NUREG/CR-1113
UCLA-ENG-7953

Licensability of CANDU-Type Reactors in the United States

Preliminary Assessment of the R and D Requirements

Manuscript Completed: September 1979
Date Published: August 1980

Prepared by
L. Cave

School of Engineering and Applied Science
University of California
Los Angeles, CA 90024

Prepared for
Division of Systems Integration
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN No. B3004-9

ABSTRACT

In this report an assessment is provided of the Research and Development required to establish the licensability of a CANDU-type reactor in the United States. It is shown that the bulk of the Research and Development effort would have to be devoted to establishing the integrity of the pressure tubes and the effects of a pressure tube failure on the remainder of the system.

Three possible options which could form the basis of the Research and Development program in relation to the pressure tube are defined and discussed; it is concluded that one of these options is likely to require less Research and Development than the other two. The principle underlying this option is that the pressure tubes would be shown to have a moderately low probability of sudden, gross failure and that the effects of a single failure would not lead to unacceptable consequences.

In the other areas where Research and Development work would be necessary, more of the problems would be similar to those encountered in LWRs, however, two novel problems are identified, viz:

(a) investigation of the effectiveness of the moderator as an alternative emergency cooling system in partial and total LOCA;

(b) the effect of the difference in reactor configuration (horizontal heat source) on natural circulation.

Overall, it is concluded that a relatively small amount of additional Research and Development work should be sufficient to support a license application to build a CANDU-type reactor in the United States.

SUMMARY

In assessing the Research and Development required to establish the licensability of a CANDU-type reactor in the United States, the main problems encountered relate to the integrity of the pressure tubes. There is a noticeable lack of precision in published statements on this aspect of the safety of the CANDU reactors. In order to make a comparison with the integrity of the primary circuits of the LWRs, it has been necessary to make specific assumptions concerning the importance of pressure circuit integrity in the design of a CANDU-type reactor. Three sets of assumptions have been used, which are referred to in the text as Options I, II and III; all three are based on a risk-allocation analysis for the reactor system. Options I and II represent the extreme conditions. In Option I pressure tube integrity is assumed to be all-important, so that the probability of gross failure must be shown to be below some specified value. In Option II a high probability of gross failure of one pressure tube is assumed to be permissable, but the probability of fuel meltdown in that channel or propagation to another pressure tube is made very low.

As might be expected, these extreme sets of assumptions lead to Research and Development programs which appear to present considerable difficulties. Option III was therefore formulated; it is defined as follows: "The probability of gross failure of a pressure tube is not to exceed 10^{-3} per reactor year and in the event of such a failure, the probability of propagation to more than nine other pressure tubes shall

not exceed 10^{-3} per reactor year." It should be noted that this definition implies that limited failure of pressure tubes can be accepted; beyond that limited number, the situation would be no more acceptable than catastrophic failure of an LWR pressure vessel and has to be shown to be equally improbable.

From the definition of the requirements for pressure tube integrity, the reliability required from the pressure tubes themselves, from those support systems which are directly relevant to pressure tube integrity (e.g., the leak detection system) and from those systems in which faults could lead to pressure tube failure, can be defined. The adoption of a specific set of assumptions also leads to some clarification of the performance required from some of the systems. Given this particular set of assumptions, it is also possible to establish the relative priorities of the principal items of Research and Development work which is required in relation to pressure tube integrity, so far as it affects safety. These are as follows:

(a) demonstration of a sufficiently low probability of "break-before-leak" type gross failures (10^{-6} per tube year);

(b) demonstration that the probability of propagation of gross failures is sufficiently low [Note: it is shown that quite high probabilities of propagation to one tube (about 0.5) are acceptable];

(c) demonstration that the ejection of fuel bundles, from failed tubes into a full calandria, would not cause any further damage by their fission-product heat;

(d) investigation of the probability and effects of channel stagnation; and

(e) development of methods for the detection of channel blockage.

This set of priorities is based on the set of assumptions defined in Option III, as above. Clearly many different sets of assumptions could be defined, these might require Research and Development work in other areas, or a change in the priorities.

Other results obtained in the risk-allocation analysis for the reactor system have been used to define the reliability required from the reactor protection systems (i.e., shutdown systems and decay heat removal systems). By comparison with established LWR practice, by consideration of the reliability requirements, and by some consideration of the difficulties known to have been encountered in the development of other pressure tube reactor systems, some additional items of Research and Development work (in areas other than those relating to pressure tube integrity) have been identified. These are as follows:

(a) adequacy of performance of the emergency cooling systems in LOCAs, without stagnation;

(b) effectiveness of moderator as an alternative emergency cooling system in partial and total LOCAs;

(c) adequacy of the emergency cooling system for LOCAs in which stagnation in one or more channels could occur;

(d) adequacy of natural circulation, including situations in which fuel cladding is temporarily overheated;

(e) development of alternative sensors to increase the diversity of the reactor shutdown systems; and

(f) reliability analysis to confirm that the designs of the shutdown and residual heat removal systems which are proposed will be adequate.

A safety advantage of the CANDU-type reactor, relative to the LWRs, stems from the use of on-load refueling. This necessitates a much smaller amount of surplus reactivity in normal operation, about one percent as compared with seven percent. Consequently, the potential hazards from reactivity accidents are substantially smaller.

Overall, it is concluded that a relatively small amount of additional Research and Development work would be required to support a license application for a CANDU-type of reactor, similar in design to that proposed by CE, to be built in the United States, providing that the approach to safety embodied in the choice of Option III as a basis for design is acceptable for licensing power reactors in the United States. If this approach is not acceptable, the amount of Research and Development required would be substantially increased but it is doubtful whether Option I (probability of gross failure of pressure tubes so low that it can be ignored) is a viable basis for design.

Table of Contents

Table of Contents (continued)

Table of Contents (continued)

List of Figures

List of Tables

1. INTRODUCTION

Some firming-up of US reactor vendor views on the likely design features of a CANDU-type reactor suitable for construction in the US has been provided by the recent Combustion Engineering design study. The main features of this design are described in Ref. 1, and the PSID, but little information is available about the transient behavior of the reactor.

The next important step, so far as NRC is concerned, is an evaluation of the extent of the R and D which would be required to demonstrate the suitability of the system for licensing in the U.S. It would, of course, be preferable to await more information about the transient behavior if time permitted, before attempting to define the R and D requirements. However, it is understood that this is not possible (Ref. 2).* Consequently this paper has had to be prepared on the basis of rather limited data; it has been necessary therefore to derive the R and D requirements in rather broad terms from considerations of general principles.

The acceptability of the main features of a CANDU-type reactor, for licensing in the US, have been discussed in a previous UCLA paper (Ref. 3). In that paper it was pointed out that it was desirable to define as closely as possible the standard of safety which had to be met. However, on the time scale now required, this is clearly impossible. A simple comparative approach has therefore been adopted in this paper, as described in the following section.

*Private communication, Dr. T. P. Speis (NRC) - L. Cave (UCLA), January 17, 1979.

The main outcome of the study described in this paper is to add emphasis to the need for R and D work to resolve the questions of the role of pressure-tube integrity in relation to the safety of this type of reactor.

A major difficulty which has been considered in this evaluation is that there has been no definitive statement concerning the possible effects of a pressure tube failure in either a CANDU reactor or in the CE design for a CANDU-type reactor. Two possible options, which represent the opposite extremes in the treatment of pressure tube integrity, have therefore been identified and the R and D requirements to meet each of these have been examined. These two options are as follows:

Option I. To show that the probability of gross failure of a pressure tube can be made so low that the consequences of such an event can be ignored.

Option II. To show that gross failure of a pressure tube is so unlikely to lead to meltdown of fuel in the parent channel, or to failure of other pressure tubes, that a relatively high probability of gross failure of a single tube would be acceptable.

Adoption of either of these extreme options would require extensive R and D work. If Option I were adopted, the work would have to include extensive seismic analysis of the pressure tubes. In practice, some compromise between these two options is likely to be desirable, and a possible approach is identified which is likely to require less R & D work than either I or II alone.

By comparison with the pressure-tube problem, the other potential causes of licensing difficulties identified in the previous UCLA work (Ref 3) should require relatively little R and D work; although they could have a significant effect on the economic viability of the reactor system in the U.S.

2. SUITABILITY OF THE CANDU-TYPE REACTOR SYSTEM FOR LICENSING IN THE US

2.1 Basis of Evaluation

Given that the overall objective is that CANDU should not be less safe than LWR's, the most satisfactory approach would be to evaluate the safety of a representative unit of the CANDU-type relative to the LWR, by means of quantitative risk assessments on the lines of WASH-1400 (Ref. 4). However, two difficulties would arise if this approach were adopted at the present time, viz: -

(a) There is not a sufficiently well-described CANDU, or CANDU-type design, available in the U.S. to provide the necessary basis for a risk assessment.

(b) At the present time (mid-1979) there is a controversy as to the feasibility of estimating reactor risks, in absolute terms, with a sufficiently high degree of certainty for the results to be meaningful. Although a relative assessment should reduce the importance of some of the uncertainties, it is not clear that the remaining uncertainty would be small enough to satisfy the critics of this approach.

In these circumstances, the best alternative appears to be a comparison on a system-by-system basis, considering the major potential faults associated with each. From this comparison it should be possible, on the basis of subjective judgment, to decide whether the potential advantages which the CANDU-type might have in some respects are sufficient to offset possible disadvantages in others.

In some areas of the design, as described below, it is possible to make the comparison, at a system level, on a semi-quantitative basis. To facilitate the comparison the reliabilities required from the various protection systems of the CANDU-type reactor have been estimated by means of a "risk allocation analysis", which is described in Appendix 1.

In the CANDU-type of reactor, the proximity of the fuel to the pressure circuit is an additional potential source of failure of the primary coolant loop; due to this proximity, a transient leading to local overheating of the fuel could cause failure of the associated pressure tube, with its potentially serious consequences to the reactor as a whole, whereas the same incident in an LWR would be much more likely to remain localized. Thus errors in the prediction of transient behavior are likely to be more serious than in an LWR.

2.2 Comparison of Systems

The comparison at the system level has been made by considering the following aspects of LWRs and CANDU-type reactors:

(a) Structural integrity of primary coolant circuit

(b) Response of reactor to loss of primary coolant-flow accidents

(c) Response of reactor to loss of primary coolant accidents

(d) Reliability of shut-down systems, in relation to relative frequency of demand, and response to ATWS

(e) Response of reactor to secondary coolant faults

(f) Effects of fuel handling faults.

In general, for the items in the above list, there are major differences between the reactor types only in relation to items (a) and (f). For the others it is possible to visualize designs in which the effectiveness and reliability of the safety systems for the CANDU-type reactor match those currently required for LWR's in the US; in fact the CE design addresses this aspect. However, without the aid of detailed fault studies it is not possible to decide whether the performance of the various systems in the CE design, as presently visualized, would be adequate. For example, the positive void coefficient of the CANDU leads to a less favorable initial response in the early stages of a large LOCA; in order to meet the current

US criteria this might necessitate a quicker-acting shutdown system and/or a more powerful injection system. These additional requirements should not present feasibility problems, but they could add significantly to the cost of the system. Moreover, additional R & D requirements could arise, such as the development of more powerful computer codes than those used for CANDU and experimental work (e.g., blowdown and re-flood tests) on models which simulate the CE design to support the codes.

In the case of Item (a), structural integrity of primary coolant circuit - the evaluation of the relative safety of the pressure vessel of the LWR and the pressure tubes of the CANDU-type presents considerable difficulty. Consequently the greater part of this report is directed to this aspect of the comparison. This evaluation does, however, involve some consideration of the reactor's transient behavior.

2.3 Effect of Lack of Data on Comparative Study of Primary Pressure Circuit Integrity

As noted above, the absence of detailed fault studies leads to difficulties, even in a qualitative comparison of the systems. One of the major difficulties encountered is the lack of information about the subsequent sequence of events following the sudden failure of a pressure tube. This aspect of the design is central to the evaluation but it has not been possible to find a definitive statement, supported by detailed argument, as to the significance of pressure-tube failures in relation to safety. In a relatively recent paper (Ref. 5) which reviewed the significance of the pressure-tube leakages in the Pickering reactors (see Sec. 4.3 below) the following statement appears:

> " SAFETY IMPLICATIONS
>
> The CANDU reactor has been designed so that the failure of a pressure tube will not endanger plant staff or the public. An exhaustive investigation into the development of these cracks has given us confidence that they will not cause a pressure tube to rupture before it

leaks. In all cases, the leakage from cracked pressure tubes has been confined within the annulus gas system, and has been quickly detected. Therefore, we do not anticipate even the limited consequences of a single tube failure."

In a more recent paper (Ref. 6), which provides a seemingly definitive review of the safety of pressure tube reactors, it is stated that "experiments.. have shown that pressure tube failures will not propagate to other tubes nor compromise overall calandria integrity."

However, as discussed in Section 6.1 below, the available evidence does not appear to support these statements sufficiently to ignore the possibility of severe sequential damage.

In these circumstances it has been necessary, therfore, to proceed on the basis that either "Option I" or Option II", as defined in Sec. I, above, might be adopted. Alternatively, the difficulties arising from the apparent lack of data might be overcome more readily (e.g., in terms of lower R and D costs) by a compromise solution. This possibility has also been examined and has, in fact, been found to be a more satisfactory approach to the problem.

3. COMPARISON OF THE STRUCTURAL INTEGRITY OF A CANDU-TYPE PRESSURE CIRCUIT WITH THAT OF LWRs.

So far as the pipework outside the vessel of an LWR and that outside the core region of a CANDU-type is concerned, there is no need for a detailed comparison, since both reactor types are designed on the premise that failure of any pipe must be catered for.

The probability of catastrophic failure of LWR pressure vessels is widely believed to be in the range 10^{-6} to 10^{-7} per reactor year (Ref. 7). Thus in order to adopt Option I, as defined above, it would be necessary to show that the probability of a gross failure in the set of pressure tubes was also in the range 10^{-6} to 10^{-7} per reactor year.

However, in the case of the CE design for a 1200 MW(e) reactor, there are approximately 700 pressure tubes: Thus, for faults which originate from the tubes themselves, the maximum acceptable failure rate per tube year must be less than 10^{-9}, to meet the proposed target. This aspect is discussed in more detail in App. I. Even for the simplest pressure-retaining envelope, in a well-defined and well-understood environment, it would be a formidable problem to show that this degree of reliability was attainable, e.g., for carbon steel pipe work an approximate rule-of-thumb suggests a failure rate of 10^{-7} per ft. run. As the CANDU-type pressure tubes are about 20 ft. long, it is necessary to demonstrate a failure rate which is better than that for conventional pipe work by a factor of 10^4, or more. For reactor vessels, on the other hand, the factor of improvement over conventional vessels which is required is between 10^2 and 10^3.

The possibility of demonstrating adequate reliability in the pressure-tubes is discussed in the following Section and it is shown that it could be a difficult task. Thus, although Option I provides an attractive and easily understood basis for design, it is desirable at this stage to examine the possible alternatives. Option II, as defined in Sec. 1, above, might be regarded as a "counsel of perfection" since it should result in a negligible release of activity to the environment, even though it might lead to a prolonged shutdown of the reactor. However, this approach presents two main difficulties, viz:

- Firstly, it is difficult to predict the behavior of the reactor subsequent to a gross failure of a pressure tube; there is no analysis of such an event, for a CANDU reactor, in the published literature nor is it discussed in the PSID for the CE design.
- Secondly, it is difficult to estimate with confidence the probability that the initial failure would not propagate to adjacent tubes.

Taken together these two sources of uncertainty would probably necessitate an R & D program comparable in scope and difficulty to that which would be necessary to demonstrate the viability of Option I. However, since the fundamental requirement is to establish that the CANDU-type reactor is at least as safe as PWR's, it is possible to consider an alternative option, which is based on the premise that at some low level of probability, meltdown of a few channels, if fully contained, would not be an unacceptable accident for a reactor sited in the US. It might be considered that in the aftermath of 3 Mile Island, this approach would not be feasible. However, the general concept of "comparability of safety" should still apply. Thus, providing that it could be demonstrated that the consequences of such an accident were no greater than those due to gross failure of an LWR vessel, then it should be sufficient to show that the probability of this type of accident in the CANDU-type reactor was no greater than that of gross failure of an LWR pressure vessel.

If this option were viable and were adopted it would then be necessary to determine the effect of failure of several pressure tubes, instead of only one, as required in Option II. However, it would not be necessary to show that the probability of propagation of failure to even a single additional tube was extremely low since, as shown quantitatively in Appendix 2, it is a characteristic of an array of pressure tubes that, if the probability of propagation to a single tube is a little less than unity, the probability of propagation to a large number of tubes is extremely low. Consequently this alternative option should require much less R and D work in relation to propagation than would Option II, and the amount of R and D work needed in relation to the effects of tube failure on the fuel in the affected channels might be little more than that required on the same problem in Option II. Clearly, if this were the case, the total amount of R and D work required

would be diminished.

