INFO-0010

IMPACT OF THE THREE MILE ISLAND ACCIDENT ON REACTOR SAFETY AND LICENSING IN CANADA

by J.D. Harvie

Atomic Energy Control Board

June 18, 1980

Ottawa, Canada

20th Annual International Conference 1980

Canadian Nuclear Association

Montreal, Canada

RÉSUMÉ

Ce document discute des conséquences de l'accident de Three Mile Island sur la sûreté des réacteurs canadiens et sur les mécanismes de réglementation de ces réacteurs. Les principes de sûreté des réacteurs qui ont été révélés ou confirmés par cet accident y sont passés en revue. Il se dégage en conclusion que la sûreté des réacteurs dépend avant tout de l'engagement ferme de toutes les personnes travaillant dans les divers secteurs de l'industrie nucléaire à l'achèvement de ladite sûreté.

IMPACT OF THE THREE MILE ISLAND ACCIDENT ON REACTOR SAFETY AND LICENSING IN CANADA

J.D. HARVIE
Atomic Energy Control Board
P.O. Box 1046
Ottawa, Ontario
K1P 5S9

ABSTRACT

This paper discusses the implications of the accident at Three Mile Island on reactor safety and licensing in Canada. Reactor safety principles which can be learned from, or are reaffirmed by, the accident are reviewed. It is concluded that reactor safety demands a firm commitment to safety by all those involved in the nuclear industry.

INTRODUCTION

Following the accident at Three Mile Island, two members of the staff of the Atomic Energy Control Board were taken from their normal duties and given the task of reviewing the vast quantity of information which was becoming available on the accident, and of making recommendations on the implications on the safety of CANDU reactors. This study resulted in a report by B.J. Pannell and F.R. Campbell (reference 1), and the technical content of my talk to-day is based largely on that study. It is not my intention to discuss all the details of the report, but I will mention some of the highlights and make some general observations of my own.

There have been many studies of the Three Mile Island accident, and a large number of technical recommendations have been made to prevent its recurrence. This is a natural result of an event which had such a serious effect on the reactor and its fuel, and a major impact on the public, although fortunately not in a medical sense. However, it is important to examine not only the details of that particular incident, but also the general lessons which can be learned from, or reaffirmed by the accident, especially when consideration is being given to the implications of the accident on a reactor of a different type.

OPERATOR TRAINING

The most obvious lesson which can be learned from the Three Mile Island accident is the importance of the plant operators to reactor safety. The accident demonstrated the need for a well-organized and thorough training program, covering not only normal operation, but also abnormal and emergency situations. My impression is that the training of operators for such abnormal situations has been better in this country than it appears to have been for the operators at Three Mile Island. On the other hand, some aspects of our operator training have not met the standards which are applied in other countries. For example, the use of simulators in the training of control room operators has not been mandatory in Canada.

One outcome of our study of the accident is that the AECB is reviewing the need for simulators to improve the facilities for operator training. This may result in a requirement that a suitable simulator be available for each type of CANDU reactor.

REACTOR OPERATION

One of the significant contributing factors at Three Mile Island was the fact that some plant equipment was in a degraded condition prior to the accident. For example, the fact that the pilot-operated relief valve was leaking before the accident contributed to the failure to detect that it was stuck open following the initial transient. Also, the releases of fission products were mainly due to leakage from the waste gas handling system which was impaired prior to the accident.

This suggests that careful attention should be given to the extent of degradation which can be permitted in an operating plant. The safety analyst

is wasting his time if the plant is operated in a condition such that the inputs to his analysis are wrong. This does not mean that the plant must be shut down every time a minor piece of equipment requires maintenance. However, it does imply that an envelope should be drawn, consistent with the safety analyses, within which the plant would be required to operate. This has been done in the past for special safety systems, and the AECB will be giving more attention in future to ensuring that it is done for all safety-related equipment.

PRESENTATION OF INFORMATION TO OPERATORS

It is possible to consider the Three Mile Island accident as an event caused entirely by operator error, because all the information needed by the operators to make the correct decisions was available. However, this is an oversimplification, as the designer must have a responsibility to make the design tolerant to operator errors, and to make sure that the necessary information is not only available, but is available in a clear and understandable form. If the position indicator on the relief valve had shown the actual position rather than the demanded position, it is likely that the problem would have been corrected without serious consequences.

There have been several problems in CANDU reactors caused by poor presentation of information to operators. For example, at Pickering 'A', the original design of the annunciation system was not adequate for upset conditions. More recently, at Bruce 'A', a serious impairment of a shutdown system was not detected for several shifts, largely because the indication of an unsafe, off-scale trip setpoint was almost indistinguishable from that of the correct trip setpoint.

The Three Mile Island accident emphasizes what should always have been apparent, namely that it is important to give very careful attention to presentation of accurate information to the operator in a clear, understandable form.

HEAT SINKS

While the initiating event at Three Mile Island was a loss of feedwater supplies to the steam generators, this was not the fundamental cause of the accident. Nevertheless, the accident did reaffirm the importance of the design and operation of heat sinks in power reactors, since the basic error made by the operators was allowing themselves to be distracted from what should be their most important task following any reactor shutdown, namely ensuring that there is an adequate heat sink for the decay heat.

The importance of heat sinks was of course recognized before the Three Mile Island accident. Indeed, it was a major licensing issue on the Bruce 'A' plant, and several changes to the design were required at that time. However, the accident at Three Mile Island emphasizes the importance of ensuring that there are reliable, effective, and testable emergency heat sinks available at all times, and the Atomic Energy Control Board will continue to give very careful attention to this aspect of reactor design.

