CANDU® 9 SAFETY ENHANCEMENTS AND LICENSABILITY

J.R. Webb and V.G. Snell

Atomic Energy of Canada Limited (AECL)
Mississauga, Ontario
Canada L5K 1B2

18th Annual Conference of the Canadian Nuclear Society,
1997 June 8-11
Toronto, Ontario, Canada

ABSTRACT

The CANDU 9 design has followed the evolutionary product development approach that has characterized the CANDU family of nuclear power plants. In addition to utilizing proven equipment and systems from operating stations, the CANDU 9 design has looked ahead to incorporate design and safety enhancements necessary to meet evolving utility and regulatory requirements both in Canada and overseas.

To demonstrate licensability in Canada, and to assure overseas customers that the design had independent regulatory review in the country of origin, the pre-project Basic Engineering Program included an extensive two year formal review by the Canadian regulatory authority, the Atomic Energy Control Board (AECB). Documentation submitted for this licensing review included the licensing basis, safety requirements and safety analyses necessary to demonstrate compliance with regulations as well as to assess system design and performance. The licensing review was successfully completed in 1997 January. In addition, to facilitate licensability in Korea, CANDU 9 incorporates feedback from the application of Korean licensing requirements to the CANDU 6 reactors at Wolsong site.

1. INTRODUCTION

The CANDU product line is built around the 700MWe and 900MWe class reactors. The CANDU 6 (700MWe class) reactors are operating in four countries and five units of the latest version are in operation or under construction in Korea and in China. There are 12 units of the CANDU 900MWe class currently operating in Canada at the Bruce and Darlington sites. The Bruce B and Darlington plants, each with four integrated reactor units, represent the second generation of the 900MWe class plants. The CANDU 9 design, with a gross output of 935MWe, is a single unit adaptation of these plants.

To satisfy client and regulatory expectations, both now and in the future, AECL has adopted an evolutionary approach in which the proven designs of the CANDU 6 and CANDU 9 products are improved incrementally and continually. This evolution is guided by the requirements of the operating utilities who look for:

- improved economics, through the reduction of plant capital and operating costs and project implementation risks;
- enhanced safety, through more reliable operation, more effective safety systems and greater resistance to severe accidents, and
- improved operability, through design simplification and the appropriate introduction of new technologies.

This paper summarizes the design and safety improvements of CANDU 9 and the results of the Atomic Energy Control Board (AECB) licensing review.

2. AECB LICENSING REVIEW

2.1 The Review Process

Although CANDU 9 is based on operating CANDU nuclear power plants, it is possible that domestic or foreign potential customers would require evidence of current licensability in the country of origin (Canada). Such evidence would dramatically reduce the risk of licensing-induced design changes once a project had been committed. It would also assure customers that the CANDU 9 design had been through a thorough independent review. An intensive "up-front" licensing process was therefore established to give this assurance, consisting of a two-year review by the Canadian regulatory authority, the AECB. The finding sought from the AECB Staff was one of "no fundamental barriers" to licensability in Canada. Although a further detailed licensing review would be done by the responsible regulatory authority after commitment of the project, this "up-front" licensing assurance would allow such an authority to proceed with confidence. The review was done against the most recent regulatory requirements, that is, those in effect on 1995 January 1.

The "up-front" licensing approach is not new in Canada, although this is the most extensive application of it to date. It is strongly supported by the AECB. In a recent paper, (Reference 1), the AECB stated its support as follows:

> "... the AECB believe that an agreement with designers and licensees on the basis for licensing and the safety-related design requirements, at a very early stage in the licensing process, will reduce the licensing risk for the owner; and the cost of modifications, should they be needed, will be much less."

The review process followed a structured and logical approach. AECL first proposed a Licensing Plan to the AECB, giving the scope and schedule of the submissions. The AECB had numerous comments on this Plan, and a revised Plan, reflecting AECB requests for additional submissions (about a 50% increase in scope), was then agreed. The document submission schedule to the AECB ensured that design requirements were submitted and agreed first, followed by the

description of how these requirements were implemented in design and satisfied in safety analysis. This approach made it possible to complete the review in a two-year period.

Early in the review process, AECL submitted the Technical Description of the CANDU 9 to familiarize the AECB with the design and to initiate the licensing review. Along with this, AECL submitted the Licensing Basis Document (LBD), the high-level listing of the major licensing requirements. It calls up the appropriate regulatory documents and codes and standards, and interprets, in case of ambiguity, how the licensing requirements will be applied. This is a key part of Canadian licensing philosophy, in which the onus is on the designer to propose how the licensing requirements will be met, with the AECB accepting or rejecting the designer's proposals. The LBD therefore included both AECB requirements and the requirements, as best they are known prior to the formal application for a license, of the foreign regulatory authorities, as well as lessons learned from previous licensing experience. The LBD, once accepted by the AECB, provides important guidance to a foreign regulatory authority on how licensability in Canada is implemented on CANDU 9.

