# Lessons for PHWRs Learned from the Chernobyl Accident

by

J.G. Waddington
and
T.J. Molloy

Atomic Energy Control Board
Ottawa, Canada

April 1996

Atomic Energy Control Board | Commission de contrôle de l'énergie atomique

Canada

SUMMARY

The Atomic Energy Control Board of Canada examined its criteria for licensing nuclear power plants following the accident to the Chernobyl reactor in 1986. The causes of the accident were studied to ascertain whether they revealed any deficiencies in the safety of CANDU PHWRs. A report published in 1987 contained nine recommendations, and this paper revisits these to indicate how they were dealt with by plant owners and the regulatory authority.

SOMMAIRE

La Commission de contrôle de l'énergie atomique du Canada a examiné ses critères pour la délivrance des permis aux centrales nucléaires après l'accident survenu en 1986 au réacteur du Chernobyl. On a étudié à fond les causes de l'accident pour déterminer si celles-ci révèlent des lacunes dans la sûreté des réacteurs CANDU. Un rapport publié en 1987 renfermait neuf recommandations. Le présent document passe en revue ces recommandations et, notamment, comment les propriétaires de centrale et l'organisme réglementaire ont répondu à ces recommandations.

## Lessons for PHWRs Learned from the Chernobyl Accident

Like most other national regulatory bodies, the Atomic Energy Control Board of Canada examined its criteria for licensing nuclear power plants following the accident to the Chernobyl reactor in 1986. It also requested the designers and owners of existing NPPs to re-examine a number of specific aspects of the safety of their facilities.

The causes of the accident at Chernobyl were studied by a working group at the AECB to ascertain whether they revealed any shortcomings in the safety of CANDU reactors. The working group prepared a report (INFO-0234), which was published in 1987, containing nine specific recommendations. In this paper, we revisit these recommendations indicating how they were dealt with by plant owners and the regulatory authority.

1987 Recommendation 1

*The safety analyses of CANDU reactors should be re-examined to confirm that shutdown systems are sufficiently effective under conditions in which a rapid increase in the volume of steam in the fuel channels may occur, or in which there may be a rapid increase in reactivity.*

The recommended re-examination was performed by Ontario Hydro and by AECL, designers of the CANDU. CANDU reactors are over-moderated, and for this reason have a positive void coefficient of reactivity. Analysis showed that a guillotine failure of the largest reactor cooling system header, with the reactor at full power, is the accident causing the fastest reactivity insertion rate. The effectiveness of the shutdown systems for such large-break LOCAs is documented in the various facility safety reports. The design criterion of preventing fuel centreline melting as a result of the initial overpower transient is met with a generous margin. No new information could be identified which would invalidate or call into question the licensing basis or the adequacy of shutdown systems.

1987 Recommendation 2

*The effects of various configurations of reactivity devices in CANDU reactors should be examined to ensure that the reactor cannot be put into a condition in which the shutdown systems might be rendered less than adequately effective. In particular, the capability of the shutdown systems should be studied under conditions in which there are spatial variations in reactivity.*

In CANDU reactors, all shutoff rods are located above the reactor. When called upon, they are released into the core under gravity or with an initial spring force. A second, equally capable and independent shutdown system injects gadolinium solution directly into the core at approximately mid plane.

Top-to-bottom variations in the neutron flux distribution (flux tilts) have the potential to decrease the effectiveness of the shutoff rods by delaying the time at which the rods reach the region of high neutron importance. A similar effect could take place for the poison injection in the event of a side-to-side tilt. Flux tilts can be induced by operating with reactivity devices, which in CANDU reactors are independent of the shutoff rods, in some off-normal positions and/or, in some reactors, with reduced moderator level. The latter is a

theoretical concern only; operation in this mode is very unusual and is conducted only under strictly controlled conditions.

Extensive analyses have been performed by plant owners to investigate the effect of flux tilts and to demonstrate the effectiveness of shutdown systems. The work has largely involved analysis of large-break LOCAs in the presence of an initial flux tilt. For certain cases where the safety margins have been found to be significantly reduced when a large tilt is assumed, revisions have been made to operating rules and reactor regulating system parameters to reduce the allowable degree of flux tilt within the licensed operating envelope.

The Bruce A and B reactors are currently operating at reduced power levels due to the predicted effect of fuel movement during certain postulated LOCA events. Assuming the presence of flux tilt exacerbates the predicted effect of fuel relocation and has contributed to the decision to reduce power.

Work is currently under way to assess more carefully the uncertainties associated with various components of the large-LOCA power-pulse analysis. Flux tilt increases energy deposition in the power pulse and consideration of it has been one of the main reasons for closer scrutiny of power-pulse analysis.