Before continuing to explore the possibilities of this alternative option, which will be refered to subsequently in this paper as Option III, it is desirable to examine in more detail the problems associated with adopting Option I or Option II, in order to define the bounds. These problems are discussed in Secs 4, 5 and 6 below.

4. THE PROBLEM OF DEMONSTRATING ADEQUATE PRESSURE TUBE INTEGRITY FOR OPTION I

4.1 The Importance of the "leak-before-break" concept

For the CANDU reactors, the approach adopted has been that gross failure of a pressure-tube would be preceded by leakage, which could be detected in ample time to shut the reactor down, so that the defective tube could be replaced as envisaged in the overall design of the reactor. An implicit assumption is also made that gross failures could only occur as a result of some slowly-developing defect, e.g., a crack overlooked in manufacture. It could be argued that with care in manufacture, including the inspection phase, and with some measure of in-service inspection, the probability of any particular tube developing a leak which would terminate in a gross failure should not exceed 10^{-5} per tube year. With this premise, together with the assumption that all potential gross failures would be preceded by a leaking phase, it would then be sufficient to provide a leakage detection system with a failure rate lower than 10^{-4} per demand, in order to meet the overall target of 10^{-9} per tube year which was suggested in the previous section. However, as shown in Sec. 4.2 and 4.3 below, the maximum permissible failure rate may be substantially less than this. Nevertheless, putting this difficulty aside temporarily, the leak-before-break approach is open to criticism on four other grounds, viz:

(a) The reliability required from the leak detection system may be difficult to attain, particularly as some measure of operator

action would probably be necessary (see Section 4.2 below).

(b) The operating record to date for reactors embodying zirconium pressure tubes does not justify the assumption that the incidence of leaks capable of terminating in gross failure is as low as 10^{-5} per tube year. (see Section 4.3 below)

(c) The premise that gross failure (due to an inherent defect) would always be preceded by a detectable leak is only valid if:

(i) The fracture mechanics analysis is valid for all the loading conditions and initiating defects which can be expected.

(ii) The properties of the material are adequately known, taking into account all foreseeable environmental effects, such as irradiation damage and hydride formation, singly and in combination.

From the information currently available, it is not possible to judge definitely whether or not these requirements are met, but on general grounds, there are reasons for disbelief. (see Section 4.4 below)

(d) There are conceivable mechanisms which could lead to pressure tube failure in service, irrespective of the quality of the tubes themselves. In this context, any situation which could lead to local overheating of a pressure-tube should be regarded as a potential cause of tube failure.

For example:

(i) partial blockage of the tube

(ii) local distortion, or more general collapse, of a fuel "bundle" due to defects in the bundle concerned (see Section 4.5 below)

(iii) sagging of pressure tubes and/or distortion of fuel bundles due to reactor transients (see Section 4.5 below).

In the case of these failure mechanisms also, there is little information of a formal nature available but there are some data in the open literature and by private communication. It should be noted that in cases where the initiating event is not attributable to the tubes themselves, the acceptable probability of that event is, as a rule, independent of the number of tubes (see App. 1). Nevertheless, in view of the extremely low probability of failure which is admissible, it is doubtful whether the information currently available about these "external" causes of failure is sufficient. (see Section 4.5 below)

The inter-relation between the various modes of failure is shown in the fault tree of Fig. 1. Some indicative values for the maximum acceptable probabilities of failure are also shown in the Figure, which would be compatible with an overall probability of gross, and unexpected, failure of 10^{-6} per reactor year.

4.2 Reliability required from the leak detection system

In general terms the reliability required from the leak detection system, u, can be defined as a failure rate per demand not exceeding

$$\frac{a\ P_T}{n\ f_F} \quad , \text{ or } \quad \frac{\text{(Target allocated to "leak-before-break" failure)}}{\text{(Number of tubes) (freq. of "leak-before-break" failures)}}$$

where

"P_T" is the maximum acceptable probability of gross failure per reactor year due to all causes,

"a" is the fraction of "P_T" allocated to gross failures due to causes which should give "leak-before-break' indications

"f_F" is the expected frequency of incipient gross failures, due to latent or inherent defects, which lead to a "leak-before-break" situation

"n" is the number of pressure tubes, ($n \sim 10^3$).

Thus, if a value of 1×10^{-6} per reactor year is assumed for P_T, as discussed in Sec. 3 above, and 10 percent of this value were allocated to "leak-before-break" failures as discussed in Appendix I, we would have

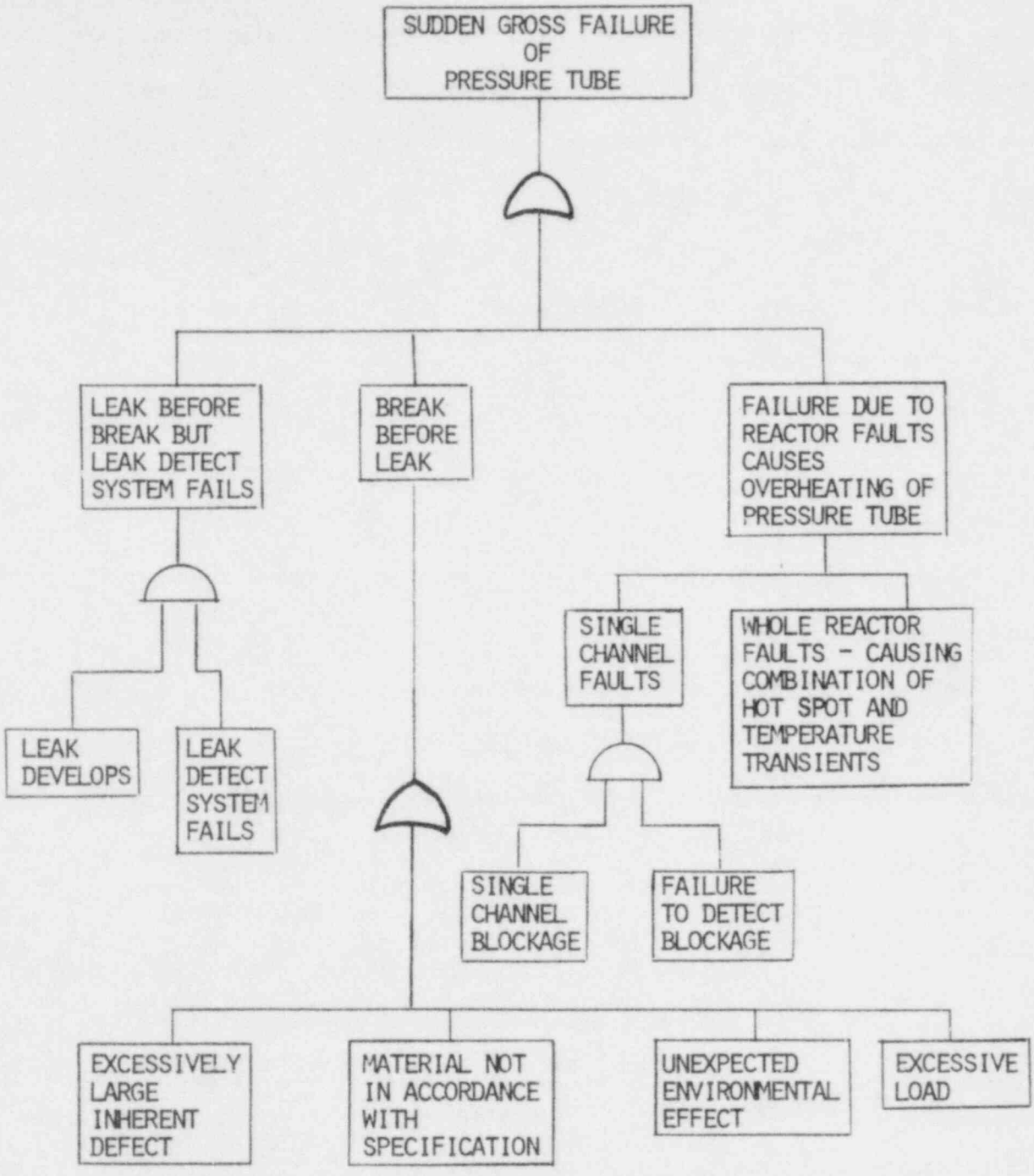

Figure 1. Fault Tree for Sudden, Gross Failure of Pressure Tube [for option I, probability of failure by propagation is $<< 1 \times 10^{-7}$ per r. year, by definition]

$$u = \frac{1 \times 10^{-10}}{f_F}$$

As discussed in Sec. 4.1 above, it can be argued that f_F should be about 1×10^{-5} per year, so that 'u' would be 1×10^{-5} but, for the reasons outlined below, this assumption may be difficult to validate in practice. However, the assumption is retained in the following discussion of the reliability required from the leak detection system.

With these assumptions, we need to consider the feasibility of providing a detection system which has a failure rate of about 1×10^{-5} per demand to deal with random defects in the tubes. The problems introduced by type-faults (i.e., those due to errors in design or fabrication which effect a large proportion of the tubes) are discussed in the next section.

It is understood (Ref. 8) that in the parent CANDU design, a single moisture detection system is provided for routine operation which is used once per 8-hour-shift during the early years of service operation but may be used less frequently in later years.* The system consists of a manifolded arrangement which enables the operator to examine all the pressure-tube/calandria-tube interspaces for moisture in a single operation. If indications of moisture content above some pre-determined level are obtained, a complete scan of the individual channels is carried out. It is understood (Ref. 9) that during refuelling an acoustic monitor is also used in the channel being refuelled, and that gross leaks should be detected by a rise in the radioactivity of the gas in the space between the pressure and calandria tubes. **

Without details of the design of the moisture detection system, it is difficult to comment on the feasibility of attaining a reliability in the range deduced above, but there are some obvious difficulties, if

*Private communication, Dr. J. Long (NRC) - L. Cave (UCLA), January 26, 1979.
**Private communication, Dr. J. Van Erp (ANL) - L. Cave (UCLA), January 19, 1979.

detection depends mainly on a single system. For example:

(a) Both the sensing and indicating parts of the system may be subject to unsafe failures which are not readily detected by the operator.

(b) The pipe-run to the bulk-sample manifold may be routed so that, in the event of failure, a sample of air is drawn in from a region in which the air is usually dry.

(c) The reliability is dependent partly on the operator. At the probability level which is of interest, operator errors could range from incorrect procedures in carrying out the test, or in interpretation of the information obtained, to ignoring results indicative of a leak or omitting the test altogether.

However, since Canada has been one of the pioneers in the application of reliability analysis, it is likely that the moisture detection system, together with the possible backup system, has been thoroughly examined from the reliability point of view, possibly with a similar maximum acceptable failure rate in mind, and that the system and method of operation have been shown to be satisfactory.

Thus an important part of the next phase of evaluation would be the review of any existing reliability analysis of the leak detection system, including the effect of possible operator errors, in the light of the reliability requirements identified above, if Option I were adopted.

If the assumptions stated above are correct, an important factor in this reliability analysis would be the rate of crack growth after a through-crack (i.e., one leading to a detectable leak) had developed, since this would determine the time available to detect the leak before the crack reached a critical length, e.g., if this were several weeks, there should be a good chance that unrevealed defects in the monitoring equipment would be remedied in the course of routine maintenance. The

rate of growth should be predictable, subject to certain reservations discussed in Section 4.4 below, from fracture mechanics analysis.

It should be noted that, if it can be shown that pressure tube failure would not lead to any significant damage to the rest of the core, the need for a detailed reliability analysis of the leak detection system would be reduced greatly. In these circumstances the reliability required would be determined mainly by economic considerations. However, if a very high reliability for leak detection were required, it might prove necessary to develop a diverse backup system, e.g., a system capable of detecting the sound (at audible or ultra sonic frequency) produced by the escape of high pressure steam from the leak, against background noises (e.g., the coolant circulating pumps).

4.3 Reliability of Zr Pressure Tubes as Indicated by Operating Experience

The accumulated operating experience with Zr pressure tubes in the Canadian HWR, amounts to about 10,000 pressure tube years, but no tubes have been operating under representative conditions for more than 10 years and some 80 percent of the operating experience has been gained with tubes which have been in service for less than 8 years; no tubes made from Zr, 2½ Nb have been in service for more than 8 years.

In this population there have been no sudden, gross failures of pressure tubes. Thus a simplistic interpretation of the data is that the probability of such a failure is less than 1×10^{-4} per tube year, at the 50 percent confidence limit. However, it would be more realistic to qualify this interpretation by the rider that this rate has only been demonstrated for tubes in the first 8 years of life. The corresponding 99 percent confidence limit is about 6×10^{-4} per tube year.

The operating experience has been less favorable in terms of the

development of defects which have been detected and rectified before they could reach a potentially dangerous size but which, it appears, required the leak detection system to function correctly. The principal defect of this type which has been reported is that of cracking at the rolled joints between the Zr, 2½ Nb pressure tubes and the end-fittings in the Pickering reactors. These failures have been described in the open literature (Ref. 5 and 10). Although they have not yet been explained fully in metallurgical terms (see Sec. 4.4 below) it can reasonably be argued that the failures were due to a combination of high residual stresses in the material (stemming from an error in fabrication) and the inherent properties of the material.

It is not entirely clear from the information currently available whether it can be argued that a crack in a pressure tube at the rolled joint would not propagate in a potentially dangerous manner. As described in the next section, the difficulties of predicting the behavior of a crack in this region appear to be very much greater than in the plain section of the tube. Consequently, any general argument to show that cracks in this region would not be potentially dangerous would be of considerable help in formulating a satisfactory safety case. For example, as argued in Ref. 10, it is possible that local design details would make the defects innocuous. Nevertheless, in that argument, the possibility of the crack "running" into the plain portion of the pressure tube is not discussed.

However, it is necessary at this stage to take the conservative view that cracks in the region of the rolled joint are a potential cause of faults which could escalate to core meltdown. It is necessary to consider, therefore, how type-faults of this nature should be treated when estimating the significance of the operating experience in relation to a probabilistic

analysis of safety. The problem is discussed in Appendix 1, where it is shown that it would be prudent to assume that the frequency of the demand for leak detection due to this cause is about 0.1 per reactor year and that the maximum acceptable unreliability of the leak detection system is 10^{-6} per demand.

Thus, the operating experience indicates that a rather higher reliability is required from the leak detection system than would be predicted from the assumption that the random failure rate of pressure tubes is not more than 10^{-5} per tube year.

A further important feature of the operating experience is the unexpectedly large axial and diametrical growth of the pressure-tubes in several of the CANDU reactors (Ref. 11). It is apparently acknowledged by the designers that this is probably due to some unknown factor in the fabrication process. The implications of this unexpected growth on the "leak-before-break" concept are discussed in the next Section.

So far as the present writer is aware, there have been no other occurrences in operation which reflect on the reliability of the pressure tubes in CANDU reactors but it would be advisable to confirm (e.g., by a direct approach to the Canadian regulatory body) that this is, in fact, the case. However, some relevant experience was obtained during the construction of the Fugen reactor (Ref. 12). This is discussed in the next section.

4.4 Validity of the "leak-before-break" concept for Zr pressure tubes

The validity of the "leak-before-break" concept depends largely on the fracture-toughness of the material, together with the shape, size and location of the initial flaw or flaws, since these factors determine whether the crack can grow to a critical length before it becomes a through crack. Prediction of critical crack length, and rate of crack

growth, is more difficult in complicated sections such as the rolled joints.

If the materials properties are in accordance with design, the minimum size of initial flaw should be so large that the probability of failing to detect it during inspection should be low. Nevertheless, uncertainty about the effect of pressure-tube failure may require the probability of gross failure, due to defects leading to "break-before-leak", to be less than 10^{-9} per tube year, as discussed in App. 1. This would be considerably below the probability level at which reliance could be placed on non-destructive testing in manufacture, due to common-mode faults in the inspection process. For example, one author (Ref. 13), as the result of a questionnaire to the UK industry, has estimated the probability of missing a 2 in. crack in a thick steel vessel to be as high as 10^{-2}. This difficulty could be overcome to some extent by a completely independent inspection at a later stage (e.g., on completion of construction, so that any damage sustained during erection might also be found) and frequent in-service inspection.

Given that the tubes, as erected, are free from initiating flaws which could give "break-before-leak" with material having the properties assumed in the fracture mechanics analysis, it would also be necessary to ensure that the properties were, in fact, within the specification and would remain so. Some factors that could be encountered in practice during manufacture are:

(a) Original ingot not to specification

(b) Heat treatment incorrect

(c) Incorrect fabrication techniques (as at Pickering and Fugen).

As in the case of non-destructive testing, the acceptable probability levels are so low that it is difficult to believe that they would be

attainable in commercial practice. Moreover these types of defects would be much more difficult to detect after fabrication than would over-size initiating flaws.

During service, the main factors which could effect the fracture toughness of the material are:

(i) Irradiation

(ii) Excessive hydrogen pick-up

(iii) Other contaminants in the coolant or in the annular space gas (e.g., radiolytic oxygen, trace impurities in primary coolant or annular space gas).