These two early submissions were followed by more detailed design requirements documentation, design methods (e.g., for safety critical software), safety analyses, probabilistic safety analysis, and other program documents such as quality assurance, decommissioning, safeguards, and security requirements. In selected cases, AECB inspected details of the design implementation. In total, over 200 formal documents were submitted. AECB review of the detailed submissions, while comprehensive, focused particularly on:

- new or unique features in the CANDU 9 design
- new or revised AECB Regulatory or Consultative documents
- Generic Action Items applying to all CANDU plants
- known operational safety issues
- importance to reactor safety

Midway through the review, the AECB staff identified thirteen key issues requiring a more detailed assessment. Intensive discussion took place for almost a year on these issues, resulting in many further submissions and analyses by AECL, and in some cases design changes, so that the issues could be closed at the end of the licensing review. To ensure that interested foreign customers were kept informed of the progress during the course of the review, the AECB issued two interim reports in June and September 1996 prior to the issue of the final report in January 1997.

2.2 Application of AECB Regulatory and Consultative documents

The AECB paper (Reference 1) notes the approach taken for the development of new regulatory requirements in Canada, as follows:

> "... new regulatory requirements for plants being designed today are based on a number of factors, including: a more rigorous application of the basic philosophy; operating experience of CANDU gained over the last 20 years; the steady development of knowledge about the behaviour of CANDU plants, and the capability of designers to predict accident behaviour; resolution of outstanding safety and licensing issues;

introduction of human factors considerations during design and operation of the plant; continued increase in computerization in new designs; simplification of the design, operation and maintenance of the plant; and, improvements in severe core accident mitigation and management."

The CANDU 9 licensing review provided the first opportunity to implement a number of new or revised AECB regulatory and consultative documents. Among these were:

- R-7, Requirements for Containment Systems (effective date 1991 February)
- R-8, Requirements for Shutdown Systems (effective date 1991 February)
- R-9, Requirements for Emergency Core Cooling Systems (effective date 1991 February)
- R-90, Policy on Decommissioning of Nuclear Facilities (effective date 1988 August)
- C-98, Rev. 1, Reliability Requirements for Safety Related Systems of Nuclear Reactor Facilities (draft dated 1995 March)
- C-129, The Requirements to Keep All Exposures As Low As Reasonably Achievable (draft issued for comments 1994 July)

Despite the draft nature of some of these documents, CANDU 9 was designed for compliance, in anticipation that the documents would be issued or approved by the time of application for a Construction License. To record this, a series of Compliance Documents was produced. They provide an audit trail for the regulator on the detailed implementation of the requirements in the design. These "live" documents will be updated during the project phase, and carried over to plant commissioning and operation to ensure that operating and maintenance procedures comply with the regulatory requirements.

2.3 Response to Generic Action Items

The AECB uses Generic Action Items (GAI) to track the progress in resolving licensing issues common to operating CANDU reactors. For the CANDU 9 licensing review, the AECB required that:

- design solutions shall be provided for GAI's, whenever feasible,
- the plans and schedules for resolution of the issues shall be documented, and
- sufficient safety margins shall be shown, or future design improvements should not be precluded.

The CANDU 9 addresses *all* the current GAI's through a combination of design changes, consideration in the design process or R&D support. As an example of a design change, the single loop Heat Transport System in combination with a large pressurizer addressed the concern of GAI 90G02, "Core cooling in the Absence of Forced Flow", since the HTS is always single phase for accidents which tend to cool and shrink the coolant, so that thermosyphoning is more easily demonstrated. As an example of a design process, the CANDU 9 approach has been to systematically identify measures taken in the design stage to achieve the goals of plant life management and to address GAI 90G03, "Management of Aging". An overall review of the CANDU Plant Life management (PLIM) program is provided in Reference 2. As an example of *R&D* support, an industry-wide program to upgrade the validation of safety analysis codes,

including the two-phase non-equilibrium transient thermohydraulics code CATHENA code, was the response to GAI 94G01, "Emergency Core Cooling Effectiveness", since it established confidence in the predictions of CATHENA.

2.4 AECB Summary and Conclusions

The summary statement of the AECB licensing review for the CANDU 9 design reads as follows:

> "AECB staff conclude that there are no fundamental barriers to CANDU 9 licensability in Canada."