Reactor operation with flux tilts which are outside the operating envelope may result from certain specific failures in the reactor regulating system. Such failures coincident with other postulated accidents such as the large-break LOCA are considered low-probability events and are not analyzed.

1987 Recommendation 3

*The safety of the Pickering 'A' reactors should be re-examined, particularly with respect to accidents involving failure of the reactor control system and loss of coolant accompanied by unavailability of the shutdown system.*

The re-examination of the Pickering A safety analysis led eventually to some significant modifications to the reactor shutdown system. These modifications, and the rationale for their acceptance, will be discussed later in this paper.

1987 Recommendation 4

*Station operating procedures should be re-examined to ensure that they specify and receive sufficient review by all pertinent and responsible personnel before tests on safety-related equipment are carried out or procedures for such tests are modified.*

Submissions were received from plant owners describing how work plans are reviewed by persons knowledgeable in system design and operation, and in safety practices. For new and revised test procedures, reviews by senior plant staff are required; these may involve closely controlled rehearsals on a plant simulator before approval is granted. The AECB concluded that there was no need to require specific changes to operating procedures.

1987 Recommendation 5

*A review should be conducted with a view to a possible increase in the frequency and extent of monitoring and auditing the performance of plant operators in complying with operating procedures and the conditions of operating licences.*

Plant owners responded to this recommendation by declaring that they already had adequate programs in place for monitoring and auditing the performance of operating staff. The AECB accepted the owners' statements in light of the fact that licensees' QA programs are subject to internal audits and to regular compliance inspection and audits conducted by AECB staff.

1987 Recommendation 6

*A study should be made of the ways in which special safety systems can be disabled in CANDU reactors. These should then be reviewed to determine whether the design includes sufficient protection to prevent the disabling of safety systems without first obtaining appropriate management review and, if necessary, approval by the regulatory authority.*

AECB staff reviewed the licensees' submissions and were satisfied that sufficient physical and administrative barriers exist to prevent safety systems from being disabled. The practice of manual blocking of the emergency core cooling system was specifically identified in all submissions. Blocking is permitted when the reactor is shut down and the reactor cooling system is depressurized for maintenance or inspection. This is done under strict administrative and procedural control. The AECB is satisfied that these controls are adequate.

1987 Recommendation 7

*Plant owners should review their on-site emergency procedures to determine the need for any changes.*

All three utilities operating NPPs in Canada undertook thorough reviews of their on-site procedures and their commitments to participate in off-site emergency measures. Significant improvements were made to communication facilities and training of staff in procedures as a result of these reviews. The AECB is satisfied with the current status.

1987 Recommendation 8

*The recommendations from the emergency planning group in Ontario should be considered by all emergency planning authorities.*

This suggestion was followed by the three provincial jurisdictions, who are responsible in Canada for emergency preparedness. One felt no major changes were necessary; another undertook major improvements. In Ontario, where three multi-unit NPP sites are located, improvements to planning and preparedness are still proceeding.

1987 Recommendation 9

*Plant owners should review their fire-fighting techniques to determine how best to protect personnel from radiation hazards which may accompany a reactor fire.*

All three utilities accepted this recommendation by undertaking thorough examinations of their procedures and the equipment available for fighting fires. Extensive retraining of staff was instituted, involving in some cases simulation exercises which revealed certain weaknesses. Remedial actions to remedy these weaknesses are still under way.

**Modifications to Shutdown System at Pickering NGS "A"**

A design element which the CANDU HWRs have in common with the Chernobyl reactors is a positive void coefficient of reactivity, although the coefficient in CANDU is about three times smaller at low power levels. It has always been a licensing requirement in Canada that each reactor have a fast-acting shutdown system capable of shutting the reactor down very quickly for a wide range of potential initiating events, including loss of regulation at various power levels. Shutdown systems have been required to be entirely independent of reactor regulating systems, and to satisfy specific requirements for reliability. Current licensing standards specify that there must be two fully effective and independent shutdown systems for each reactor.

The AECB concluded that for reactors conforming to its current licensing requirements the shutdown system specifications are adequate to ensure that a fast reactor shutdown will occur when required, including all those accidents in which the positive void coefficient of reactivity plays a significant role. It was, however, considered prudent to re-examine the safety analyses of CANDU reactors, with particular attention to events in which a rapid increase in the volume of steam may occur, or in which there may be a rapid increase in reactivity, to confirm that the shutdown systems are indeed sufficiently effective. In addition, it appeared appropriate to examine possible configurations of reactivity devices to ensure that it is not possible to put a reactor in an unusual configuration in which the shutdown systems might be rendered less than adequately effective.