There are also possibilities of synergistic effects between these three factors. It should be noted also that there is a possibility of stress corrosion in zirconium alloys, which could lead to a radically different type of initiating flaw.

Reference 5 provides some indication of the practical difficulties of controlling factors of this type in relation to delayed hydrogen cracking which were revealed by the investigation of the cracks in the Pickering tubes. For example, it is stated (p. 6) that the "back" ends of the pressure tube extrusions "have a finer grain structure and higher strength and are apparently more susceptible to delayed hydrogen cracking" and later (p. 8) the following statement appears:

"MANUFACTURING BATCH EFFECT

> It has become apparent that some batches of tubes have a greater tendency to crack than others. Statistical analysis of the results indicates that this is related to the ingot, and intensive investigations have been carried out to determine the actual cause. At the time of writing this report, it is believed that variations in the oxygen content of the tube is a major contributing factor. Our objective is to isolate the basic cause of this batch effect, to eliminate it from new tubes now being produced, and to reject any existing tubes with this deficiency."

and the authors conclude (p 8)

> "In this paper we have reviewed our current knowledge of this problem. Many programs are now proceeding and we expect to understand this phenomenon more closely in several years."

In addition to the metallurgical factors noted above, the stress levels in the tube are of importance; in Ref. 5 it is stated (p 7) that

> "Improper alignment between the tube wall and the end fitting bore also causes high stresses. Such misalignment may be due to machining tolerances or distortion of the reactor end shields, by improper alignment of the rolling bench used in preassembling one end fitting and the pressure tube, or by component variations (particularly the straightness of the tube end). Tooling is being developed to check and correct this alignment."

Thus, with care in fabrication, this difficulty can be avoided but it must represent a further potential source of trouble, particularly as the critical crack length tends to diminish with increasing stress. Clearly, to quantify the uncertainties of the type described above, is virtually impossible in our present state of knowledge, but the existence of these uncertainties emphasizes the practical difficulties which would be encountered if Option I were adopted.

Potential defects were also found in the ends of the Fugen pressure tubes, which are fitted with rolled-joint end pieces similar to those in CANDU. In the Fugen case, after a special inspection undertaken because of the Pickering experience, it was found that the residual stresses in the lower rolled joints were higher than expected by a factor of 2.5. (35 tons per sq. in., instead of 14 t.p.s.i.), although it is stated "rolling operations (had) progressed at the factory, under highest quality control". (Ref 12)

The difficulties presented by the uncertainties in the materials data in estimating theoretically the probability of pressure vessel failure are discussed in Ref. 13. In the analysis of a PWR vessel which is described in that paper, various simplifying assumptions have had to be made in order to obtain a solution.

The incompleteness of the available knowledge about the pressure tube material is also illustrated by Ref. 5; in discussing the problems presented by the Pickering failures it is stated (p 14) that:

> "It should be noted that the cracking of cold-worked Zr2.5 wt Nb tubes does not occur easily. Although cracking by delayed hydrogen embrittlement has been reproduced in small test specimens, numerous attempts to reproduce the cracking and leaking of over-extended joints in the laboratory have failed. The right combination of stress, metallurgical factors and operating conditions has not yet been found"

....and yet this combination occurred accidentally in the Pickering reactors.

Lastly, it should be noted that the unexpectedly high rates of axial and diametral growth of the pressure tubes in Pickering & Bruce, referred to in Sec. 4.3 above, are indicative of additional uncertainties about the effects of age and environment on the material properties which detract from the validity of the "leak-before-break" concept and thus make it still more difficult to adopt Option I.

4.5 Effect of Reactor Transient Behavior on the Integrity of the Pressure Tubes.

It is necessary to consider three different types of effect, viz., (a) Increase in stress levels generally, due for example to overpressurization, thermal effects and seismic disturbances, (b) Local overheating of pressure tubes and (c) High local stresses in special circumstances, such as the effect of seismic forces on a pressure tube which is being refuelled.

The first type of effect represents the addition of a limited number of large, low-cycle, fatigue stresses which may be of considerable importance in relation to the rate of crack-growth. This should only proceed slowly in response to the high cycle, low strain, situation usually encountered in normal operation but it would be accelerated substantially by a few high stress cycles.

In the extreme case, of course, a single large cycle could precipitate failure, but unless this occurs there would be an opportunity for the operator

to detect a leak and to take remedial action.

At the low levels of failure probability which would be required if Option I were adopted, it is likely that the second type of effect would be of greater importance since, owing to the proximity of the fuel to the pressure boundary, there is the possibility that the temperature of the pressure wall may increase sufficiently to reduce the ultimate stress of the material to a level at which ductile failure occurs.

In this respect, two broad classes of transient must be considered:

(i) Those in which only one, or a few, channels are affected

(ii) Those which affect the reactor as a whole.

In the first class of transients, the following possibilities would need to be considered.

Break up of fuel bundle, leading to a concentration of fuel rods in close proximity to the channel wall

Blockage of a channel by debris

Presence of a bundle with incorrect enrichment

Asymmetric reactivity faults.

To date the experience with CANDU fuel has been good (about 0.03% defective rods in a population of some 3×10^6) and the majority of the defects are readily explainable (Ref. 14). Nevertheless, at the level of probability which would be of interest, it would be necessary to consider the effects of highly unlikely failures, such as failure of the end-plate welds due to manufacturing defects, which could lead to the collapse of a fuel bundle. Whether or not this could lead to failure of a pressure tube before the operator could become aware of the condition is not clear.

Blockage of channels has been recognized as a potential source of hazard in many types of reactors, and precautions are taken in design to prevent it, e.g., by the provision of "lantern" features at the inlets to

channels. In the case of a pressure tube reactor the effects of channel blockage are potentially more serious than in a vessel type, but the scope for design features to prevent it would seem to be more limited, since each channel is fed directly from a manifold, via a separate "feeder" pipe, instead of from a sizeable plenum chamber. Thus, although in the CE design the equivalent of a "lantern" is proposed to protect the channel inlet, there appears to be less protection against blockage of its "feeder" pipe by large pieces of debris left in the circuit during maintenance.

It is understood (Ref. 7) that in the CANDU design there is sufficient instrumentation in each channel to detect a potentially dangerous blockage (2 continuously monitored temperature detectors and channel pressure drop, on demand). Since there have already been at least 3 incidents of channel blockage leading to core meltdown in commercial or demonstration power reactors (Fermi 1 (US); St. Laurent 1 (France) and Chapel Cross 4 (UK)); the frequency of such events cannot be assumed to be extremely small. Consequently detailed reliability analysis of the system for detecting blockage, in time to prevent damage to the pressure tube, would be necessary if Option I were adopted.

At the level of failure probability which would be of interest if Option I were adopted, seemingly bizarre events, such as the fabrication of fuel bundles with excessive enrichment, cannot be excluded. It is not clear that the instrumentation would necessarily detect the presence of such a bundle; it seems more likely that the channel rating would be lowered slightly by the automatic control system. However, in a severe transient the "rogue" bundle could experience a much larger rise in clad temperature than the rest. Further investigation is necessary to determine whether this type of event presents a significant problem.

In a reactor system such as CANDU, the possibility of xenon

instabilities, together with the provision of a sector control system to combat them, introduces the possibility of quite severe asymmetric reactivity faults. These have been a cause of considerable concern in the UK magnox reactors and have necessitated the provision of additional sensors for the reactor shutdown systems. It is not known whether the CANDU reactors are adequately protected against faults of this type.

In the case of transients which affect the whole of the core (or one half in the case of LOCA,) the situation seems to be potentially more serious for a CANDU type reactor than for an LWR, since a fault which could lead to clad melting and "slumping" of the more highly rated fuel bundles appears to present a direct threat to the integrity of the pressure boundary, whereas this would not be the case in an LWR unless the fault escalated to a level at which a substantial proportion of the fuel melted, in addition to the cladding. This aspect is discussed further in Section 6 below; it is sufficient for our present purpose to note that this class of transient may also be a significant contributor to the probability of gross failure of pressure tubes and that it may be difficult to reduce their contribution to a level at which it would be possible to adopt OptionI.

The possible effects of reactor transients, originating elsewhere in the system, on the integrity of the pressure tubes demonstrate the greater vulnerability of the pressure-tube reactor in this respect, as compared with pressure vessel reactors. As discussed in Sec. 6, below, the horizontal arrangement of the pressure tubes in the CANDU-type reactors, combined with vertical tubes for other purposes,appears to increase slightly the dependence of the system's safety on the continued integrity of the pressure-tubes, as compared with an arrangement in which all the tubes are vertical.

In the CANDU-type of reactor, refuelling is carried out on load and necessitates connecting the ends of the pressure tube being refuelled to

large, heavy charge and discharge machines, which are not otherwise connected to the reactor vault or calandria. Thus the integrity of the pressure tube/machine connections in seismic conditions presents special problems. These are discussed in Sec. 6.4.

4.6 An Interpretation of Canadian Experience with Zr Pressure Tubes in Commercial Reactors.

Since the CANDU reactors are designed so that defective pressure tubes can be replaced at any time during the reactor's life, it can be argued that the incidence of failures encountered so far is acceptable on economic grounds. Moreover, in view of the relatively limited experience with zirconium in this application, particularly with Zr-2 1/2 Nb, it is not surprising that some difficulties have arisen, but with further experience the incidence of failures should decrease. However, the extracts from the Canadian papers quoted above, together with the reference to Japanese experience, demonstrate that a large amount of R and D is still required to obtain sufficient understanding of the behavior of Zr-2 1/2 Nb, in a reactor environment, to ensure that all the factors in manufacture and operation which could lead to failure are adequately controlled.

Nevertheless, it could be argued on the basis of CANDU experience that, if economic considerations alone had to be considered, it would be possible to embark on a program of commercial CANDU-type reactors in the US at the present time. However, it would appear to be over-optimistic to assume that the reactors could be demonstrated to be adequately safe on the basis of an "Option I" type of argument.

The extent of the R&D on pressure tube technology required to proceed on the basis of Option I is outlined in the next section but a considerable amount of subjective judgement would be required in deciding whether or not

the requirements had been met. Further discussion of the R and D required to support the adoption of Option I is also contained in Sec. 6.2 below.

5. OUTLINE OF R AND D REQUIRED ON PRESSURE TUBE TECHNOLOGY TO SUPPORT OPTION I.

5.1 Review of Previous Work

A substantial amount of work on zirconium alloys (include Zr 2 and Zr-2 1/2 Nb) was carried out in the U.S. prior to 1968 and in the UK up to 1976; some work continues in Italy and Japan. However, presumably considerably more has been done in Canada than elsewhere. It would therefore be desirable to develop a collaborative program with Canada in order to avoid unnecessary duplication.

A collaborative program could presumably provide access to all the Canadian work on pressure tubes. Thus the first step in the U.S. program could be a complete review of previous work in Canada, U.S. and, if possible, in other countries, such as Italy, Japan and UK. A review of this nature, if carried out in a critical fashion, might show how errors in interpretation of experimental data had occurred that led to the incorrect estimate of growth in the Pickering and Bruce reactor tubes, referred to above.

5.2 Material Properties

It appears inevitable that extensive additional work would be required on material properties of selected Zirconium alloys in the following areas:

(i) Effects of ingot manufacturing methods and fabrication methods.

(ii) Effects of initial hydrogen content and pick-up of hydrogen in service.

(iii) Effect of initial oxygen content and of pick-up in service.

(iv) Effects of irradiation.

(v) Effects of contaminants likely to be encountered in service.

(vi) Combined effect of creep and fatigue.

(vii) Synergistic effect of (i) through (vi).

5.3 Fracture Mechanics

As a means of bounding the materials R and D work, the fracture mechanics analyses could usefully be extended to determine the effects of uncertainty in the materials data on the probability of "break-before-leak" and of the numbers of "service" cycles of various types between "leak" and "break", for situations in which "leak-before-break" type of failure is expected.

This work should also include the effects of uncertainties in stress, particularly in complicated sections such as the rolled joints, and of flaw size and shape.

5.4 Effects of Conditions to be Expected in Service

The effects of possible operational conditions, such as local overheating of a tube, can be examined on a generic basis in the first instance, both theoretically and experimentally. As conceptual designs are developed, the effects of a complete range of operating conditions can then be predicted with more certainty.

This part of the work should include the effects of seismic forces and should extend to cover situations in which one pressure tube is connected to the charge and discharge machines at the time of the earthquake.

A further aspect of a generic nature in this area is the effect of improving, to U.S. standards, the protection against pipe-whip in the large runs of relatively small pipes. There may be a fundamental difficulty in providing sufficient restraint for this purpose and yet accommodating the thermal movements of the pressure tubes, and other pipework, in transient conditions. If the thermal stresses become excessive this could effect the prediction of critical crack length and of crack growth.

5.5 Development of Inspection Methods

In order to meet the reliability requirements implicit in the adoption of Option I, improvements in methods of inspecting pressure tubes for incipient cracks would be desirable, particularly for use in In-Service Inspection procedures.

5.6 Leak Detection Methods

It follows from the previous discussion (Secs. 4.2 and 4.3 above) that a review of the reliability of methods already in use in the CANDU reactors would be necessary.

It is likely that the development of alternative systems would also be desirable, if not essential, in order to improve reliability by increased diversity.

5.7 Transient Behavior of Reactor

The transient behavior of the CANDU-type reactor is a possible cause of pressure tube failure. Discussion of the R and D work required to confirm the theoretical transient analyses is deferred to a later part of this paper (Sec. 8), as it is necessary to examine the major differences between LWR and CANDU-type reactors in this respect.

5.8 Depth of R and D Work Required

In assessing the cost of the R and D work required to support the adoption of Option I, it is necessary to consider not only the scope but the depth of the R and D work that would be required. In this context it must be borne in mind that the cost of the on-going R and D work in relation to the safety of LWR in the U.S. alone is about $60 m per year and world-wide it is probably about $100 m per year (Ref. 15).

Since the LWRs have already been built, or are being constructed in large numbers, this continuing expenditure must be interpreted as an effort to increase the depth of understanding of the underlying phenomena.

Consequently, if the CANDU-type reactor is to be acceptable for licensing in the US, a comparable depth of understanding of safety-related phenomena is likely to be required. Thus, in the context of the possibility of adopting Option I in relation to pressure tube failure, it seems unlikely that this would be an acceptable basis whilst the uncertainties referred to in Sec 4.4, above, still exist.

The nature and extent of the R and D work which would be required to justify adoption of Option I, Option II or Option III, is discussed in more quantitative terms in subsequent sections.

5.9 Further Development of R and D Program on Pressure Tube Integrity

The preceding Sections have provided a qualitative description of the R and D work which is likely to be required in relation to pressure tube integrity, if Option I were adopted. However, they do not provide a quantitative indication of the degree of assurance that would be required in the results of the R and D work, nor do they provide an indication of the relative priorities which should be given to each item. It is also necessary to consider how the choice of other design options would affect the extent of the R and D program on pressure-tube integrity.

In order to clarify these points, a closer examination of the possible design options is necessary. This is provided in the next Section, together with an examination of the possible effects of gross failures of pressure tubes.

6. FURTHER DEFINITION OF R AND D REQUIREMENTS IN RELATION TO PRESSURE TUBE TECHNOLOGY

6.1 The Potential Consequences of Gross Pressure-Tube Failure

6.1.1 Experimental Evidence

6.1.1.1 Evidence from Operational Experience

In the relatively limited operating experience with pressure tube reactors, two cases have been reported in the open literature in which

a pressure tube has suffered a sudden and severe failure.

These cases were:

(i) Lucens research reactor, Switzerland.

(ii) Plutonium re-cycle test reactor (PRTR), U.S.

It is not known whether any similar failures have been experienced in the USSR commercial pressure tube reactors. Although relatively little information has been published as yet about the accident to the Lucens reactor, it appears (Ref. 16) that failure of one pressure tube led to severe damage to almost all the calandria tubes and to the calandria itself. However, only the one fuel element in which the fault was initiated was seriously damaged. It is not clear whether there was any damage to the other pressure tubes which, in this reactor, form part of the fuel assemblies. The damage to the calandria led to the loss of all the heavy water. It is not known when a more complete account of this accident will be published.

The accident to the PRTR is described briefly in Ref. 17. According to this source, the failure was of limited extent (it was not a critical crack propagation type of failure) and it was recovered from without a significantly greater effort than was required for a gross fuel element failure. A complete account of the investigation is given in Ref. 18. The information in this Reference illustrates the potential threat to pressure-tube integrity which is presented by local over-heating of the fuel. However, as indicated above, the failure was not disruptive but was in the form of a simple hole, about 0.5 in. in diameter; the calandria tube did not fail.

Thus we can only conclude from the operating experience that pressure tube failure is a possible, though unlikely, source of sequential damage. Moreover the experimental evidence from the test work described below also suggests that the probability of severe sequential damage may be small.