This statement results from the review of the information provided to the AECB, and is based on three general conclusions: that the CANDU 9 design complies, or can be made to comply with licensing requirements in effect, in Canada, on January 1, 1995; that the proposals to address AECB Generic Action Items on the CANDU 9 design are acceptable; and that the major issues identified during the course of the licensing review have been adequately addressed.

This has been a successful application of "up-front licensing". Prospective owners can take comfort in the consequential reduction of licensing risk to the project.

3. SIGNIFICANT SAFETY ENHANCEMENTS

Safety enhancements for CANDU 9 either build on the inherent safety characteristics of the CANDU design (especially in the area of severe accidents) or respond to operating experience.

3.1 Radiation Protection

The CANDU 9 plant has been designed to comply with ICRP-60, the recommendations of the International Commission on Radiological Protection issued in 1991. These ICRP recommendations reduce the limits for occupational exposure dose to 20mSv/a, averaged over 5 years, and public exposure dose to 1mSv/a. As a design target, the CANDU 9 plant has been designed so that total worker exposures will be less than 1 person-Sv/a and the maximum exposure to a member of the public will be less than 50 μSv/a. Specific details are provided in Reference 3. The approach taken to reduce the internal exposures of workers and tritium emissions to the public has been to reduce tritium-in-air levels by upgrading the vapour-recovery system. The approach taken to reduce the external exposures of workers during shutdown conditions has been to improve equipment layout and reduce corrosion-product activity transport. Relatively easy access to the reactor building during plant operation has been a traditional CANDU advantage, and by careful attention to segregation of higher activity water vapour from lower activity areas this has been retained, while achieving the targets for total worker and public exposure.

3.2 Control Centre

For improved operational capabilities, the CANDU 9 design has incorporated an advanced control centre. Specific details are provided in Reference 4. The control centre layout incorporates the results of Human Factors analysis; a new computerized Plant Display System is separated from the digital control computer system; and the two computerized reactor shutdown systems have increased capability. The CANDU 9 control centre provides plant staff with a layout and information organization that is better matched to operational tasks.

A major evolutionary change from previous CANDU plants is the separation of the control from the display/annunciation features, both of which were formerly provided by the digital control computers (DCC). Control is now in the distributed control system (DCS) and display/annunciation is in the plant display system (PDS). This strategy allows powerful computers without application memory constraints or execution limits to provide extensive control, display or annunciation enhancements within an open architecture.

The control centre features standard panel human-machine interfaces that provide an integrated display and presentation philosophy; and includes the use of a common plant display system for all consoles and panels. A large, central overview display presents immediate and simplified plant status information to facilitate operation staff situational awareness in a legible and recognisable format. A powerful and flexible annunciation system provides extensive alarm filtering, prioritising and interrogation capabilities to enhance staff recognition of events and plant state.

The reactor shutdown computers for CANDU 9 include automated system testing and on-line neutronic trip calibration capabilities. One specific benefit of on-line calibration is an improved "margin-to-trip". Safety system monitor computers provide automated safety system testing, resulting in shorter test duration with reduced opportunity for human error.

3.3 Severe Accidents Program

In the CANDU context, a severe accident is not the same as severe core damage since, in the absence of coolant and failure of emergency core cooling, the moderator can preserve the pressure tube geometry without fuel melting. Therefore, if the moderator water can be cooled or even just topped up, core melt is not an issue. The CANDU 9 design underwent a systematic review to identify, prevent, and mitigate severe accidents. A detailed description of the program is provided in Reference 5. First, severe accidents and severe core damage frequency targets were set. A preliminary Probabilistic Safety Assessment was done early in design, and identified risk-dominant sequences. Changes required to meet the frequency targets for severe accidents were then identified and implemented.

While the overall severe accident program ensures a balance between preventative and mitigation measures, the role of the containment system is significant. For this reason, the licensing review noted the following enhanced features of the CANDU 9 containment:

- Large containment, with judicious layout of equipment resulting in large, open volumes, with good potential for natural circulation and no apparent hydrogen traps.

- Pre-stressed concrete boundary with steel liner resulting in increased design pressure (210kPa) and low leakage rate (0.2%/day)
- Large structural steel heat sinks that augment engineered safety systems provided to remove heat, moisture and fission product aerosols from the containment atmosphere
- Hydrogen mitigation systems that allow systematic and timely dispersion and reduction of hydrogen concentrations
- Instrumentation for measurements under accident conditions
- Reliable isolation of large containment penetrations through independence and diversity
- The elimination of the dousing system and the incorporation of the Reserve Water System

The Reserve Water System is a storage and distribution system designed to deliver light water under gravity to a variety of systems whenever normal water sources are unavailable and make-up water is required. During normal operation, the system is isolated. The system consists of a large tank located at a high elevation within the reactor building, and is designed to provide make-up to the Heat Transport System, the Moderator System, the Steam Generators, the Emergency Core Cooling System and the Shield Cooling System. It has enough heat removal capacity for three days, so that severe accident management is relatively straightforward and decisions need not be made in haste.