CONTAINMENT

The safety feature at Three Mile Island which was most effective in preventing a large release of radioactive material was the containment system. On the other hand, the releases which did occur were largely due to failures of containment through unrecognized paths and leaking equipment. The accident therefore reaffirms the importance of containment as the last engineered line of defence, and the need to be very thorough in eliminating possible breaches or bypasses of containment.

A licensing document has now been prepared by AECB staff to specify appropriate standards for design, operation, and testing of containment systems. This document demands a more rigorous approach to ensuring that there are no unidentified weaknesses in the containment envelope, and regular testing to make sure that the integrity of containment is maintained.

SAFETY ANALYSES

Safety analyses in the past have generally been done in a conservative way, taking credit only for highly reliable safety equipment and conservatively assuming that less reliable equipment cannot be credited with mitigating the consequences of a postulated accident. The rationale for this is that the analysis must show that public safety does not depend on unreliable equipment. There is no point in building very reliable and redundant safety systems if they can be made ineffective by

failure of a single piece of equipment which is not built to high standards.

However, this approach can lead to the safety analyses giving a very distorted picture of an accident, with predictions being totally different from what would occur in a real situation. The Three Mile Island accident demonstrates this, since in the analysis of a loss of feedwater it was conservatively assumed that the pilot-operated relief valve failed to open, and no consideration was then given to its failure to close. It is now obvious that failure to open is not always the conservative assumption.

Clearly there is a need to develop methods for analyzing postulated accidents which will give a reasonable prediction of the most likely sequence of events, and also demonstrate that the equipment necessary for protection of the public is sufficiently reliable. The AECB has been examining this problem, and attempting to define an appropriate set of principles which would achieve this. We have also asked the analysts themselves to define suitable principles.

A further point relating to safety analyses is that the Three Mile Island accident has shown the importance of giving consideration to the long-term reliability, maintenance, and accessibility of equipment which must continue to operate following an accident. This is of particular importance in some CANDU reactors in which piping, in areas outside containment which are normally accessible, could contain significant quantities of radioactive material following an accident.

OPERATIONAL EXPERIENCE

If the nuclear industry in the United States had had a systematic program for evaluating experience in operating reactors prior to the Three Mile Island accident, changes might have been made following previous incidents such as the one at the Davis-Besse plant in 1977, and the Three Mile Island accident might have been avoided. The accident clearly demonstrates the necessity for ensuring that events which occur in operating reactors are carefully evaluated, and that the lessons to be learned are communicated to other operators and fed back into the design process for future reactors.

Since the accident, the nuclear industry in the United States has established a large program for reviewing operating experiences. Some excellent work has also been done by Ontario Hydro in evaluating event reports and feeding back information and recommendations. However, there is still evidence that many designers, safety analysts, and operators in this country are unaware of many of the important safety-related events which have occurred in CANDU nuclear power stations. Communication is a two-way process, and it is the responsibility of all those who are involved in the various aspects of reactor safety to keep informed about safety-related incidents and their implications. It is also important to make sure that the feedback of information is not inhibited by organizational, provincial, or international boundaries.

We can take advantage of knowledge gained from operational experiences only if the events are thoroughly reviewed to derive the important information, and if there is a good communication system to make sure that the information is fed back to people involved in all aspects of nuclear safety.

RESPONSIBILITY FOR SAFETY

One of the important points raised by the report of the Kemeny Commission related to attitudes and practices within the nuclear industry in the United States. The attitude which concerned the Commission was that satisfaction of regulatory requirements was equated with safety. Plant owners did not appear to be fulfilling their responsibility to satisfy themselves that proper standards of safety were met, but took the attitude that, if all NRC standards were met, a plant must be safe.

Clearly, there are many conscientious and dedicated people in all areas of the nuclear industry who take a responsible attitude to reactor safety. Nevertheless, the record shows that there have been occasions in Canada where important safety problems have not been dealt with expeditiously until the AECB demanded that action be taken.

It is not clear precisely when it became apparent that low pressure emergency cooling systems were not nearly as effective as they were supposed to be. It was perhaps a gradual realization starting in the early 1970's. However, nobody took the initiative to re-examine the

effectiveness of emergency cooling systems in existing plants until the AECB demanded a re-examination in 1976. Equally, no action was taken to make changes to improve the systems in existing plants, or to design more effective systems, until the AECB made it a requirement that this be done.

Another example, also related to emergency cooling systems, is the emergency cooling recovery system at Bruce 'A', which did not have a heat exchanger to reject the heat removed from the core, until it was made a requirement by the AECB.

It is interesting to note that one of the recommendations of the Kemeny Commission is very similar to one of the recommendations of the Ontario Royal Commission on Electric Power Planning. This is the recommendation that each nuclear power plant company have a separate safety group, independent from the design organization, that reports to high-level management. In my view, this is an excellent suggestion, not only for utilities but also for consultants involved in nuclear design. It is important to have people inside an organization whose prime responsibility is to determine what is necessary to make reactors safe, rather than what is necessary to obtain a licence.

Perhaps the most important lessons to be learned from the accident at Three Mile Island are that the responsibility for reactor safety must rest with the owners and designers of the reactor, and that safety cannot be achieved merely by meeting regulatory requirements.

CONCLUSION

The accident at Three Mile Island has demonstrated that the safety of nuclear reactors is not only dependent on the type of reactor or the major safety features inherent in the design. It has shown that safety depends on good design, a sound operating organization, and most of all a firm commitment to safety by all those involved in the design, operation and regulation of nuclear reactors.

REFERENCES

1) B.J. Pannell and F.R. Campbell, "Three Mile Island - A Review of the Accident and its Implications for CANDU Safety", Atomic Energy Control Board Publication INFO-0003, March, 1980.