6.1.1.2 Experimental Evidence from Test Work on Pressure Tube Failure

A number of tests have been carried out to determine the effect of burst-type failures of pressure tubes. Descriptions of tests have been published in Canada (Ref. 19 and 20); in Italy (Ref. 21 and 22), France (Ref. 23) and Japan (Ref. 24). A considerable amount of test work has also been carried out in the UK but this does not appear to have been reported in the open literature.

The most definitive tests are those carried out in Canada. The first set were conducted in 1963, using a mock-up of the NPD reactor configuration. In the 8 tests, failure of the associated aluminum calandria tube occurred on 3 occasions, leading to ejection of the fuel bundles, and there was considerable damage to adjacent calandria tubes and other reactor internals. However, no other pressure tubes failed. In the second set of 18 tests, carried out more recently, the configuration of the CANDU commercial reactor was simulated, embodying the stronger zirconium calandria tubes and larger exhaust areas for the annular space between pressure and calandria tubes, introduced after the NPD tests. In these tests no calandria tubes failed but in some cases the dummy fuel bundles had been pushed into contact with the calandria tube. As the test lasted only 0.5 seconds it is not clear whether, in more representative conditions, there would have been more extensive sequential damage.

The Italian test work described in Ref. 22 was aimed primarily at establishing the pressure-time behavior in the calandria; it does not clarify the situation concerning the possible nature of the sequential effects by direct observation. The French work (Ref. 23) was of a similar nature.

Thus, based on the Canadian work, there are grounds for believing that design features can be introduced which should reduce the probability of severe sequential damage following the failure of a pressure tube, but the

test work reported is not adequate to rule out completely the possibility of severe sequential damage in current designs.

In Ref. 19, the author states explicitly that "no attempt will be made in the report to apply the results of these tests to an NPD incident." Unfortunately it has not been possible to find any subsequent report in which this has been done.

6.1.2 Some General Considerations Relevant to the Possible Effects of the Gross Failure of Pressure Tubes

6.1.2.1 The Applications of General Considerations to the Definition of R and D Requirements

Since failures of pressure-tubes would only be of major importance to safety if they could lead to severe damage to the fuel, it is necessary to establish the accident conditions in which such damage could occur. In this Section, therefore, a number of the generic features of CANDU type reactors are examined qualitatively in terms of their possible contribution to the probability of severe fuel damage, combined with gross failure of the containment in accident sequences which involve pressure-tube failure. The results of this examination provide a basis for grouping the numerous possible accident sequences in a way which should facilitate the identification of R and D requirements in the absence of any detailed accident analysis.

6.1.2.2 The Importance of Pressure Tube Orientation and Moderator Retention

In CANDU-type reactors the pressure tubes are horizontal. For reasons discussed below this may be of importance in relation to the number of other tubes which may fail as a result of sequential damage.

In the event of a gross pressure tube failure, sequential damage could occur in the following ways:

(a) Failure of the pressure tube may lead to failure of the calandria

tube. The probability of failure of the calandria tube is to some extent within the control of the reactor designer, since he can increase the strength of the tube at his discretion. However, this procedure would introduce an economic penalty and also it might be difficult to provide complete protection against highspeed fragments from the pressure tube, if this were to fail in a brittle manner.

(b) If the damage were a nearly complete circumferential tear of the pressure tube and calandria tube, it is to be expected that one or both parts of the tube would develop a substantial droop. If the breach were long enough, or if the two broken ends were sufficiently offset, there would be nothing to prevent ejection of the fuel bundles from the two parts of the tube and their fall towards the floor of the calandria. As noted in Section 6.1.2 above, this was observed in the NPD mock-up tests (Ref. 19). At the time of tube failure there would be a rapid rise of pressure within the calandria. If the relief valves function correctly, there should be no immediate structural damage to the calandria. However, if the pressure is not relieved adequately, there would be some probability of failure of the end shields, allowing the moderator and primary coolant to drain away. In this situation, severe over-heating, or melting, of the ejected fuel could occur. However, failure of the calandria barrel would not lead to this situation; as described below, the fuel would still be immersed in water.

A single fuel-element bundle ejected into a water-filled calandria should be sufficiently cooled by pool boiling. However, it is less certain that a number of bundles falling in a heap in a small area would be cooled sufficiently to prevent progressive

melting of the cladding and fuel. Nor is it clear at what stage, if at all, the calandria floor would melt or collapse. Nevertheless, if it should collapse, the next step in the sequence would be intermixing of the heavy water from the calandria and primary circuit with the light water in the steel/concrete tank which forms the side shields. Thus the fuel bundles would still be immersed in water. Eventually, however, the heap of ejected fuel might cause failure of the shield tank and draining of the water but in view of the large volume of water this seems unlikely.

(c) In addition to the sequential effects described in (b) above, there is the possibility that a descending fuel bundle would be trapped between a lower calandria tube and a vertical control rod guide tube,or liquid absorber tube. In this case also, a single fuel bundle should be adequately cooled by pool-boiling but, as indicated above, there is a possibility that the moderator may be lost due to failure of the calandria end plates. In the latter circumstances it seems likely that the calandria tube supporting the bundle, together with this associated pressure tube, would also fail, thereby releasing additional fuel bundles, with the possibility of damage to more calandria and pressure tubes by the same mechanism. The other tube, or tubes, might be in the opposite half of the primary coolant circuit leading to a further, large release of energy into the calandria. (See Section 6.1.2.4, below).

(d) In (b) and (c) above, sequential damage to other tubes due to the ejection of intact fuel bundles has been described. Damage to the adjacent calandria/pressure tubes and to the calandria itself could also occur as the results of more direct effects such as:

(i) Missile attack due to fragments from a bursting pressure tube.

(ii) Disruptive effect of violent local boiling along the path of the released fuel bundle.

(iii) Shock and jet effects from a bursting tube.

(iv) Whipping of the ends of a broken tube.

(v) Damage due to fuel/coolant, or fuel/moderator interaction, if melting of the fuel occurs.

It is possible that on closer investigation it could be shown that, of the various sequences outlined above that could lead to severe overheating, or melting, of the fuel none is sufficiently probable to add significantly to the risk presented by a CANDU type reactor. However, in the absence of analysis to show that the risk is negligible, these sequences should not be ignored. Some R and D may be required to obtain data needed for the analysis

6.1.2.3 The Importance of Reactor Shutdown

In general, the probability of gross damage to the containment of a CANDU-type reactor would be dependent on the probability of a violent FCI. The probability of such an event depends in part on the degree of "coherence" with which melting and agglomeration of the fuel occurs i.e., if the fuel were widely separated spatially, and remained so, or if it only arrived at a given point over a period of several minutes, the process could be described as "incoherent" and a violent FCI would be less likely.

However, as discussed in the previous section, the characteristics of the CANDU-type reactor would tend to give spatial coherence within the calandria if fuel bundles were ejected from the channels.

If the reactor were shut down correctly at the onset of any severe fault condition it can readily be shown that the rate of rise of fuel temperature would not exceed some 5°C per second and that fuel melting would take at least 10 minutes. On the other hand, if the reactor had not

been shut down, fuel melting could occur in less than 100 seconds, in the most highly rated parts of the core.

Thus we would expect to find a greater probability of gross damage to the containment in those accident sequences in which the reactor does not shut down. In addition, it should be possible to reduce the probability of gross damage to the containment, particularly when the reactor has shut down, by design features beneath the calandria which would serve to decrease the spatial coherence.

6.1.2.4 The Importance of Primary Coolant Pressure

It follows from the previous discussion that if, due to some external effect, a calandria tube and its associated pressure tube were caused to fail, the subsequent effects of that failure would depend to some extent on the pressure within the pressure tube at the time of failure. If it were at full pressure, the probability of failure of adjacent tubes due to effects such as missile attack, pipe whip, shock, and jet action would be a maximum, whereas if the primary coolant pressure had fallen to a low value, these effects could not occur and propagation of tube failure could only take place as a result of interaction between spilt fuel (either as molten UO_2 or as virtually undamaged fuel element bundles) and a second pair of tubes, or as the result of a violent FCI. Thus some general conclusion can be drawn:

(a) Large LOCAs should only lead to the propagation of pressure tube failures by the creation of spilt fuel (from grossly overheated channels) and its interaction with other channels, or by a violent FCI.

Thus, the importance of the contribution of large LOCAs to the overall probability of a large release of fission products to the atmosphere depends on:

(i) whether the reactor shuts down

(ii) the reliability and performance of the ECCS

(iii) The subdivision of the primary coolant system into two parts. In this context the subdivision of the primary coolant system might be inimical to safety. This is because propagation of tube failure by spilt fuel (due to inadequate ECC) to one or more pressure tubes in the pressurized half of the circuit could lead to a situation in which the probability of failure of several tubes in both circuits was increased.

(iv) If the large LOCA were accompanied by a failure to shutdown, a violent FCI would be more likely to occur.

(b) Accidents in which primary coolant pressure is not lost at the outset (e.g., loss of primary coolant flow, reactivity excursions, secondary coolant faults and single channel faults) are more likely to be the cause of widespread pressure tube failures due to propagation effects than are large LOCAs, since an overheated tube could be subjected to full reactor coolant pressure.

(c) Some small LOCAs (other than self-failure of pressure tubes), such as failure of channel feeders, which can lead to stagnation of flow and over-heating of the fuel in the associated channel, may need to be treated as a separate, intermediate class. This is necessary since in some cases the reduction of primary coolant pressure at the time of sequential failure of the first pressure tube could be quite small.

6.1.3 Grouping of Possible Accident Sequences in Relation to the Likelihood of Sequential Failure of Pressure Tubes

The preceding discussion leads to the following grouping of possible accidents:

Group	Description of Accident Group
A1	Self failure of pressure -tube; reactor shutdown (S-D)
A2	As A1 but reactor Not S-D
B1	Non-LOCA faults - reactor S-D; first P-T fails due to transient temperature rise
B2	As B1, but reactor not S-D
C1	LOCA faults - other than self failure of PT, reactor S-D; first P-T fails due to transient temperature rise,as B1
C2	As C1, but reactor not S-D.

The R & D requirements for the various groups are discussed in the following sections, for each of the options defined in Section 1 above.

6.2 Definition of R and D Requirements to Justify Option I

6.2.1 The Nature of the R and D Work Required to Justify Option I

In order to justify the adoption of Option I (i.e., to proceed on the basis that the probability of gross failure of a pressure tube can be made so low that it can be ignored) it would be necessary to demonstrate two characteristics, viz:

(i) That the probability of failure of a tube due to its own defects was acceptably low

(ii) That the probability of reactor faults which would not be harmful to the majority of the core, but which could lead to failure of at least one pressure tube, was also acceptably low.

It should be noted that in adopting this Option it would be implicitly assumed that there was no reliable information about the sequence of events following gross failure of a pressure-tube. Thus in establishing an acceptable probability for such a failure it has to be assumed that the conditional probability of exceeding 10CFR 100 guide lines following the failure, would

be unity (See also Appendix 1.)

These two different aspects of the R and D requirements are considered separately in the following sections.

6.4.2 R and D Work in Relation to Self-Defects in Pressure Tubes

It follows from discussion in Section 4 and 5, above that the principal areas in which R and D work would be required to demonstrate an acceptably low probability of gross failure due to self-defects are:

(a) Material properties of the pressure tubes, with particular reference to the effects of deviations from the normal manufacturing process and of the reactor environment.

(b) Effect on the failure mechanics analysis of departures from the nominal condition of the pressure tube material.

(c) Reliability of the leak detection system, or systems.

(d) Reliability of the in-service inspection methods.

As discussed in Section 5.8, above, in order to be consistent with the standards of safety demanded today, extremely low probabilities of failure would have to be demonstrated. Assessment of the scope of the R and D program necessary is difficult, particularly for the first two of the areas listed above. The nearest analogy, perhaps, is the scale of the effort required to demonstrate the safety of LWR pressure vessels. In this context it should be noted, moreover, that Zirconium and its alloys are fundamentally less satisfactory materials for high integrity pressure parts than the low alloy steels. This difference stems mainly from the greater inherent tendency of Zirconium alloys to absorb hydrogen, with the subsequent formation of hydride particles within the parent lattice (Ref. 5).

The R and D work required to develop leak detection systems and in-service inspection methods could, in principle, be defined more readily. Nevertheless, as discussed in Section 4.3, the reliability required

from the leak detection systems depends to a large extent on the frequency of minor failures in the pressure tubes which, if undetected, could lead to gross failures. Thus the first step would be to define the frequency of demand; in view of the more recent operating experience with pressure tubes in the CANDU reactor, it is difficult to see how a low failure rate can be claimed without many years of trouble-free operation from today onwards. I.e., if a U.S. program of development of CANDU-type reactors were started in the near future, it would have to be based on the premise that the incidence of minor, but potentially dangerous failures, in pressure tubes was quite high (of the order of 10^{-1} per reactor year).

6.2.3 R and D Work in Relation to External Causes of Pressure Tube Failure

6.2.3.1 Transients Affecting the Whole Reactor

As discussed in Appendix 1, not only would it be necessary to demonstrate extremely low probabilities of pressure tube failure, of the order of 10^{-10} per tube year, due to self-defects but it would also be necessary to show, at a higher level of probability, that failure of a single pressure-tube would not occur as the result of reactor transients. The transients in question are those in which the conditions in virtually all of the fuel channels would remain satisfactory, so far as the continued integrity of the pressure tubes is concerned, but in at least one channel the conditions of temperature and/or pressure could lead to failure. For example, if the "hot-spot" factors were under-estimated, a loss-of-primary-coolant-flow fault could lead to sufficient clad melting and fuel-slumping in the hottest channel to endanger that pressure tube, whereas a corresponding error in prediction of hot-spot factors and transient behaviour in a PWR would have much less severe effects.

Thus, in order to adopt Option I, a higher standard of accuracy in the prediction of hot-spot-factors and transient behaviour would be required for a CANDU-type reactor than has been necessary for LWRs. This higher

standard would have to extend to the performance of the shutdown and shutdown heat removal systems, since, in the limiting condition, these contribute significantly to the safety margin. In this context the positive reactivity coefficient of the CANDU-type reactors may be significant.

Consequently, in this area also, the R and D work required would be substantially more extensive than has been the case for LWR. An alternative approach, in order to reduce the R and D costs, would be to reduce the peak linear rating. However, the increased number of channels required could add substantially to the capital cost of the NPS. For example, it was found in the UK that a 10 percent decrease in rating for a 660 MW(e) steam generating heavy water reactor (SGHWR) led to an increase of about 5 percent in the capital cost of a station (i.e., about $50 m). Thus for a large program of CANDU-type reactors, this alternative approach would probably be unattractive.

6.2.3.2 Transients Affecting Single Channels Only

If Option I were adopted then, by definition, faults such as channel blockage, which would affect only one channel at a time, are as important as faults which affect the whole reactor. Thus, a considerable amount of R and D work would be required to prove adequate reliability in the devices used to detect partial blockage.

Some indication of the cost of this R and D could be gained from examination of the scope of the R and D work which was visualized for LMFBR, when it was believed that single channel faults could lead to dangerous transients affecting the whole core.

6.2.3.3 Feasibility of Proceeding on the Basis of Option I

Overall it appears that the R and D program required to support the adoption of Option I would prove so extensive and prolonged that this would not be a viable approach.

The first alternative, that of adopting Option II, is discussed in the next Section.

6.3 Definition of R and D Required to Justify Option II

6.3.1 Nature of the R and D Required to Justify Option II

In order to justify the adoption of Option II (i.e., to proceed on the basis that gross failure of a pressure tube is so unlikely to lead to meltdown* of the fuel in the parent channel, or to failure of other pressure tubes, that a relatively high probability of gross failure of a single tube would be acceptable). The R & D work that would be required is as follows:

Stage (a) Work to show that the probability of fuel meltdown due to a single tube failure, which does not propagate to others, would be acceptable.

Stage (b) Work to show that the probability of the single initiating failure propagating to other pressure tubes is acceptably low.

It should be noted that, by definition, Option II implies that no upper limit should be placed on the probability of pressure tube failure. However, as discussed below, this definition leads to difficulties, if used as a basis for a probabilistic analysis. For this reason alone, some modified form of Option II, in which a specific limit is placed on the probability of the initiating event, is required. This requirement is satisfied in the definition of "Option III".

The type of work required for Stages (a) and (b) is discussed briefly in the following sections.

6.3.2 Acceptable Value for Conditional Probability of Fuel Meltdown Following Pressure-Tube Failure

From the discussion in Sec 6.1.2, above, it seems unlikely that gross failure of a pressure-tube due to an inherent defect would lead to rapid meltdown of the fuel from that channel, providing that the reactor was shutdown promptly. However, some possible ways in which meltdown could

---

*Note: In Option II, "meltdown" also implies prolonged heating of unclad fuel in an air/steam atmosphere.

occur after a delay were identified. In particular there is the possibility that ejection of fuel bundles could be accompanied by failure of the calandria end plates, leading to draining of the heavy water, so that the exposed bundles would then have insufficient cooling to prevent melting of the cladding and subsequently melting or prolonged overheating of the fuel.

