems since 1975. This paper briefly describes AECL's experience in the use of PSAs on support systems and the application of PSA for the CANDU 3.

II. HISTORY

Risk and reliability assessments have been a cornerstone of CANDU nuclear power plant design since the late 1950s due, in part, to experience with the NRX research reactor accident in 1952 [failure of a normal process system together with partial failure of the shutdown (protective) system]. The accident spurred recognition of the importance of a more *rational* approach to public safety, and in turn, reliability targets for key systems.

The design of the first nuclear power reactors, and every one since 1952 in Canada, incorporated the philosophy of separating the process and safety systems and adding a reliability target for each. Achievement of the specific reliability targets was later verified by in-service testing. AECL was a pioneer in applying risk analysis as a way of analyzing both rare and common upset events in reactor design in a consistent manner.

More sophisticated reliability methods were applied to current CANDUs during the 1970s to confirm the goals of reliability and separation between process and safety systems. The accident sequences were extended to systems not included in the earlier reliability studies. The first such study performed by AECL was on the service water system at the Bruce A generating station in 1975. The benefits from this study were

1. a comprehensive identification of cross links since service water interfaces with many systems
2. identification of support functions needing backup cooling
3. definition of necessary operator actions to mitigate the consequences of a loss of service water.

Later, four more initiating events at the Bruce A station were studied: loss of instrument air, loss of electrical power, loss of maintenance cooling, and loss of moderator and end shield cooling.

The Bruce A station safety assessments were so useful to both designers and engineers that 15 PSA studies were proposed for the next plants being built in Canada. The various station designs had defined main system elements, but the detailed design, including control and instrumentation, was not finalized. These plants were all at different stages of construction.

The Canadian regulatory agency also recognized

the usefulness of the Bruce A station studies, and the 15 PSA studies were made a regulatory requirement for these stations:

1. Gentilly Unit 2 (Hydro Quebec)
2. Point Lepreau Unit 1 (New Brunswick Electric Power)
3. Wolsung Unit 1 (Korea Electric Power Corporation)
4. Pickering B station (Ontario Hydro)
5. Bruce B station (Ontario Hydro)
6. Darlington A station (Ontario Hydro).

These PSA studies were performed from 1978 to 1983 and went beyond the assessment of support systems; they were used to systematically identify and quantify all major scenarios that could release radiation from the plant at credible event frequencies. More information on these PSAs can be found in Refs. 1 through 4. Also, between 1982 and 1987, Ontario Hydro completed a level 3 PSA for Darlington A station. This PSA was used to support an application from the Canadian regulatory body for an operating license.

All of this PSA work reviewed support system failures such as loss of electrical power, loss of service water, and loss of instrument air as initiating events during full-power operation and during plant shutdown conditions.

The key results from this work were the following:

1. For losses of service water and instrument air, the failure frequency was dominated by passive component failures. Expansion joints and piping contributed to the passive failure contribution for a loss of service water: The expansion joints contributed ~80% of the loss of service water frequency according to failure data obtained from actual experience at CANDU nuclear power plants. Active failures in the service water system were not a driving force in the analysis because of the high level of redundancy. Piping failure or leakages from pressure boundary components contributed to passive failure for a loss of instrument air. At AECL, fault trees are prepared to predict initiating event frequencies for the above events. Predictions are confirmed using operating CANDU experience.

2. The plant response dictated the need for design changes to meet the probabilistic acceptance criteria used for licensing at that time. To make design decisions, AECL uses mean probability values. For the Point Lepreau plant, 80% of the design changes due to PSA were in the nonnuclear (conventional) part of the plant.

II.A. Service Water

The design changes arising from the PSA work on service water (including raw service water and recirculated cooling water) on CANDU 6 units fall into the following categories:

1. Prevention of loss-of-coolant accident (LOCA): The changes involved protection of the heat transport reactor coolant pump seals by automatically isolating the hot heavy water (D_2O) injection to the seals. This would continue operation of the pumps to cool down the heat transport system.

2. Maintaining a long-term heat sink (i.e., continuous feedwater supply to the steam generators) until service water is restored: The design changes involved backup cooling to the class III (on-site) diesel generators, instrument air compressors, and feedwater pumps (main and auxiliary). The main feedwater (MFW) pump trips, on loss of service water cooling, were deleted to avoid spurious trips. The MFW pump motor status is annunciated in the main control room. However, the decision is left for the main control room operator to trip the MFW pump. The backup cooling supply to these users was taken from the firewater system or the reserve feedwater storage tank depending on the site.