The oldest NPP in Canada still licensed for operation is the four-reactor station known as Pickering NGS "A," near Toronto. At the time when Pickering "A" was originally licensed, the requirement for two independent shutdown systems had not been formulated, but there was a requirement to analyze accidents in which a loss of reactor control or a loss of coolant was accompanied by complete failure of the shutdown system. This was some years before ATWS studies were undertaken in the USA.

The original safety report for Pickering "A" included analysis of this postulated accident, and it was concluded that doses to the public would not exceed the AECB reference dose limits. However, a detailed quantitative analysis was not performed; indeed, with the computing tools available in the 1960s, it was not really possible. It was largely because of the speculative nature of such analyses that the requirement for a second shutdown system was subsequently introduced. While the Pickering "A" reactors have always had two shutdown mechanisms, dumping of the heavy water moderator and insertion of neutron-absorbing rods,

these mechanisms are not independent of each other because they rely on common instrumentation. In addition, dumping of the moderator is relatively slow.

In an effort to produce a more sound basis for the safety of the Pickering "A" reactors, the plant owners had taken advantage of major modifications to the reactors in the mid 1980s to nearly double the number of shutoff rods in each unit. They then performed analysis of the effectiveness of the shutdown system with various levels of impairment, and concluded that the shutdown system could be effective in preventing serious consequences even if several shutoff rods failed to fall. These analyses improved the level of confidence that an accident with severe consequences would have a low probability of occurrence.

Nevertheless, in view of the severity of the consequences of the Chernobyl accident, it was considered prudent to re-examine the safety of the Pickering "A" reactors, particularly with respect to accidents involving failure of the reactor regulating system or loss of coolant accompanied by unavailability of the shutdown system. It should be remembered, however, that the Chernobyl accident was not the result of failure of the shutdown system to act, but rather of inadequate shutdown capability for that reactor design.

In response to a request by AECB staff (and recommendations from the Ontario Nuclear Safety Review), Ontario Hydro submitted (October 1987) a revised analysis of the consequences of a large loss-of-coolant accident (large LOCA) combined with a failure to shut down. This analysis concluded that the structural integrity of containment would be maintained and that the reference dose limits for serious failures accompanied by unavailability of a safety system would be met. AECB staff found this analysis to be speculative and concluded that the consequences could not be quantified with confidence. Ontario Hydro was requested to prepare backfit design proposals to reduce the probability of a failure to shut down.

In January 1992, Ontario Hydro submitted a report which considered four options for improvement in the shutdown system capability. Each option would incorporate a regional overpower system (ROP) (using in-core flux detectors as sensing elements) to protect against local power increases in the core. The proposals ranged from the incorporation of a second, fully independent, shutdown system using poison injection to a significant upgrade of the existing single shutdown system.

The proposal for a full second shutdown system included the development of a scheme for injecting gadolinium solution into the moderator from vertical access tubes which could be made available. This option would have approached the current licensing requirements, but at high cost to the utility. The more important reasons for rejecting it were the delay which would have been involved in its implementation and the high radiation dose to personnel who would have had to perform the installation modifications. A variation on this proposal also involved the poison injection scheme but employed only neutron flux parameters to initiate shutdown action.

Another proposal involved dividing the 21 shutoff rods into two banks, each with its own set of sensor devices for process and neutronic parameters. This option would afford a degree of independence and diversity from the existing shutdown system, but with the fewer number

of rods per bank there was insufficient depth of shutdown to ensure, with a high degree of confidence, the preserving of fuel channel integrity following the most severe initiating events.

The chosen option consists of a separate logic train with neutron overpower and log-rate power increase as trip parameters, using in-core detectors and out-of-core fission chambers. Both the new and the existing logic trains actuate all the shutoff rods. The total number of shutoff rods has also been further increased from 21 to 23. The enhanced system for the Pickering "A" reactors will continue to be considered as only one shutdown system which must be capable of safe shutdown for the limiting case. The unavailability target for each of the logic trains has been set at $10^{-3}$, and past operating experience at the station suggests that this can be achieved. Hence the probability that an event requiring reactor shutdown will not be sensed should be very low. Furthermore, as only 19 of the 23 rods now available will accomplish a full shutdown for all postulated events, the probability that an adequate number of rods will not fall into the core when required is also very low. The new design will, therefore, achieve a significant reduction in the probability of failure to terminate a reactor power excursion. These factors, together with a reasonable schedule for design and implementation of the changes and an acceptable prediction for dose commitment to the installers, led to acceptance by the AECB of this option.

The modifications to the four units at Pickering "A" are under way and are expected to be completed on schedule by the end of 1997.