If the failure of the pressure-tube occurred as a result of over-heating of the fuel (e.g., due to a channel blockage), the fuel could be in a condition at the time of the tube failure where melting would be more likely, in an empty calandria, since there would be more heat stored in the UO_2.

A possible limiting value for the conditional probability of meltdown (or prolonged over-heating) of the fuel from a single channel has been derived in Appendix 1; this value is $1x10^{-6}$ per event. This value is associated with the specific fault-sequence. "Single pressure tube fails; calandria tube fails; calandria damaged and drained of heavy water; fuel bundles left uncooled in an air/steam atmosphere". However, as indicated in the previous Section 1, the nature of "Option II" leads to a rather artificial target: in deriving the value of $1x10^{-6}$ a very conservative assumption about the probability of the initiating event has been used.

It is likely that an extensive R and D program would be required to confirm that the conditional probability of this sequence was as low as $1x10^{-6}$ per event. Moreover it is not known how much information would be available from Canadian or other sources. However, because of the artificial nature of the target, consideration of the need to examine the R and D implications is deferred until Sec. 6.4.4 where a more realistic design target is discussed.

6.3.3 Acceptable Value for Conditional Probability of Propagation of Pressure-Tube Failure

In order to construct a satisfactory safety case for a pressure-tube reactor it would be necessary to show that propagation is a low probability event. However, in order to design an R and D program to demonst this, there must be some indication of the level of conditional probability which is acceptable. A possible target is derived in Appendix 2, by an extension of the risk-allocation procedure.

A possible target value derived for the conditional probability of propagation of the initial failure to a large number of other pressure-tubes is 1×10^{-6} per event. However, as in the case discussed in the previous Section, this is a somewhat artificial value, since the definiiton of "Option II" necessitates the use of a very conservative value for the frequency of the initiating event. Consequently discussion of the R and D requirements in relation to tube-to-tube propagation is also defined until a more realistic design basis has been identified (see Sec 6.4.4 below).

6.4 Optimum Design Basis

6.4.1 Summary of the Difficulties Encountered in the Use of Options I and II

It follows from the discussion in the preceding sections that:

Firstly, it is unlikely to be feasible to demonstrate by R and D work that the adoption of Option I is a viable approach, on account of the extremely low probabilities of specific events, such as pressure tube failure due to self-defects, that would be a necessary condition for this to be valid.

Secondly, Although a reduction in peak linear rating would reduce the R and D work required to demonstrate some aspects of Option I, it is unlikely that this would be an economically viable approach for a large program of reactors.

Thirdly, in the case of Option II, it is not possible to define realistic quantitative values for the parameters which would be the subject of R and D work. Thus, the adoption of this

Option could not lead to the definition of a completely satisfactory R and D program

Thus, as has been indicated previously, an alternative to both Option I and Option II is required as a basis for design. A suitable alternative is described in the next Section.

6.4.2 Formulation of an Alternative Approach to Design (Option III), in Relation to Pressure-Tube Integrity

In the light of the preceding discussion, the most promising alternative appears to be as follows:

The probability of gross failure of one of the pressure-tubes in the set, due to all conceivable causes, is assumed to be less than 10^{-x} per reactor year and the conditional probability that a single gross failure would propagate an unacceptably large number of other tubes is assumed to be less than 10^{-y} per event. In order to give comparability of safety with LWRs the product $10^{-x}.10^{-y}$ must lie in the range 10^{-6} to 10^{-7} per reactor year. The phrase "unacceptably large number of other tubes" has to be interpreted in accordance with the effects of the tube failure on its associated fuel and on the reactor and containment as a whole. Licensing policy at the relevant time may be a further factor. For example, it might not be considered acceptable to contemplate the failure of more than, say, 10 channels, at a probability of more than 10^{-6} per reactor year, even though it might be possible to demonstrate that the failure of 100 pressure tubes would present a smaller hazard than failure of the reactor vessel of an LWR.

The lower limit to the range of "unacceptably large numbers" is obviously zero. However, this would still represent a more readily demonstratable design than one based on Option I, since failure of one tube would be permitted.

It will be seen from the analysis in Appendix 2 that, as the size of the "unacceptably large number" is increased, the problem of demonstrating that propagation to some larger number of other tubes would not occur becomes progressively easier. The limitations on the choice of the maximum acceptable probability of gross failure of one pressure tube in the set (i.e., 10^{-x}) are discussed in the next Section.

6.4.3 Limitations on Maximum Acceptable Probability of Pressure-Tube Failure

In the event of a pressure-tube failure of the "leak-before-break" type, the reactor operator would have to shutdown, locate the faulty tube and replace it. For randomly occurring single failures the downtime would be of the order of 10 days; the differential cost of operating reserve fossil fired plant to replace the output of a 1200 MW(e) nuclear plant for 10 days is about $\$5 \times 10^6$. Economic considerations alone would make a failure probability of less than 10^{-2} per reactor year desirable, i.e., on economic grounds the maximum acceptable probability of random "leak before break failures" would be about 10^{-5} per tube year. Type-faults, leading to several simultaneous "leak-before-break" failures, or incipient failures, would lead to longer outages, but the outage time should not increase in direct proportion to the number of failures. Canadian experience (Ref 10) suggests that a typical period would be about 100 days, so that on economic grounds a maximum probability of about 10^{-3} per reactor year for type-faults in the pressure tubes would be desirable.

It will be seen that these "economic objectives" demand a better performance than has as yet been demonstrated operationally. However, a possible maximum value for the conditional probability of gross pressure-tube failure, which would be acceptable on safety grounds, (without having to assume probabilities of "leak-before-break" failures as low as those likely

to be required for economic reasons) has been derived in Appendix 1. The value derived in Appendix 1 is 10^{-3} per reactor year. In order to derive this value a number of assumptions have had to be made but with one exception it is believed that these can be verified by development programs of manageable dimensions. The one exception is the probability of a "break-before-leak" failure, for which a probability of 10^{-6} per tube year has been assumed. The difficulty of substantiating this value by analysis or by experiment, is analogous to that of confirming that the maximum probability of catastrophic failure of an LWR pressure-vessel is less than 10^{-6} per vessel year. In this instance, therefore, comparability of safety might be demonstrable in a qualitative manner by a detailed comparison of the arguments which have been used in each case. In this context it should be noted that the pressure-tube arrangement has one major advantage over the use of a single vessel, in that one or more complete tubes can be removed at intervals for comprehensive tests in laboratory conditions, including hydraulic tests to destruction, if necessary. Before proceeding to a formal definition of Option III it is necessary to determine whether possible seismic effects on the pressure-tubes need to be taken into account.

6.4.4 Seismic Resistance of Pressure-Tubes

The design of the pressure-tubes to resist a "design-basis" earthquake presents a well-defined structural problem for which, it is assumed, a satisfactory design solution can be found. However, it is usually difficult to define the probability distribution for size of earthquake at levels of probability lower than 10^{-4} per year. The implicit assumption is usually made, for sites in low areas of seismic activity, that in the event of an earthquake more violent than the "design-basis", sufficient of the plant (e.g., the containment) would survive to reduce the probability of a large

release of activity into the atmosphere to an acceptably low value. In the case of a CANDU-type reactor a "beyond design-basis" earthquake could conceivably cause simultaneous damage to a large number of pressure tubes and/or their connecting pipe work. Sufficient analysis should therefore be performed to obtain a clear picture of the likely sequence of events in such circumstances.

A further seismic problem in relation to the pressure tubes is that of a tube which is connected to the fuel charge and discharge machines at the time of an earthquake. In this situation three additional effects can be identified, viz:

(i) The movement of the machines relative to the ends of the pressure tubes could create substantial additional loads on those parts of the tubes and their end fittings which protrude beyond the outer calandria end-plates. The additional loads on the end-plates could also be substantial but the part of the pressure tube which is within the calandria should be adequately isolated from the additional loads, since it is usually regarded, for structural analysis purposes, as a beam fixed at both ends.

(ii) The additional loads on the end parts of the pressure tubes could conceivably cause them to fail. This failure would be seen as a small LOCA by the rest of the primary circuit and thus should be within the capacity of the existing emergency cooling systems. Ejection of one or more fuel bundles from the failed tube is conceivable, in which case the bundles would be retained within the pressure tube and would be cooled initially by the flow of escaping heavy primary coolant and later by the injected emergency coolant.

(iii) The additional loads on the calandria and end-plates could conceivably cause failure of the seals and draining of the whole, or part of the moderator. However, this would not create any direct hazard, although it would not be possible to claim the moderator as an additional means of cooling the fuel in all the other channels (by radiant heat transfer to the moderator), if the other emergency cooling systems failed. Overall, therefore, the special case of a pressure tube being refuelled at the time of a severe earthquake should, at the worst, lead to a release of activity into the containment equivalent to one complete channel.

Thus, considering both the general and the special cases of possible seismic effects, it is concluded that these do not affect the choice of assumptions concerning pressure tube integrity which are required to provide a basis for design.

6.4.5 Definition of Option III

The probability of gross failure of a pressure tube is not to exceed 10^{-3} per reactor year and in the event of such a failure, the probability of propagation to more than 9 other pressure tubes shall not exceed 10^{-3} per reactor year.

6.4.6 Summary of the Reliability Requirements Implicit in the Adoption of Option III as a Basis for Design

From the work described in the earlier parts of Section 6.4, it is now possible to list the reliability requirements which are implicit in the adoption of Option III as a basis for design, so far as the pressure tubes and the systems directly relevant to the maintenance of their integrity

are concerned. These reliability requirements indicate the scope of the R and D work required and its priorities. The reliabilities required from other systems are summarized in Section 7.1 below.

The reliability requirements are as follows:

(i) Pressure Tubes

- Probability of random "leak-before-break" failures, $\leq 10^{-3}$ per tube year
- Probability of type-faults, each leading to the order of 10 "leak-before-break" faults before recognition as type faults, $\leq 10^{-1}$ per reactor year
- Probability of "break-before-leak" failures, $\leq 10^{-6}$ per tube year.

(ii) Leak Detection Systems

- Probability of failure $\leq 10^{-4}$ per demand (it is assumed that at least two diverse systems would be provided)

(iii) Channel Blockage Detection

- Probability of failure $\leq 10^{-2}$ per demand

These reliability requirements should provide a useful basis for defining the detailed R and D programs for pressure tube material fabrication and inspection methods and for the leak-detection and channel blockage detection systems. Since the acceptable probability of gross failure is much higher than if Option I were used as a basis for design (10^{-3} per reactor year, as compared with 10^{-6} per reactor year) many of the rare and bizarre events discussed in Section 4, above, can

be ignored. Associated with the reliability requirements defined above for the pressure tubes and their protection systems are a number of requirements which are more of a "performance" nature. Each of these is described below.

(a) Propagation of Pressure Tube Failure

The fundamental requirement is to show that the probability of propagation to some acceptable number of other pressure tubes (assumed in this this analysis to be 9) is less than 6×10^{-4} per event. However, as shown in Appendix 2, it should be sufficient to demonstrate that:

Probability of the initial failure causing the direct failure of

1 other pressure tube is less than 0.5 per event

2 other pressure tubes is less than 0.1 per event

3 other pressure tubes is less than 0.08 per event

and 4 other pressure tubes is less than 0.02 per event

It should be noted that in view of the arrangement of the pressure tubes (on a square lattice) and the available experimental evidence, it is considered unnecessary to consider cases in which more than 4 failures result directly from the initial one. However, any lack of validity in this assumption should become apparent during the test program. It should be noted also there are different sets of boundary conditions for different fault sequences. However, with one exception, the calandria is assumed to be full at the time of the first failure, so that a single test program based on the most severe conditions in the tubes and a full calandria could cover nearly all the situations. It will be seen that relatively few tests should be sufficient to prove, or disprove, that the probability of propagation to, say, 10 other tubes is low enough to meet the reliability requirements, at an adequate level of confidence.

The one exception which has been identified in this study is the following sequence:

(i) Initial pressure tube failure leads to failure of calandria end plates.

(ii) Calandria drains.

(iii) Ejected fuel bundle is wedged against calandria tube in the undamaged loop.

(iv) Calandria and pressure tube fail, at full primary coolant pressure, with empty calandria.

As discussed below (para (b))it should be possible to so arrange the design that the overall probability of this sequence is so small that it can make no significant contribution to the overall risk. In any event, a much higher probability of propagation than is indicated above would be acceptable, so that a very small number of tests should suffice.

It should be noted that the main test program could be arranged in two parts; the first part could be aimed at establishing the probability of failure of the "parent" calendria tube. If this proved to be quite low the number of tests with arrays of tubes, which would form the second part of the program, could be reduced substantially.

(b) Probability of Channel Blockage

It has been postulated in the derivation of the other reliability requirements that the probability of channel blockage would be less than $1x10^{-3}$ per reactor year. The design of the "feeder pipe" and channel inlet features would have to be developed with this requirement in mind.

(c) Probability of Stagnation in a Single Channel

It has been postulated in Appendix 1 that the probability of this event would not exceed 10^{-5} per reactor year. The initiating event would be failure of a 'feeder' pipe within a relatively narrow range of positions.

Assuming that the frequency of such an event would be less than 10^{-2} per reactor year, it would be necessary to show that the conditional probability of fuel overheating and pressure tube failure was less than 10^{-3} per event. Conceivably this could be done purely by analysis but it is possible that some device to prevent back-flow from the tube might be desirable. In the latter case, this definition of the reliability required would provide some guidance in the development.

(d) Performance of Reactor Instrumentation

It is postulated in Appendix 1 that the probability of an inadequate margin against fuel melting due to lack of an adequate "hot spot" margin is 10^{-4} per reactor year. This requirement should provide some guidance in the development of the instrumentation for assessing steady state core conditions and in the development of the transient analysis. It is also postulated that the probability of local clad-melting escalating to channel blockage and fuel melting is less than 0.3 per event; this requirement also provides some guidance for the development of the transient analysis. However, the reactor designer is free to revise the allocation, within the target value for the fault, without having to consider the repercussions of the change elsewhere in the system e.g., in order to save some analysis he could assume that clad melting always escalates to fuel melting and then improve the instrumentation accordingly.

(e) Performance of the Containment

For faults involving failure of only one pressure tube it has been assumed that the probability of the containment proving ineffective is 10^{-3} per demand and for multi-tube failures (up to 10) a probability of 10^{-1} per demand has been assumed. The former value is consistent with the assumptions made for the CANDU reactors: the value of 10^{-1} should be conservative. Both should provide some guidance to the designer.

(f) Performance and Reliability of Calandria Pressure Relief System

The potential hazard from pressure tube failure is likely to be increased substantially if the end-plates of the calandria fail, allowing the heavy water to drain from the system. Clearly it would be uneconomic to design the end-plates to resist a pressure approaching that of the primary coolant. Thus prevention of damage to the end-plates must depend on the adequacy and reliability of the pressure relief system. Taking the value of 10^{-3} per reactor year for the annual probability of pressure tube failure for design purposes (as derived in Appendix 1), a probability of failure of 10^{-4} per demand for the pressure relief system should be adequate. It should be possible, in fact, to meet this requirement without further development but detailed reliability analysis will be required to support the design. In this context it should be noted that, if the design basis permits propagation up to, say, 10 tubes in all, the calandria pressure relief system capacity must be adequate for this condition.

(g) Behavior of Ejected Fuel Bundles

In the derivation of the proposed treatment of the problem of pressure tube integrity, it has been assumed that:

(i) If the calandria is filled with water a single ejected fuel bundle would be adequately cooled and, even if lodged against another calandria tube, would not cause it or the associated pressure tube to fail.

(ii) If a number of ejected bundles fall into a single heap, cooling would be adequate, if the calandria is filled with water.

(iii) If the calandria has been drained (e.g., by failure of the end-plates) a single ejected bundle could cause failure of another pressure tube, if lodged against its associated calandria tube.

(iv) If a number of ejected bundles fall into a single heap in a drained calandria, fuel melting could occur.

Sufficient analysis, supplemented as necessary by test work, would be necessary to confirm (i) and (ii) above and to obtain a better understanding of the phenomena associated with (iii) and (iv).

(h) Seismic Effects on Pressure Tubes

Some scoping calculations to determine the likely effects of multiple pressure tube failures as a result of earthquakes more severe than the nominal "design basis" earthquake are desirable. These should indicate whether it is reasonable to assume, for example, that the containment would still retain some degree of effectiveness or whether a violent fuel/coolant interaction is so probable that the assumption would be invalid.

6.5 Priorities for R and D Work Required in Relation to Pressure Tube Integrity

In the previous Section a basis for design has been proposed which is believed by the present writer to be near the optimum so far as the amount of R and D required to support the design in relation to pressure tube integrity is concerned. Reliability requirements for this design basis have been deduced. Clearly other designers might choose a different basis, leading to a change in reliability requirements.