A cost-benefit analysis was made to reduce the loss of service water initiating event frequency. However, the costs were too high in the late stages of commissioning the CANDU 6 plants.

In 1986, N. V. tot Keuring van Elektrotechnische Materialen (KEMA) of The Netherlands and AECL collaborated on a study[5,6] that looked at severe beyond-design-basis accidents (i.e., core disassembly or core melt) for an operating CANDU 6 unit in Canada. The core melt frequency for the CANDU 6 was 4.6×10^{-6}/yr. This PSA effort focused only on internal events at 100% power. Different initiating events during plant shutdown[1] were also studied by AECL. Loss of service water as an initiating event was the major contributor (60%) to the CANDU 6 severe core damage frequency (Fig. 1). The implemented design changes on the CANDU 6 units reduced the core damage frequency to a low value as a result of the diversity and redundancy in the CANDU design.

For future CANDUs, design improvements will be implemented to further reduce the core damage frequency. The design improvements are discussed in Sec. III.

II.B. Instrument Air

The design changes arising from the PSA of the loss of instrument air on the CANDU 6 also fell into the same categories as service water:

1. Prevention of consequential LOCAs: Additional local air tanks were provided for the heat transport reactor coolant, liquid relief valves, pressurizer relief valves, and pressurizer steam bleed valves.

2. Maintaining a long-term heat sink (i.e., continuous feedwater to the steam generators and shutdown

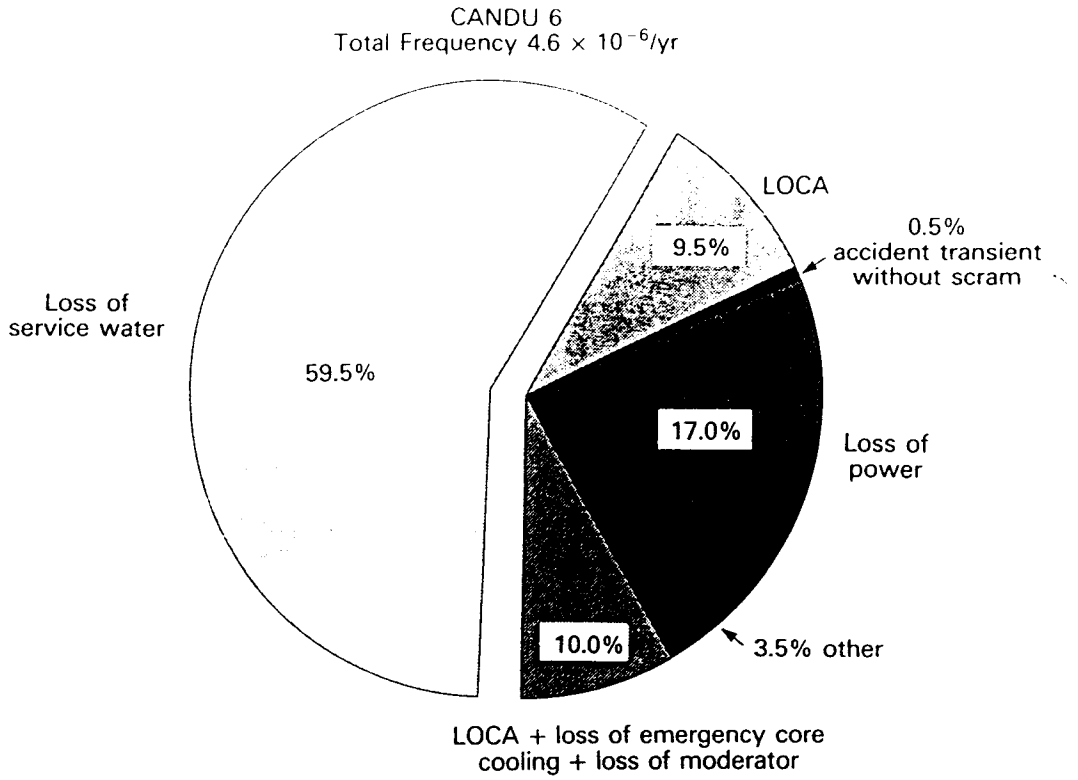

Fig. 1. Severe core damage frequency.

cooling) until instrument air is restored: The design changes provided local air tanks to the main steam safety valves and to the auxiliary condensate extraction pump and auxiliary feedwater pump regulating valves.