Makeup from the Reserve Water System to the moderator, as noted, prevents fuel melting following a Loss of Cooling Accident and loss of Emergency Core Cooling (LOCA/LOECC). This is backed up again by makeup to the shield tank to remove decay heat by boiloff. Thus, even a severe core damage progression would be arrested at, or contained within, the calandria tank.

3.4 Grouping And Separation

The concept of grouping and separation of safety related systems has been an integral to CANDU plants. This concept provides physical and functional separation of safety related systems to ensure that common cause events do not impair the capability to perform essential safety functions. In this concept, the plant can be shut down, decay heat removed, and the plant conditions monitored independently from systems and components of either one of two groups, known as Group 1 and Group 2. For the CANDU 9 design, this concept has been enhanced through additional redundancy and diversity in the provision of cooling water and power supplies.

The main control room and the secondary control area are part of this concept. Although both have independent functions of shut down, cool, contain and monitor, the main control room can be used for all design basis accidents, including external events, so that the secondary control area is only required for a major fire or hostile takeover which requires an evacuation of the main control room. Both locations are qualified to operate during design basis and external events, and the necessary structures and systems have been appropriately protected and qualified.

3.5 Design Simplification

System reliability has been improved and the plant is more forgiving. Some examples are as follows:

- ECC component simplification, and reduction in the use of active components (replacement of valves by one-way rupture disks and ball seals)
- Longer operator action times, generally 8 hours for serious process failures; for example, the provision of a larger pressurizer improves the plant response following loss of flow events
- Design of the Shutdown Cooling System such that it can be placed in service under zero power, full pressure, hot conditions
- Improvements to heat sink redundancy and diversity in all shutdown conditions, e.g. high pressure Group 2 feedwater
- Reduction of manual operations such as the automation of the Group 2 feedwater system, automation of all ECC phases, and automatic startup of the Group 2 diesel generators for emergency power supply as a back up to the Group 1 Class III diesel generators.

3.6 Enhanced Human Factors Engineering

All aspects of plant design for which there is an interface with plant personnel incorporate consistent human factors considerations through the application of a formal Human Factors Engineering Program Plan (HFEPP). This plan defines the process of incorporating human factors into the design of CANDU 9 system and equipment. Underlying this approach is a refined engineering design process that cost-effectively integrates operational feedback and human factors engineering to define operations staff information and information presentation requirements. As part of the CANDU 9 design strategy, a physical, full-scale mock-up of the control centre panels and consoles is being used for conceptual evaluation, rapid prototyping, design decision-making, and for the verification and validation of the design features, displays and operator interactions. The functionality of the simulation supported control centre mock-up provides a dynamic mechanism for the on-going verification and validation design activities by system designers.

4. SUMMARY AND CONCLUSIONS

CANDU 9 is a stand-alone version of the successful multi-unit Darlington and Bruce Nuclear Generating Stations operating in Ontario, Canada. Added to the advantages of using proven systems and components, CANDU 9 offers a higher electrical output, better site utilization, shorter construction time, improved station layout and better operability. Significant progress has been made on the CANDU 9 Basic Engineering Program, and in 1997 January, the licensing review of CANDU 9 design was completed by the Canadian Regulatory Agency, the AECB, and the final report issued. In addition to identifying a number of CANDU 9 improvements over previous CANDU designs, the AECB concluded that there were no fundamental barriers to CANDU 9 licensability in Canada.

REFERENCES

1. J.D. Waddington, "Power Reactor Licensing in Canada, 1995", presented at the KAIF/CNA CANDU Seminar, Seoul, Korea, 1996 May
2. B.A. Shalaby and E.G. Price, Plant Life Management and Extension for CANDU NPP, presented at NUTHOS 5, Beijing, China, 1997 April.
3. C.R. Boss, P.J. Allsop and N. Gagnon, "Compliance of CANDU Nuclear Power Plants with ICRP 60", presented at the 12th KAIF/KNS Annual Conference, Seoul, Korea, 1997 April.
4. L. Lupton, N.M. Ichiyen, and S.K.W. Yu, Operational Improvements in the CANDU 9 Control Centre, presented at the 12th KAIF/KNS Annual Conference, Seoul, Korea, 1997 April.
5. S.M. Nijhawan, A.L. Wight and V.G. Snell, Addressing Severe Accidents in the CANDU 9 Design, presented at the IAEA Technical Committee meeting on Impact of Severe Accidents on Plant Design and Layout of Advanced Water Cooled Reactors, Vienna, 1996 October.