The discussion of R and D priorities in this section relates only to the design basis proposed above. On reviewing the reliability requirements summerized in the previous section, it will be seen that the only areas in which long-term R and D might be required, from the safety point of view, in relation to pressure-tube integrity are:

(i) Demonstration of a sufficiently low probability of "break-before-leak" failures;

(ii) Demonstration that the probability of propagation of pressure tube failures is sufficiently low;

(iii) Demonstration that the ejection of fuel bundles, from failed tubes, into a fuel calandria would not cause any further damage by their fission product heat;

(iv) Further investigation of the probability and effects of channel stagnation; and

(v) Development of methods for the detection and effects of channel blockage.

From the economic point of view, it might be desirable to give high priority to R and D work aimed at establishing lower probabilities of "leak-before-break" failures, due to both random faults and to type-faults.

As discussed in Section 6.4.3, above, it is possible that qualitative arguments alone might be enough to show that the probability of "break-before-leak" failure is sufficiently low to meet the design basis requirement postulated in Appendix 1 (i.e., 10^{-6} per tube year) bearing in mind that it should be sufficient to show comparability of safety with LWR vessels in this respect. If this proved to be the case, no major R and D program would be required in relation to this aspect.

Although investigation of tube-to-tube propagation has been identified as a high priority, attention has been drawn in Appendix 3 to quite extensive tests carried out in other countries, which do not appear to have been reported in the open literature. It is possible that, if the full reports of these tests could be obtained, they would be sufficient to justify reducing the priority accorded to this item. Moreover, as noted above, concentration of the test work initially to determine the probability of failure of the "parent" calandria tube, as a result of failure of its pressure tube, might reduce substantially, the total amount of test work required.

7. A POSSIBLE BASIS FOR DESIGN OF A CANDU-TYPE REACTOR TO BE LICENSED IN THE U.S.

7.1 A basis for design.

In the preceding Sections, a possible approach to the problems of demonstrating adequate integrity of the pressure tubes has been outlined. This should meet the requirement of achieving a standard of safety comparable with the LWRs in respect of primary circuit integrity. This approach implies some assumptions about the risk-allocation made for the reactor as a whole. However, the allocation made to the pressure tubes is so small (10 percent of the total) that changes in it could not have any significant effect on the problems of obtaining the target reliability which might be established for the other safety systems. It remains to be shown therefore, that a viable risk-allocation can be chosen and that the conceptual design outlined would be consistent with this. As in the case of the pressure tubes, the risk allocation can then be used to provide an indication of the R and D requirements and priorities.

Experience with conceptual designs of other pressure tube heavy water reactors suggests that the target allocation proposed in Appendix I should be satisfactory. This requires the following reliabilities:

(a)	Shut down system	1×10^{6} failures per demand
(b)	Residual heat removal (pressurised)	7×10^{-7}*
(c)	Residual heat removal (depressurised)	1×10^{-4}*
(d)	Critical structures (other than the pressure tubes)	1×10^{-6} failures per r.yr. ϕ
(e)	Safe shut-down in event of external hazards beyond design levels	1×10^{-2} failures per extreme demand

*Note: For RHR the allocated target has to cover both starting and running reliability

ϕNote: The reliability required from the pressure tubes is derived in Appendix 1.

With the possible exception of "Residual Heat Removal, (pressurized)" it is believed that the design proposed by CE should meet these requirements; the reasons for this belief are described in the following Section. However, as discussed in Section 6.4, above, it is necessary to consider not only the reliability of the safety systems but also their performance in limiting transients, since the overall safety of the CANDU-type reactor is likely to be more sensitive to adverse combinations of "hot spot" factors and transient behaviour than is an LWR. Both of these aspects are discussed in the following Sections.

7.2 Adequacy of Shut-Down Systems

The current CANDU designs embody two quite diverse sets of absorbers, each of which presumably has sufficient capacity to shut the reactor down and to keep it shut down. In addition it is believed that both systems are sufficiently rapid in action to be effective in all types of fault conditions. However, the diversity between the systems does not extend to the sensors employed to detect the onset of conditions which require a reactor trip.

The proposed CE design embodies the same types of shut-down systems as in the current CANDU designs but it is not yet clear whether a more diverse set of tripping parameters would be included.

Because of its positive void coefficient, the CANDU-type reactor designed by CE would be provided with an automatic control system, operating on each of several sectors of the core. Consequently there is some chance that absorber might be removed inadvertently in one sector, leading to an asymmetric reactivity fault.

This problem of diversity in choice of tripping parameters may be particularly difficult in the case of these asymmetric reactivity faults, as alternatives to flux measurements may not be readily available.

Although LWRs are less likely to experience asymmetric reactivity faults than the CANDU-type reactors, their potential hazard from symmetric reactivity faults is much greater. This is due to the much larger amount of excessive reactivity which is available (about 7 percent as compared with 1 percent).

Subject to these reservations about diversity of sensors and subject to the assumption made in Appendix I concerning the frequency of faults requiring an automatic trip (1 per year) it is considered that the proposed design should be satisfactory, so far as reliability is concerned, and in this respect the design is superior to current LWRs. It should be noted that the value of 1 genuine demand per year is intermediate between the value used in the CANDU safety assessments (0.3 per r.yr) and that assumed by NRC for LWRs in their ATWS studies (about 6 per r.yr).

Insufficient data are provided in the available descriptions of the CE design to estimate the performance of the two reactor shut-down systems. However, providing that both can terminate all major faults safely, the CE design should have better resistance to ATWS-type faults than is the case for current LWRs.

7.3 Residual Heat Removal Pressurized

As noted above, the reliability target for this system must be apportioned between starting and running modes. In the pressurized condition the latter should prove a less onerous requirement and provisionally it can be assumed that targets of 5×10^{-7} and 2×10^{-7} per demand, for starting and running respectively, would be appropriate. To meet the target for starting reliability two diverse systems, each with at least "2 out of 3" redundancy would be necessary, or both the primary and secondary side. It could be argued that natural circulation of the primary coolant would be sufficient to maintain satisfactory fuel conditions. However, further work is necessary for the following purposes:

(i) To confirm that the CANDU-type of configuration would provide adequate natural circulation: in this context it should be noted that the horizontal arrangement of the fuel tends to reduce the available buoyancy head, as compared with a PWR, and the horizontal arrangement could also lead to some stratification of flow, due to the formation of local natural circulation "cells" in the individual tubes, which could have an adverse effect on the temperature distribution. It will also be necessary to determine whether this configuration is less, or more, prone to loss of natural circulation if the fuel cladding becomes sufficiently over-heated, temporarily, to produce hydrogen in large quantities, as in the case of the Three Mile Island reactor.
It is likely that some test work has been carried out on CANDU reactors, the results of which could resolve some of these points. However, it has not yet been possible to identify the appropriate references.

(ii) To confirm that the reliability of the circulation and/or emergency feed supplies on the secondary side would be adequate, as the water level must be maintained in the boilers to secure natural circulation on the primary side.

(iii) To confirm that the reliability of the electrical supplies needed to run the emergency feed pumps is adequate. The most critical case would be loss of all main AC supplies: according to local conditions the frequency of loss of the main grid could vary from 10^{-2} to 1 per r. year. Moreover, a similar variation may be expected in the probability of sequential loss of internal generation, owing to variations in the "balance of plant" design. When the reliability of the necessary switching operations is taken into account, in addition to that of the diesel alternator sets starting systems, it is unlikely that an unreliability better than 10^{-4} per demand could be demonstrated for a

typical 3 x 100 per cent arrangement of diesel generators. Thus, unless the reliability of the grid and of continued in-house generation are near the lower end of the range suggested above, a second, independent source of energy would be required for the emergency feed pumps. In principle this could be provided by separate small turbines, supplied with steam from the secondary coolant side, as in some PWR designs. In other fault conditions of this type it should be possible to rely partly on continuity of grid supplies.

(iv) It has been claimed for the CANDU reactors (Ref. 25) that radiative transfer to the moderator can provide a sufficient heat sink to prevent fuel melting in the absence of all convective cooling. Although this characteristic is of more importance in LOCA accidents, it would also be of considerable value in fault conditions, such as those encountered in the Three Mile Island reactor accident, where partial loss of coolant leads to temporary voiding of the channels. This characteristic of the CANDU-type reactor is discussed more fully in the next Section.

Overall, therefore, the type of design proposed by CE should provide sufficient starting reliability in pressurized faults, providing that adequate natural circulation can be demonstrated. If adequate natural circulation could not be demonstrated it might be possible to claim sufficient additional starting reliability from the longer-term cooling systems, although these are intended primarily for use in prolonged shut-downs for maintenance.

Clearly, it would be much easier to meet the requirement for running reliability, pressurized, if there were adequate natural circulation. However, even without this facility, the CE design might be just adequate.

In order to assess the adequacy of performance of the emergency cooling in pressurized faults, further information will be required concerning:

(a) The accuracy with which the steady state rating and temperature distributions in individual channels can be predicted, with the instrumentation proposed.

(b) The extent of the transient temperature rise; in this context it should be noted that division of the primary coolant into two parts, which are virtually independent of one another hydraulically, tends to accentuate the transient effects of loss of a single coolant pump, or locking of a rotor, since the reduction in flow is proportionately greater. In this case also there may be CANDU data in existence which could clarify the situation.

As noted in Sec 2.2 above, because of the proximity of the fuel to the primary circuit, a higher standard of accuracy in the prediction of steady state conditions and of transient effects is likely to be required.

7.4 Residual Heat Removal, Depressurized

In this case the risk allocation suggested in Appendix I leads to a maximum acceptable unavailability which is relatively high (10^{-4} per r.yr) although, as in the previous case, this has to cover running reliability as well. However, so far as large LOCA are concerned (failure of pipes greater than, say, 6 in. in diameter) the frequency of occurrences should only be a small fraction of the total of 1×10^{-2} per r. year which was assumed in Appendix I. If the frequency were as high as 1×10^{-3}, the unavailability could be as high as 3×10^{-2} per demand, assuming an allocation of 3×10^{-5} per year to this type of fault. This could be met by a single system with a 2 out of 3 redundancy. However, because of the time factor, it would probably be desirable to identify at least three phases; in the first reliance would be placed on the injection of water from pre-pressurized tanks; in the second reliance would be placed on high-pressure injection

pumps and, in the third, long-term phase, water at atmospheric pressure would be circulated by pumping. The reliability target proposed above should be large enough to permit the use of one system in each phase, given sufficient redundancy in each.

Smaller LOCAs, excluding those due to inadvertent opening of relief valves on the primary circuit, would have a substantially higher frequency than larger LOCAs, but the proposed value of 1×10^{-2} per r.yr. should be reasonably conservative in this respect. In this case, rapid injection of water in the initial phase should not be necessary. However, the system provided to cope with large LOCAs, would be operative and would, in effect, provide some diversity in the initial stage. In the second and final stage, dependence on a single system would be rather difficult to justify. Nevertheless, the long-term heat removal system, which is assumed to form part of the protection against pressurized faults, could probably be arranged to operate in the depressurized condition as well.

Inadvertent operation of primary coolant relief valves, followed by a failure to re-close, is a potential cause of small LOCAs. If there were at least two relief valves per steam generator and two on the pressurizer then, using the data of WASH-1400 (Ref. 4), we should expect a frequency of spurious valve opening of about 1 per r.yr. However, the probability of failure to re-close is likely to be less than 0.1 per event, thus the overall frequency of this type of event is unlikely to exceed 10^{-1} per r. yr. This should not be high enough to invalidate the arguments about the adequacy of protection against small LOCAs which has been developed above.

It has also been argued (Ref. 25) that an advantage of the CANDU type of reactor is that, after a LOCA, there would be sufficient heat transfer from the fuel to the moderator to provide an alternative, and highly diverse means of removing the shut-down heat. However, the relevant transient

analysis, as summarized in Ref. 25, is not entirely convincing: for example, it is assumed that there would be no zircalloy/steam reaction. In addition, for this mode of cooling to be useful, upgrading of the reliability of the moderator cooling system would probably be necessary. If adequate cooling in this mode could be demonstrated, it would also provide a valuable increase in safety in fault conditions where there is a temporary loss of aqueous phase coolant from the channels, as in the case of the 3 Mile Island reactor accident.

Overall, it is considered that provision of adequate reliability in the shut-down heat removal systems required in depressurized conditions should not be unduly costly, or unduly difficult to demonstrate.

However, demonstration of adequate performance may be more difficult, some potential problems are:

(i) In the small LOCAs there is the possibility of stagnation of flow in one or more channels.

(ii) In the large LOCAs the effectiveness of the initial injection system is uncertain, due to the possibility of steam binding.

Stagnation can arise only as a result of failures between the pumps and the fuel channel inlets. This possibility is discussed in Ref. 6, where the use of check valves as a partial solution is suggested. This solution had also been considered in the UK for the same problem in SGHWR.

The full implications of stagnation on shut-down heat removal in depressurization accidents in CANDU-type reactors cannot be deduced from the published literature. However, providing that the effects were confined to one, or very few channels, fuel melting due to this cause would be within the overall safety philosophy for a CANDU-type reactor on which Option II of Section 6.4 is based. It also follows from the discussion in Appendix I that the maximum acceptable probability of pressure circuit failures which

could lead to severe stagnation effects in a single channel would have to be shown to be less than, say, 10^{-3} per reactor year; this value is based on the assumption that some moderately reliable device would be provided to mitigate single channel stagnation. If no such device were provided then, for the relatively small diameter pipework on the inlet side of the fuel channels (notably the feeder pipes), the maximum acceptable probability of failure might have to be substantially lower than for other small diameter pipework.

Detailed analysis will be required to confirm that stagnation effects on a larger scale cannot occur due to failures of the larger diameter pipes on the inlet side.

Steam-binding has never been considered a significant problem in the development of the CANDU reactors but it should be noted that in the UK the opposite view was taken in relation to the problem in the development of the SGHWR. As a result provision was made to deliver emergency cooling water as a spray distributed throughout the length of each channel, by means of a sparge-pipe, which replaced the central fuel pin in a 37 pin cluster.

Thus, in relation both to steam binding and to stagnation effects on the performance of the shut-down heat removal systems, additional theoretical analysis and experimental work would almost certainly be necessary.

7.5 R and D Work Required to Support the Proposed Design

It is clear from the preceding discussion that some additional R and D work would be necessary to confirm that certain proposed design features would have both adequate performance and adequate reliability. Before summarizing these requirements, it is desirable to consider whether the CE design would be more susceptible to damage due to operator error than an LWR. This aspect is discussed in the next Section and the R and D requirements are summarized in Section 9.

8. SENSITIVITY OF THE SAFETY OF CANDU-TYPE REACTORS TO OPERATOR ERRORS

Although the exact sequence of events which led to severe fuel damage in the "Three Mile Island" reactor may not be known for several months, there seems to be little doubt that inappropriate procedures during abnormal operation had a substantial effect on the severity of the fault sequence.

Quantification of the probability of major errors by the operator is extremely difficult but in a comparison between the safety of LWRs and of CANDU-type reactors it is useful to consider the effects of similar types of error on each system. viz:

(a) Errors leading to a sudden increase in reactivity.

From the reliability point of view, errors of this type should be rare events, consequently the lower reliability of the single shut-down system of an LWR is usually considered to be adequate to reduce the probability of fuel damage to an acceptably level. I.e., in this respect the higher reliability provided by the dual systems in the CANDU-type reactors might be regarded as immaterial. Nevertheless it would be a positive advantage of the CE design, if operator errors led to a relatively high frequency of reactivity faults. The positive temperature coefficient of the CANDU-type reactor is more likely to lead to a situation in which the response of the shut-down system is insufficiently rapid to prevent some fuel damage; the greater potential hazard of primary circuit failure, due to interaction between the fuel and the pressure envelope, would then become important. However, response of the system in fault conditions of this type is purely automatic. Consequently, operator errors, such as failure to maintain correct trip settings, would be no more significant than in LWRs, providing that the response of the system, in the design conditions, were sufficiently rapid.

(b) Errors leading to inadequacy of shut-down heat removal.

If it is assumed that similar errors would lead to similar degrees of fuel damage in both types of reactor, the CANDU-type of reactor would, in general, be more sensitive to errors, due to the proximity of the fuel to the primary pressure circuit envelope (as in the case of reactivity faults). However, if it can be firmly established that radiant heat transfer to the moderator would be sufficient to prevent fuel damage proceeding to fuel meltdown and pressure tube failure, as is claimed in Ref. 25, then the CANDU-type of reactor could be regarded as having a better resistance than the LWRs to operator errors of this type. However, as indicated in Section 7.4, above, the description of the transient analysis which is available in the open literature leaves some doubts as to the validity of this claim for the CANDU-type reactors.

Overall, therefore, the CE design for a CANDU-type reactor has some potential advantages over current LWR designs, so far as resistance to operator errors is concerned. However, further work is required to confirm this.