These design changes allowed the operator to cool down and depressurize the heat transport system for repair and recovery.

The design changes for loss of instrument air came about because the support system PSAs were the first ones attempted. Thus, as the PSA results became known, design changes were implemented to ensure that the PSA acceptance criteria at the time (any event sequence with severe core damage must occur $<10^{-7}$ event/yr) were met.

III. PSA PROGRAM FOR CANDU 3

The CANDU 3 is the latest CANDU reactor model.[7] It extends the proven economies of the larger CANDU units to a smaller size range [450 MW(electric) net]. To build a smaller unit at a low specific capital cost, the design, construction, commissioning, procurement, and project management of the project all require an innovative approach with a major emphasis on a significantly shorter construction schedule. Including PSAs as part of the design process is one way of ensuring that safety-related requirements are defined early, minimizing the probability of engineering rework during plant construction. In addition, PSA also plays the more traditional roles in safety assessment and licensing for the CANDU 3 design.

The objective of the CANDU 3 is to lower the initiating event frequency of loss of service water by an order of magnitude. The following design improvements have been incorporated to achieve this objective (see Fig. 2):

1. The raw service water system will have four pumps with a low passive failure rate. Common piping between two trains will be minimized by removing the cross tie (see Fig. 2).

2. Rubber expansion joints will be replaced with victualing couplings in the recirculated cooling water system. The use of rubber expansion joints in the raw service water system will be minimized.

3. Testable check valves will be installed in the recirculated cooling and raw service water systems.

The design improvements resulted in a reduced number of pneumatic valves in the plant, thus minimizing the effect of a loss of instrument air.

The CANDU 3 PSA program is divided into four phases[4]:

1. mini PSA
2. conceptual PSA (level 1)