9. SUMMARY OF R AND D WORK REQUIRED IN RELATION TO DESIGN FEATURES OTHER THAN THE PRESSURE TUBES

In Section 6 the R and D work in relation to pressure tube integrity was identified. From the discussion in Sections 7 and 8 it will be apparent that some additional R and D work is required in order to substantiate other parts of the design. Although the discussion in Sec. 7 is in terms of a particular set of design options, the range of R and D work required, in areas other then pressure tube integrity, would be similar if any other likely set of design options were adopted. The main topics may be summarized, in order of priority, as follows:

(a) Adequacy of performance of the emergency cooling systems in loss of coolant accidents, without stagnation;

(b) Effectiveness of moderator as an alternative emergency cooling system, in partial and total loss of coolant accidents;

(c) Adequacy of the emergency cooling systems for loss of coolant accidents in which stagnation in one of more channels could occur;

(d) Adequacy of natural circulation, including situations in which the fuel cladding is temporarily overheated;

(e) Development of alternative sensors to increase the diversity of the reactor shutdown systems; and

(f) Reliability analysis to confirm that the design of the shutdown and the residual heat removal systems which are proposed will be adequate.

Detailed discussions with Canada and other countries who have developed pressure tube reactors to at least the demonstration plant stage may reduce the amount of new R and D work required to support the CE design.

10. CONCLUSIONS

The main concern about the safety of CANDU-type reactors, as compared with LWRs, stems from the difference in the nature of their primary coolant circuits; the presence of the pressure-tubes in the former introduced a range of potential fault conditions that either do not occur in an LWR or whose consequence, in that type of reactor, would be less serious.

Comparison between the two types of reactors is made more difficult by the absence of detailed information about the CANDU-type of reactor in the published literature and by a lack of precision in statements concerning the importance attributed to the integrity of the pressure tubes. However, by postulating specific assumptions on which this aspect of the design of a CANDU-type reactor would be based, it has been possible to compare pressure circuit integrity with that of the LWRs. This comparison, which is mainly on a quantitative basis, leads to the definition of an R and D program which, if successful, would demonstrate parity of safety between the CANDU-type reactor and the LWRs, so far as primary circuit integrity is concerned. However, this demonstration will require more extensive theoretical analysis and experimental investigation of three main areas of pressure tube reactor technology than appears to have been carried out hitherto.

These areas are:

(a) conditions which affect critical crack length in the zirconium alloys likely to be used for pressure tubes;

(b) the effect of pressure tube failure and of fuel bundle ejection on the remainder of the reactor.

(c) the probability of propagation of failure of one pressure tube to one or more of its neighbors, in a variety of initial conditions.

Seismic effects do not appear to present insurmountable problems in a CANDU-type reactor but response to very severe earthquakes, which hav a probability of occurrence below that usually associated with the "design-basis" earthquake, should be investigated to see whether there are any unusual problems.

In general it should be easier to demonstrate comparability of safety in relation to other types of major potential faults but in this respect two difficulties have to be considered. These are:

(i) the adequacy of performance of the EECS, with particular reference to the possibility of steam binding and of temporary stagnation in one or more fuel channels; and

(ii) the need for more precise definition of the safety margins which would exist in various fault conditions, on account of the possibility of damage to the pressure tubes. It should be noted that consideration will have to be given to both the steady state rating and temperature distributions and to the transient temperature changes.

Additional R and D work is likely to be required in both of these areas.

It is possible that, if the safety of the CANDU-type reactors were found to be inferior to that of the LWR in one or more of the aspects discussed above, this deficiency could be offset by the following.

(i) The reduced severity of potential reactivity accidents, stemming from the much lower surplus reactivity present in the core during normal operation

(ii) The greater resistance to fuel meltdown which may be provided by the near-permanent presence of the moderator. However, analysis additional to that which has been carried out for CANDU may be necessary to demonstrate with sufficient confidence that this additional line of protection is, in fact, effective.

Overall, therefore, it is concluded that a relatively small amount of additional R and D work would be required to support a license application for a CANDU-type of reactor, similar in design to that proposed by CE, to be built in the U.S, providing that the approach to safety embodied in the choice of "Option III" as a basis for design is acceptable for licensing power reactors in the US. If this approach is not acceptable, the amount of R and D required would be substantially increased and it is doubtful whether "Option I" (probability of gross failure of pressure tubes so low that it can be ignored) is a viable basis for design.

REFERENCES

1. Speis, T. P., Meyer, et al., Report on visit to Combustion Engineering Inc., Dec 1978.

2. See footnote on pages 1 and 79.

3. Cave, L., Comments on "Preliminary Evaluation of Licensing Issues Associated with US sited CANDU-PHW. Nuclear Power Plant - ANL report 77-97" UCLA report (unnumbered) 1978.

4. UASEC "Reactor Safety Study" USAEC Document, WASH-1400, 1974.

5. Jackman A. H. and Dunn, J. "Delayed Hydrogen Cracking of Zirconium Alloy Pressure Tubes", AECL Report-5691, Oct. 1976.

6. Pease, L., and Sawai, S., "Heavywater Moderated Pressure Tube Reactor Safety" AECL-5856, Aug. 1977.

7. ACRS "The Integrity of Pressure Vessels for LWR." ACRS Report Jan. 1974.

8. See footnote on page 13.

9. See footnote on page 13.

10. Ross-Ross P. A. et al., "Some Engineering Aspects of the Investigation into the Cracking of Pressure Tubes in the Pickering Reactors", AECL Report-5261, January 1976.

11. Nucleonics Week. August 17, 1978, page 8.

12. Shima, S. and Akebi, M., "The Fugen Reactor-Construction and Startup". Trans. Second Pacific Basin Conference, ANS, September 1978.

13. Lidiard, A. G., and Williams, M., "A Simplified Analysis of Pressure Vessel Reliability." J. Br. Nucl. Energy Soc. 1977, 16 July, p. 207.

14. Page, R. D., "Canadian Power Reactor Fuel", AECL Report 5609, March 76.

15. Various Authors. Papers on "Reactor Safety Research Programs" - ANS Topical Meeting on Thermal Reactor Safety, Sun Valley, Idaho, August 1977.

16. Miller, J. M., "Incident at the Lucens Reactor" Nuclear Safety, Vol. 16, Jan/Feb 1975/76.

17. Harty, H., "Plutonium Recycle Test Reactor (PRTR) - "Operating Experience and R & D", Proc. of IAEA Symposium on "Heavy Water Reactors" Vienna 1967, p. 161.

18. Freshley, M. D., Wheeler, R. G., et. al., "Investigation of the Combined Failure of a Pressure Tube and Defected Fuel Rod in PRTR", Battelle N.W. Report BNWL-272, May 1966.

19. Ross-Ross, P.A., "Experiments on the Consequences of Bursting Pressure Tubes in a Simulated NPD Reactor Arrangement", AECL-1736, Fbe. 1963.

20. Ross-Ross, P. A., "Experiments on the Consequences of Bursting Pressure Tubes in a Simulated Power Reactor Arrangement. Proceedings of 2nd Ed. SMiRT Conference. Berlin, Sept. 1973 (Paper F2/2).

21. Holtbecker, H., et.al., "Consequences of the Rupture of a Pressure Tube or of a Complete Channel in an ORGEL-Type Reactor EUR-4493e (June 1970).

22. Famigbetti, M., et. al., "Pressure Bursts Due to Power Channel Explosion in a Pressure Tube Reactor", Energio Nucleare" Vol. 23, No. 2, Feb. 1976 p. 98.

23. Lemactne R., and Peuchman A., "Etude d l'explosion d'un tube de force, dans un reacteur nucleaire". Energie Nucleaire, Vol. 5, 1963, p. 355.

24. Hayomigu, Yel al. "Experimental Studies of Dynamic Forces Caused by Pipe Rupture, PNC-N341 74-15, November, 1974.

25. Rogers, J. T., "CANDU Moderator Provides Ultimate Heat Sink in a LOCA". Nucl. Eng. Intl.

APPENDIX 1

Derivation of Targets for Pressure Tube R and D Program

For CANDU-Type Reactor

1. Introduction

In order to define the extent and depth of an R and D program it is useful to carry out a simple risk-target allocation analysis. To do this it is necessary to define an overall risk-target which is believed to be acceptable and then to allocate this, using whatever previous experience is available between the various systems and structures. Some examples of the application of this method to other systems are given in References 1, 2, 3, and 4.

2. Application of Risk-Target Allocation Analysis to a CANDU-Type Reactor

For the purposes of this analysis the principal assumptions are as follows.

(a) The maximum acceptable median value for the overall probability of very large releases to atmosphere (i.e., 10 percent or more of the inventory of gaseous and volatile fission products) is 10^{-6} per reactor year.

(b) The probability that the containment would retain at least 99 percent of the volatiles in the event of core meltdown is 10^{-1} per event (median value).

It follows from these assumptions that the maximum acceptable median value for the probability of core meltdown (10 percent and/or more of the channels) is 10^{-5} per reactor year.

It is desirable that the acceptable confidence limits on this probability should also be stated.

However, there is no point in specifying requirements that it will not be possible to attain in practice.

Thus it is assumed that the upper and lower 95 percent confidence limits for the maximum acceptably probability of core meltdown are 10^{-4} and 10^{-6} per reactor year.

As WASH-1400 (Reference 5) and subsequent discussions (e.g., Reference 6) have shown, it is likely that the 95 percent confidence limits will be at least a factor of 10 on either side of the median.

A possible allocation of this risk target for a CANDU-type reactor is shown in Table A1.1. Also shown in the Table are the estimated frequencies of demand and the corresponding reliabilities required from the various safety systems.

Table A1.1. Estimated Maximum Acceptable Unreliabilities for CANDU-Type Reactor, Based on Preliminary Risk Allocation and Frequencies of Demand.

Serial No.	Reactor Sub System	Risk Allocation per r. yr.	Frequency Demand per r. yr.	Minimum Acceptable Unavailability per Demand
1	Shutdown system	$1x10^{-6}$	1^{ϕ}	$1x10^{-6}$
2	Residual heat removal pressurized*	$4x10^{-6}$	6	$7x10^{-7}$
3	Residual heat removal depressurized*	$1x10^{-6}$	$1x10^{-2\dagger}$	1x10-4
4	Local protection systems (e.g., P-T leak detection)	see text	see text	see text
5	External hazards	$1x10^{6}$	$1x10^{-4}$	$1x10^{-2}$
6	Critical structures (including P-tubes)	$2x10^{-6\dagger}$	not applicable	see text
7	Contingency	$1x10^{-6}$		
	Total	$1x10^{-5}$		

* In these cases the risk allocation has to cover both "starting reliability" and "running reliability" (See text).

ϕ It is assumed that ample relief valve capacity is provided.

$\dagger$ This allocation is consistent with the more general argument used in Section 3 of main text.

† Excluding relief valve failure

In making this allocation a number of factors have had to be taken into account. The principal ones are as follows.

(a) It is axiomatic that to allocate a very large fraction of the total target to any one subsystem, for which it is anticipated that difficulties will be encountered in achieving adequate reliability, is likely to be self-defeating as the difficulties are likely to be transferred to the other systems.

(b) The "Maximum Acceptable Unavailability Per Demand" for Serial "i" (denoted by "u_i") is defined by the relationship

$$u_i = \frac{p_i}{f_i}$$

where p_i is the fraction of the risk allocated to Serial "i" and f_i is the estimated frequency of demand.

(c) The estimated frequency of demand for the reactor shutdown system (1 per reactor year) is considerably lower than that estimated for the earlier LWRs in Ref. 6 (about 6 per reactor year); in making this estimate it has been assumed that improvements in balance-of-plant design would reduce the demand to a level closer to that achieved in the United Kingdom gas cooled reactor.

(d) "Residual Heat Removal" (Serials 2 and 3) has been divided into "pressurized" and "depressurized" because of the large difference in system requirements, and in frequency of demand, in the two cases. This enables a larger proportion of the target to be allocated to the pressurized case, where experience with other systems suggests that one of the major reliability problems would be encountered. In both cases it is necessary to distinguish between "unavailability"

(i.e., starting unreliability) and reliability in running after a successful start.

(e) "Local Protection Systems", which include systems for detection of leakage from a partially failed pressure tube and for the detection of channel blockage, appear in the target allocation owing to the sensitivity of the system to gross failure of a pressure tube, as discussed in the main text. However, no quantitative allocation is made as these faults are covered by Serial 6.

(f) "External Hazards" (Serial 5) appear separately in the allocation so that the response of the system in the relatively rare event of a hazard exceeding its design level can be considered separately.

(g) As discussed elsewhere (e.g., Ref. 2) in most reactors failure of certain structures can lead to a situation in which the reactor protection systems cannot prevent core melt down (e.g., failure of the pressure vessel of an LWR).* It is convenient to describe these as "critical structures" (Serial 6). This aspect of the design is of particular importance in the case of pressure tube reactor, accordingly, a detailed allocation for the critical structures is described in the next section.

(h) A contingency allowance (Serial 7) is provided so that, if unexpected difficulties arise with a particular sub-system, these can be eased without having to make a series of minor adjustments elsewhere in the analyses.

3. Allocation of Sub-Target for Critical Structures in a Pressure-Tube Reactor

In addition to the pressure-tubes themselves, which, as discussed in the main text, may prove to be particularly sensitive items, there are

*Private communication, Dr. T. P. Speis (NRC) - L. Cave (UCLA), January 17, 1979.

other structures such as the steam generator vessels to consider. In view of the large amount of energy stored in these, a gross failure could have severe effects on the remainder of the primary circuit and on the containment structure. Accordingly, only half of the total allocation for the critical structure is allocated to the pressure tubes, as a group.

As discussed in the main text, it is necessary to distinguish between four different cuases of gross failure of pressure, viz:

(i) self-defects leading to "leak-before-break" situation, but accompanied by a failure to detect the leak before the crack reaches a critical length;

(ii) self-defects leading to "break-before-leak", i.e., the crack reaches a critical length before it becomes a through crack;

(iii) single channel faults, leading to gross pressure-tube failure; and

(iv) whole reactor faults which do not cause significant fuel damage in the great majority of channels but may cause sufficient damage in the hottest channel to result in gross failure of its pressure tube.

Bearing in mind that in the case of Causes (i) and (iii) the reliability of the detection systems can be taken into account, these Causes can be given a smaller part of the target allocated to this part of Serial 6 than that allocated to Cause (ii). Similarly, in the case of Cause (iv) since only one, or a few channels can be at risk at any one time, this too can be given a smaller part of the target allocated to this group of faults.

A preliminary target allocation, consistent with these factors is shown in Table A1.2. The numbers shown in the Table are based on the assumptions that the probability of gross failure of one pressure-tube

Table A1.2 Proposed Target Allocation for Specific Causes of Gross Failure of Pressure Tubes. (Option I)

Serial No.	Cause of Gross Failure	Proposed Allocation per r. yr.	per t. yr.	Equivalent failure rate	Remarks
1	Leak-before-break	$1x10^{-7}$	$1x10^{-10}$	$1x10^{-6}$ per t. yr.	See Note 1
2	Break-before-leak	$1x10^{-7}$	$6x10^{-9}$	$1x10^{-9}$ per t. yr.	
3	Single channel faults	$1x10^{-7}$	-	$1x10^{-5}$ per r. yr.	See Note 2
4	Whole-reactor faults	$1x10^{-7}$	-	$1x10^{-7}$ per r. yr.	See Note 3
	Total	$1x10^{-6}$			

Note 1. Equivalent failure rate (EFR) for Serial 1 is based on the assumption that a reliability of 10^{-4} failures per demand would be attainable for the leak detection system.

Note 2. EFR for Serial 3 is based on the assumption that the frequency of single channel faults would not exceed one per reactor year and that a reliability of 10^{-2} failures per demand would be attainable for the blockage detection system.

Note 3. EFR for Serial 4 is based on the assumption that the frequency of whole reactor faults leaking to severe transients is one per reactor year.

in the entire set should not exceed 1×10^{-6} per reactor year and that, as explained in the main text, in evaluating "Option I" the conditional probability of exceeding 10CFR.100 conditions in the event of a tube failure is unity. The implications of this proposed risk-allocation for reactor design are discussed in the main text.

4. Allocation of Risk Target for "Option II" of the Main Text

In the preceding Section of this Appendix, a risk-allocation was derived suitable for evaluating the reliability requirements for a design based on Option I, as defined in the main text; in this Section a risk-allocation is derived for use in evaluating the reliability requirements for a design based on "Option II". As explained in the main text, in the case of Option II the very conservative assumption is made that the probability of gross failure of a pressure tube per reactor year is unpredictable, thus a high value (unity) has been used.

As Option II is an alternative to Option I the risk allocation of 1×10^{-6} per reactor year allocated to structural failure of the pressure tubes can be re-allocated to Option II. However, in Option II we have to consider two distinct situations.

Situation 1, failure of a single tube, which does not propagate to any other tubes, leads to an unacceptably large release

Situation 2, failure of a single tube propagates to a large number of other tubes and leads to an unacceptably large release.