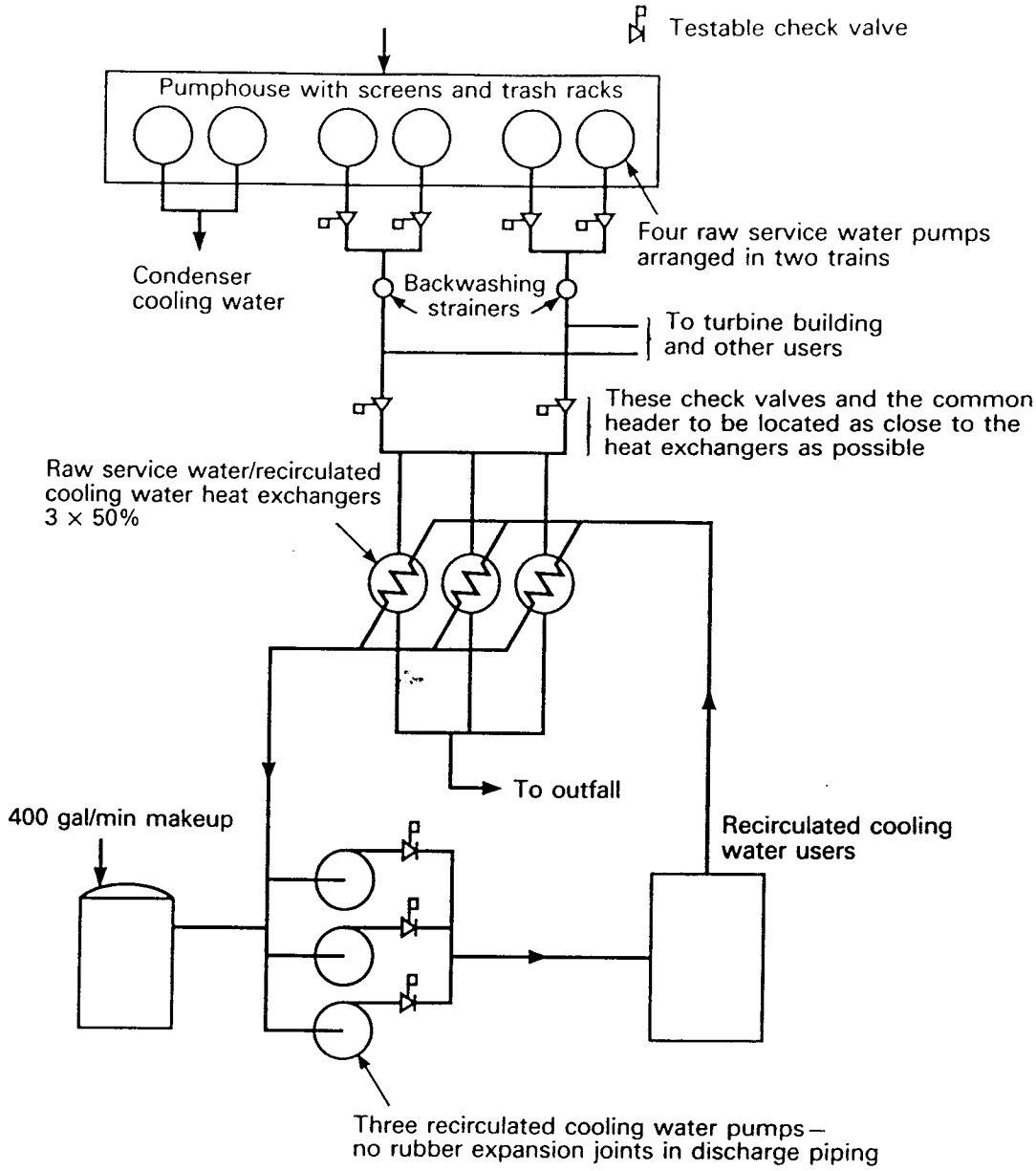

Fig. 2. Raw service water/recirculated service water schematic.

3. generic PSA (level 2)

4. site-specific PSA (level 3).

The mini PSA activity on the project is now complete. This stage consisted of a review of the proposed concept for three initiating events that previous CANDU PSA experience had shown were the main contributors to core melt frequency for CANDU: loss of off-site power, loss of service water, and small loss of primary heat transport reactor coolant. Improvements were identified and incorporated in the design.[8]

The usual practice has been to carry out the PSA after the design is complete. In some cases, however, the PSA has been done after the plant is in operation. In these situations, there is very little doubt about how the plant has been designed and constructed, and in most cases the procedures are in place for all foreseeable accidents, so the analyst knows how the operator is supposed to respond.

Performing PSA in parallel with the design poses a different challenge. During the conceptual design phase in particular, the plant configuration is not defined enough to be sure that all the system failure modes and interdependencies have been identified.

The approach taken during the conceptual PSA phase of the CANDU 3 work is to use the existing flow sheets to identify cross links and common-cause failures arising from common components and common

support services (electrical power, service water, and instrument air). System reliability targets are set based on past experience with similar systems or a simple fault tree analysis based on flow sheet information. These system reliability targets are then used in the event trees, which describe the plant response to the initiating event, to calculate the event tree end point frequencies.

Great care must be taken to document all assumptions about system performance and system interdependence so that the design either proceeds in a way that is consistent with our assumptions or the PSA team is made aware of deviations from the assumptions. At the end of the conceptual PSA activity, a plant performance specification (PPS) is produced that outlines system performance assumptions, interdependencies, and reliability targets. The PPS is used by the system designer to set system performance specifications and system design requirements, and deviations from the PPS are flagged.

The level 1 conceptual PSA activity is now almost complete. It includes a review of the proposed design concept for a wider selection of initiating events than those used in the first stage. Initiating events include large and small LOCAs, steam and feedwater system failures, and service water and electrical failures. Preliminary results indicate that the safety targets will be met with only minor modifications, in particular, automation of some mitigating actions.

Once the conceptual design has been frozen, a rigorous fault tree assessment of system reliabilities is done, and where cross links exist, the fault trees are merged to give a more accurate assessment of plant performance. Thus, the level 2 generic PSA is carried out to state-of-the-art standards with state-of-the-art methodology.

The generic PSA confirms whether the system reliability targets are met via detailed fault tree analysis and forms the basis of an application to the regulatory body for generic design approval for the CANDU 3 design.

For cases where the plant that is constructed deviates significantly from the generic design because of customer request or local siting or licensing requirements, a level 3 site-specific PSA is carried out. This PSA covers internal events only. External events will be covered deterministically, e.g., the seismically qualified equipment is designed to cope with a design-basis earthquake (a 10^{-3}/yr earthquake). The nonseismically qualified equipment is not credited in any safety analysis. However, following a design-basis earthquake, the seismically qualified equipment will ensure the following:

1. the plant is shut down
2. a heat sink is maintained
3. plant monitoring is maintained.