Some preliminary calculations are sufficient to show that the main difficulties would arise in demonstrating an adequately low probability of propagation in Situation 2. Consequently only 10 percent of the target (i.e., 1×10^{-7} per r.yr) has been allocated to the first situation.

In Situation 1 it is reasonable to assume that the conditional probability of failure of the containment is considerably less than the value of 0.1 per event which has been assumed in Sec. 2 of this Appendix. For Situation 1 this conditional probability is assumed to be 1×10^{-3} per event. Thus the target can be increased from 1×10^{-7} to 1×10^{-5} per r. yr.

Complete meltdown of a single channel or prolonged heating of the fuel

an air/steam atmosphere might release nearly 100 percent of the gaseous and volatile fission products in that channel. However, a high proportion of these would have to escape to atmosphere in order to exceed 10 CFR.100 limits. This would only be likely to occur if the calandria had drained before the fuel over heated, so that little partitioning between air and water would occur. As discussed in the main text, this is also likely to be a necessary condition for overheating of the fuel.

Thus, in Situation 1 it would be necessary to show that the conditional probability of the combined sequence: "Single pressure tube fails; calandria damaged and drained of water, and fuel bundles left uncooled in air/steam mixture" was less than 10^{-5} per event.

In Situation 2, the conditional probability of containment failure cannot be assumed to be better than $1x10^{-1}$ per event. Thus the target allocation is about $1x10^{-6}$ (actually $9x10^{-7}$) per reactor year, and it would be necessary to show that the conditional probability of propagation of the initial failure to a large proportion of the other tubes, followed by overheating of the fuel, was less than $1x10^{-6}$.

It should be noted that, if no credit were taken for the containment, the target would be reduced to $1x10^{-7}$ per r. yr which is the lower bound for the estimated annual probability of catastrophic failure of an LWR pressure vessel. Thus, if it were assumed that in the event of a catastrophic failure of an LWR pressure vessel there would be a high probability of containment failure, the target derived for Situation 2 would give comparatility of safety between the CANDU-type reactor and LWRs, in respect of gross failure of the primary circuit.

5. Allocation of Risk Target for "Option III" of the Main Test

5.1 Cases to be considered

Option III, as defined in the main text, requires the allocation of

targets for 2 distinct cases in which propagation is assumed to occur and, as in Option II, in order to obtain a satisfactory overall risk for the plant, it is also necessary to consider the case in which only one channel of fuel could overheat and give rise to a moderate size release to the atmosphere, owing to a defect in the containment. Thus we have the following cases:

Case 1. Gross failure of a single pressure tube, with overheating of fuel but no propagation

Case 2. Gross failure of a single pressure tube, with indirect propagation to not more than 9 others

Case 3. Gross failure of a single pressure tube, with direct propagation to not more than 9 others.

All Cases have to be considered as "Structural Failures", they must therefore, meet jointly the target of 10^{-6} per reactor year identified in Section 3 of this Appendix, but the definition "critical structure" so far as the pressure tubes are concerned, becomes "failure of 10 pressure tubes" instead of only one, in Cases 2 and 3. In Case 1 a lower probability of containment failure is assumed. A possible allocation of this target between the 3 cases is as follows:

Case 1 1×10^{-7} per reactor year

Case 2 3×10^{-7} per reactor year

Case 3 6×10^{-7} per reactor year.

The corresponding maximum acceptable conditional probabilities are derived for each case in the following sections.

5.2 Discussion of Case 1

In Case 1 it is reasonable to take a lower value for the conditional probability of containment failure than the value of 10^{-1} on which Table A1.1 is based. Moreover, since by definition only one pressure tube fails in Case 1 the maximum fission product release is limited. These two factors

are taken into account by assuming that the conditional probability of containment failure is 10^{-3} instead of 10^{-1}. Thus a nominal allocation of 10^{-7} per r. yr to this case can be increased to 10^{-5} per r. yr, as in Option II.

As discussed below (Sec. 5.5), difficulties would probably be encountered in demonstrating that the probability of gross failure of at least one pressure tube in the set is less than 10^{-3} per reactor yr., and this value has been assumed in the analysis of all three cases. Thus, the maximum acceptable conditional probability that, in this case, the fuel element would melt, or would be overheated for a long period in an air/steam atmosphere, is $\frac{10^{-5}}{10^{-3}} = 10^{-2}$ per event. As discussed in the main text, fuel melting or overheating would be unlikely to occur unless sufficient damage had been caused to the calandria to drain it almost completely.

5.3 Discussion of Case 2

The behaviour of the reactor following gross failure of one pressure tube has not yet been examined in sufficient detail to identify all the possible sequences which would fall into Case 2. However, one such sequence has been discussed in the main text. In this sequence at least one fuel bundle lodges between a calandria tube of the other loop of the primary coolant circuit; the calandria is assumed to drain; the calandria tube and its associated pressure tube then fail and, in circumstances more favorable than in a water filled calandria, direct propagation to other tubes ensues.

In this Case, the maximum acceptable conditional probability of sequences leading indirectly to propagation would be $\frac{3\times10^{-7}}{10^{-3}} = 3\times10^{-4}$ per event.

5.4 Discussion of Case 3

In this case the maximum acceptable conditional probability of direct propagation to several other tubes would be $\frac{7\times10^{-7}}{10^{-3}} = 7\times10^{-4}$ per event.

The relationship between the probability of propagation to at least one tube and to some specified number (e.g., 10) is discussed in Appendix 2.

5.5 Derivation of maximum acceptable probability of gross failure of pressure tubes, for use in risk-allocation analysis

In the analysis of Cases 1, 2 and 3 it has been assumed that the maximum acceptable probability of gross failure of a pressure tube is 10^{-3} per reactor year. This assumption leads to maximum acceptable condition probabilities for the various other events and sequences that have to be considered which are not unreasonably small. The justification for the value of 10^{-3} per reactor year is provided below.

Considering the same four potential causes of gross failures as in Sec. 3 above, we have:

(a) Leak-before-break, with failure of leak detection system

(i) Random failures 10^{-3} per tube yr. ≈ 1 per reactor year

(ii) Type-failures - 10^{-2} per reactor yr, at 10 failures each, ≈ 0.1 per reactor yr

(iii) Failure of leak detection system, 10^{-4} per demand (assuming that there are 2 fully independent systems)

Conditional probability of gross failure is 10^{-4} per reactor yr.

(b) Break-before-leak

The probability of this event is assumed to be 10^{-6} per tube yr. or 10^{-3} per reactor yr.

The probability per tube year is as high as the maximum probability usually assumed for catastrophic failure of an LWR reactor pressure vessel. Balancing the simpler structure of the tube against the better known properties of the vessel material provides some qualitative justification for the assumed value. However, it is doubtful whether the assumed value for either the vessel or the tube can be demonstrated satisfactorily by reliability analysis.

(c) Single Channel faults

As the contribution to the total value of the maximum acceptable conditional probability for the "break-before-leak" events is 10^{-3} per reactor yr. due to latent defects in the pressure tubes, it is unnecessary to establish a probability lower than, say, 2×10^{-5} per reactor yr. for the single channel faults, since any smaller value would make the contribution insignificant.

This value could be regarded as made up from a probability of 2×10^{-3} per reactor year for the fault conditions (equally divided between channel blockage and "stagnation" faults) together with a probability of 10^{-2} per event for failure of the detection system to reveal the fault in the case of channel blockage and a probability of 10^{-2} per event for failure of whatever device is provided to prevent, or mitigate, stagnation.

(d) Whole-Reactor faults

As in the previous case, a small nominal value is proposed, 1×10^{-5} per reactor year appears to be a reasonable choice.

This value could be regarded as made up in the following way:

(i) Probability of severe reactor transient, 0.3 per reactor yr.

(ii) Probability that transient temperature rise and "hot-spot" factors have been so underestimated that local clad melting occurs in the hottest channel, 1×10^{-4} per event.

(iii) Probability that local clad melting escalates to channel blockage and fuel melting, 0.3

It will be seen that in order to derive an overall value for the conditional probability it has been necessary to make several assumptions. However, it should be possible to verify all of these, except perhaps that made about "break-before-leak" faults, in the course of the development

program. Nevertheless, should further considerations (of the development program needed to verify these assumptions) indicate an excessively heavy expenditure on one or two items, an alternative set of values could be derived which might lead to a reduction in the cost of development.

References

(Appendix I)

1. Cave L., Probability Methods for GCRs,"Nuclear Engineering" October 1968.

2. Cave L., "A Comparative Study of the Safety of Liquid Metal Cooled and Gas Cooled Fast Reactors". ANS Topical Meeting on Fast Reactor Safety. Los Angeles 1974.

3. Cave L., "The Relationship between Reliability and Safety in NPP", IAEA Symposium on Reliability of NPP", Insbruck 1975.

4. Cave L., UCLA paper on verification of natural circulation FFTF, 1978.

5. U.S.A.E.C. Reactor Safety Study, WASH-1400, 1974.

6. Lewis H. A., et al., "Risk Assessment Review Group report to the USNRC" NUREG-CR-0400.

Appendix 2. Derivation of an Acceptable Probability of Propagation of Pressure Tube Failure

1. Introduction

Gross failure of a single pressure tube, followed by meltdown of the fuel in that channel, would not necessairily be an unacceptable situation; in fact, providing that the containment retained some measure of effectiveness (e.g. as claimed in WASH-1400 for many core meltdown sequences in PWRs) meltdown of some 10 percent (about 70) of the channels might be acceptable.

Unless failure of one tube leads, on average, to the failure of at least one other on every occasion, propagation could not continue indefinitely. The relatively few experimental results which have been published indicate that the probability of propagation of the initial failure to even one of the immediately adjacent tubes is quite low (less than 0.3, see main text). This probability is denoted in this Section by p_i. If it is assumed that propagation of the initial faliure to as many as N tubes is not necessarily unacceptable, the probability of this occurring can be estimated for only given value of p_i; a simple model for this purpose is derived in the next section.

2. Probability of Propagation of Initial Failure to (N-1) Other Tubes.

It is assumed that propagation would be due to effects such as strikes by high speed fragments, mechanical damage due to "pipe whip," or overheating due to lodging of an ejected fuel bundle against the calandria tube, as indicated in the main text. For simplicity it is assumed that the

probability of propagation from one tube to its neighbors is the same in each "generation" of failures. This assumption should be conservative for two reasons, viz:

(a) Propagation is assumed to occur by a "random walk" process, thus if many tubes were to fail, the chance of a strike against an unfailed tube would be reduced. Moreover, no account has been taken of "edge effects", which should also tend to reduce the probability of propagation.

(b) As tubes failed, primary coolant pressure would begin to fall; if the rarefaction waves created at the various breaches propagated round the circuit more rapidly than propagation proceeded across the core, then the membrane stresses in tubes struck in the later generations would have been reduced. In these circumstances the probability of failure would be reduced and, if failure were to occur, the process would be less violent and therefore less likely to propagate.

For simplicity it is assumed that the propagation process can be modelled by assuming that the failure of any one tube can lead to the failure of "i" additional tubes but the probability of this occurring, denoted by p_i, is less than unity.

Denoting the number of "generations" of propagation by "n", the total number of tubes which would have failed after n generations, N, can be written as

$$N = 1 + \frac{(n - 1)}{i - 1}.$$

The values of N for various values of "i" and "n" are shown in Table A.2.1.

Table A.2.1. Total Number of Pressure-Tubes Ruptured by Propagation, N, as a Function of the Number of "Generations" of propagation, n, and the number of tubes failure per initiating failure, i.

No. of generations, n	Total Number of Failed Tubes, N			
	i = 1	i = 2	i = 3	i = 4
2	2	3	5	6
3	3	8	14	22
4	4	16	40	86
5	5	32	122	342
6	6	64	-	-
7	7	128	-	-

The principal objective, in terms of defining a test program to establish the probability of propagation, is to determine the values for p_i which correspond to overall conditional probabilities of 10^{-3} to 10^{-4} of propagation to some specified number of channels (e.g., N~10 or N~100).

The probability of propagation continuing for "n" generations, if each initiating gave rise to "i" failures, with probability p_i, would be p_i^n. In practice the situation would be more complicated but this simple approach provides a useful starting point.

The limiting values of p_i which would have to be demonstrated experimentally to show that the probability of propagation to about 10 and to about 100 tubes (i.e., N~10 and N~100) is:

(a) less than 10^{-3} per reactor year,

(b) less than 10^{-4} per reactor year,

are shown in Table A.2.2.

Table A.2.2. Limiting Values of p_i, the Probability of Propagation to 'i' Tubes as the result of one Tube failure, for Specific Values of N, and p_N

No. of tubes failing per Initiating event	N ~ 10				N ~ 100			
	$p_{10} = 1 \times 10^{-3}$		$p_{10} = 1 \times 10^{-4}$		$p_{100} = 1 \times 10^{-3}$		$p_{100} = 1 \times 10^{-4}$	
i	none*	p_i	none	p_i	none	p_i	none	p_i
1	10	0.5	10	0.4	100	0.95	100	0.87
2	3	0.1	3	0.05	6	0.3	6	0.2
3	3	0.1	3	0.05	5	0.25	5	0.15
4	2	0.03	2	0.01	4	0.2	4	0.1

* "n_{gen}" is the number of propagation generations corresponding to the specified value of N.

Appendix 3. Some Comments on the Interpretation of Existing Test Data for Propagation of Pressure Tube Failures

The existing test data, described in Section 6.1.1.1 of the main text, concerning the propagation of pressure tube failures show that in 16 tests, with a simulation of a CANDU core, there were no cases in which propagation occurred. Possible interpretations of these results are as follows:

(a) Although failure of the pressure tubes used in the tests may have given rise to fragments capable of causing propagation, in these tests either, by chance, the more dangerous fragments passed harmlessly between the adjacent tubes or struck at such oblique angles that propagation did not occur.

(b) In reactor conditions, the number of fragments capable of causing propagation may be substantially greater e.g., due to embrittlement caused by irradiation or hydriding of sound material or to the inadvertent inclusion of unsound tubes; this "unsoundness" could be due to an error in material composition or to an error in the fabrication process.

(c) In reactor conditions, propagation could be due to causes other than fragment strikes, which were not revealed in the test, owing to differences in conditions (e.g., the duration of flow from the break in the first tube was much less in the tests than it would be in the reactor situation and the unsupported length of tube, in some of the tests, was less than in the reactor; consequently the possibility of tube failure due to pipe which was not fully explored). It should be noted also that in reactor conditions, as discussed in Section 6.1.2.2 of the main text, the ejection of fuel bundles could be a potential source of damage, leading to propagation.

Detailed discussions of these tests with AECL, and discussion of the unreported UK tests with UKAEA might clarify some of the uncertainties in interpretation referred to above.

NRC FORM 335 (7-77) U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER (Assigned by DDC): NUREG/CR-1113 UCLA-ENG-7953

4. TITLE AND SUBTITLE (Add Volume No., if appropriate)

Licensability of CANDU-Type Reactors in the United States

Subtitle: A Preliminary Assessment of the R and D Requirements

2. (Leave blank)

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)

L. CAVE

5. DATE REPORT COMPLETED: MONTH September YEAR 1979

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)

University of California at Los Angeles
Los Angeles, California 90024

DATE REPORT ISSUED: MONTH August YEAR 1980

6. (Leave blank)

8. (Leave blank)

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)

U.S. Nuclear Regulatory Commission
Office of Nuclear Reactor Regulation
Division of Systems Integration
Washington, D. C. 20555

10. PROJECT/TASK/WORK UNIT NO.

11. CONTRACT NO.

FIN No. B3004-9

13. TYPE OF REPORT: Technical

PERIOD COVERED (Inclusive dates): October 1, 1978 - September 30, 1979

15. SUPPLEMENTARY NOTES

14. (Leave blank)

16. ABSTRACT (200 words or less)

An assessment is provided of the R&D required to establish the licensability of a CANDU-type reactor in the U.S. It is shown that the bulk of the R&D effort should establish the integrity of the pressure tubes and the effects of the pressure tube failure on the remainder of the system. Three possible R&D program options are defined and discussed; it is concluded that one of these options is likely to require less R&D than the other two. The principle underlying this option is that the pressure tubes would be shown to have a moderately low probability of sudden, gross failure & that the effects of a single failure would not lead to unacceptable consequences.

In other areas where R&D work would be necessary, more of the problems would be similar to those encountered in LWR's, however, two novel problems are identified, viz:

(a) investigation of the effectiveness of the moderator as an alternative emergency cooling system;

(b) the effect of the difference in reactor configuration (horizontal heat source) on natural circulation.

Overall, it is concluded that a relatively small amount of additional R&D should be sufficient to support a license application to build a CANDU-type reactor in the U.S.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

HWR's; CANDU; Advanced Reactors; Licensability; R&D needs

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT

No restrictions on availability

19. SECURITY CLASS (This report): Unclassified

21. NO. OF PAGES: 96

20. SECURITY CLASS (This page): Unclassified

22. PRICE: $

NRC FORM 335 (7-77)