The approach is similar for other external events (e.g., a design-basis tornado).

In addition to the usual PSA optimization of component redundancy, the PSA program for CANDU 3 allows optimization of new aspects of the design. In the past, PSA activities were initiated after a large part of the design work had already been completed. With the earlier start of PSA work on CANDU 3, it is possible to use the early PSA results to better optimize the environmental qualification program for safety-related equipment and to design the control room displays and access to equipment to better reflect the postaccident requirements. As in the past, the results of the PSA program will be used in the preparation of postaccident operating procedures and in setting test and maintenance plans.

IV. SUMMARY

The following statements summarize this paper:

1. Atomic Energy of Canada Limited has performed PSAs on support systems since 1975. The PSA work initiated design changes during the construction commissioning phases between 1978 and 1983.

2. The CANDU utilities recognize the usefulness of PSA input to design and operation of their stations.

3. AECL recognized early the importance of the nonnuclear (conventional) part of the plant on overall plant safety.

4. To avoid design change and backfit possibilities during the construction phase of the CANDU 3 project, reliability targets and interface requirements are set early and are required to be met.

5. Preliminary results indicate that safety targets will be met with only minor modifications, in particular, automation of some mitigating actions.

ACKNOWLEDGMENTS

The author would like to acknowledge the efforts of the 1975–1983 AECL PSA team in helping to prepare the PSA. The system designers from AECL, Ontario Hydro, and Canatom provided the relevant information for the PSA preparation. The site staffs from New Brunswick Electric Power, Hydro Quebec, and Ontario Hydro, and the staff from KEMA, The Netherlands, were helpful in the review of the PSA.

REFERENCES

1. H. SHAPIRO and J. E. SMITH, "Probabilistic Safety Assessments in Canada," presented at American Institute of

Chemical Engineers Summer National Mtg., Boston, Massachusetts, August 1986.

2. P. GUMLEY, "Use of Fault Tree/Event Sequence in a Safety Review of CANDU Plants," presented at Int. Conf. Current Nuclear Power Plant Safety Issues, Stockholm, Sweden, October 20-24, 1980.

3. P. GUMLEY, P. S. NARAYANAN, and J. SMITH, "CANDU Alarm Sequence Analysis Following Abnormal Conditions," presented at Specialists' Mtg. Systems and Methods for Aiding Nuclear Power Plant Operators During Normal and Abnormal Conditions, Balatonaliga, Hungary, October 4-6, 1983.

4. D. F. RENNICK, V. G. SNELL, P. GUMLEY, and P. S. NARAYANAN, "Enhancements in Safety Resulting from Probabilistic Safety Assessments—A Designer's Perspective," Topl. Mtg. Nuclear Power Plant Operations, Chicago, Illinois, September 1, 1987.

5. V. G. SNELL et al., "CANDU Safety Under Severe Accidents," presented at Int. Symp. Severe Accidents in Nuclear Power Plants, Sorrento, Italy, March 21-25, 1988.

6. J. Q. HOWIESON et al., "A PRA Study of CANDU 600," presented at Int. Symp. Severe Accidents in Nuclear Power Plants, Sorrento, Italy, March 21-25, 1988.

7. P. J. ALLEN, "The Use of PSA in the Design, Safety Assessment and Licensing of the Advanced CANDU Design," presented at Int. Topl. Mtg. Probability, Reliability and Safely Assessment, Pittsburgh, Pennsylvania, April 2-7, 1989.

8. R. JAITLY, J. R. FISHER, S. NAMAN, and H. S. SHAPIRO, "CANDU 3 Probabilistic Safety Assessment—Insights and Design Decisions," Int. Mtg. Probabilistic Safety Assessment and Management, Beverly Hills, California, February 4-7, 1991.

Hymie S. Shapiro (BEng, chemical engineering, McGill University, Canada, 1973; MASc, chemical engineering, University of Waterloo, Canada, 1977) is team leader of the probabilistic safety assessment (PSA) studies group for the Canada deuterium uranium (CANDU) 3 project at Atomic Energy of Canada Limited. He is the Canadian representative to the Organization for Economic Cooperation and Development. He has lectured extensively on PSA.