Paper number 72-CNA-102

REACTOR LICENSING AND SAFETY REQUIREMENTS

D.G. Hurst and F.C. Boyd
(Atomic Energy Control Board)

The Atomic Energy Control Board, in its reactor licensing, proceeds through the stages of Site Approval, Construction Licence and Operating Licence. The basic information requirements are outlined in the paper. With increasing experience there have been some evolutionary changes in design and operating requirements, although the radiation dosage criteria remain essentially the same. As an alternative to the conceptual division for safety evaluation into process systems, protective systems, and containment, a nuclear plant may now be regarded as composed of two groupings of process systems and safety systems. The target reliabilities for safety systems have been made somewhat more stringent. Some possible trends in safety criteria and licensing requirements are outlined.

Although considerable attention is given to effluents and to radiation exposures from normal operation, the licensing process will continue to concentrate on ensuring that the chance of a major release of radioactive fission products is negligibly small.

INTRODUCTION

The Atomic Energy Control Act gives the Atomic Energy Control Board broad powers which clearly should be used in the interests of public radiation safety. Accordingly, as the nuclear power program was getting underway, the Board published an order classifying nuclear reactors as "prescribed equipment" under the Act, and establishing the requirement for a licence. Both construction and operating phases are licensed, but at an early stage the applicant is required to provide information on the proposed site and reactor, in effect seeking assurance from the Board and its advisers that they see no fundamental bar to the eventual licensing.

Construction is defined as beginning with the pouring of concrete or erecting of essential foundations for the reactor proper. Issuance of a construction licence implies approval of the general design or design specifications as suitable for the site in question, but it does not mean that an operating licence will automatically be granted. In Canada details of design are normally still under consideration when civil construction begins and these details are kept under review as construction proceeds.

The operating licence authorises operation of a plant within certain defined limits, including the use in the reactor of fuel and heavy water which must be obtained under separate Board orders. Start-up and the early operation are usually covered by an interim operating licence with special conditions and restrictions.

In 1956 the Board created the Reactor Safety Advisory Committee to advise it on the health and safety aspects of nuclear reactors licensed by the Board. This Committee is composed of senior engineers and scientists chosen because of their individual competence, together with technical representatives of relevant federal and provincial departments and local medical officers of health. The representatives vary, depending upon the location of the station. No reactor has been licensed by the Board without first being reviewed and approved by this Committee. The extent and detail of the Committee's review depends, of course, on the complexity, novelty, and size of the project.

The Board staff performs a role supporting and complementary to that of the Committee in the detailed review of design and analysis. It assists the Committee by reviewing the submitted documents and giving advice on technical matters. It also undertakes inspection and compliance reviews at the sites, and approves design and procedural changes within the terms of the licences.

LICENCE REQUIREMENTS

Although *site approval* is not a formal licensing stage, applicants are encouraged to hold exploratory discussions with the Board staff and the Reactor Safety Advisory Committee when requesting approval of a site. At this time the entire project may be in a

very preliminary stage and it is necessary only that the plant size, reactor type, and proposed containment method be identified, together with general information concerning the actual or proposed site or sites.

More detailed information pertaining to the site, such as land use, population, principal sources and movements of water, water usage, meteorological conditions, and geology, is required when a formal request is made for a *Construction Licence.* Technical information on the reactor and auxiliary equipment is also required with the application for a Construction Licence, and this is usually submitted in a comprehensive report sometimes termed a "Safety Report" combining the design description and specifications and the preliminary analyses of accidents. Although many aspects of the design may not be firm, the design description and specifications must provide a clear picture of the plant design and be sufficiently complete to enable independent analyses to be done. The Board has prepared, as a guide for prospective licensees, a document entitled "Requirements for Safety Report".

The granting of a construction licence does not imply acceptance of every argument or conclusion in the Safety Report. The Reactor Safety Advisory Committee and the Board staff, while not accepting the specific claims made for certain aspects of the design, may conclude that they are adequately safe. For example, the report may claim an extremely low unreliability for a component system, whereas the Committee, while not endorsing the value quoted, might accept the system as adequate.

Since many details of the design may be undecided at the time the construction is licensed, subsequent submissions and revisions to the Safety Report are required as the design progresses. The submission and acceptance of such information may be made a necessary condition for carrying the construction beyond a certain stage. In general, the design descriptions and supporting analyses of major reactor systems must be submitted well before these systems are installed. From time to time throughout the period of design and construction the Reactor Safety Advisory Committee and the Board staff meet with the applicants.

The issuing of the *Operating Licence* implies acceptance by the Board of the safety aspects of the plant as constructed. Permission for full operation may be preceded by two substages of authorisation: 1) permission to load fuel; and 2) permission to start up. Prior to loading of fuel, all reactor systems affected by having the fuel in the reactor must have been satisfactorily tested as far as it is possible to do so. The permission to start up requires assurance that all reactor and auxiliary systems have been constructed according to the design and have been satisfactorily commissioned to the extent possible prior to start-up of the reactor. The design description and accident analyses must have been brought fully up-to-date. The operating procedures, the organisation of staff and senior members of the operating staff, must all have been approved, and there must be an approved procedure for handling emergencies involving radiation.

The operating licence includes (either by listing or by reference) conditions and restrictions on the level of radioactive effluents from the plant, the test conditions, and on allowable modifications to the plant and procedures. The Board receives formal annual reports on operation, radiation exposures and radioactive effluents, but the staff reviews these on a continuing basis.

SAFETY PRINCIPLES AND CRITERIA

Background

The major hazard, of course, arises from the large inventory of radioactive fission products produced and contained in the fuel. Therefore, all criteria are directed (i) toward minimizing the chance of mechanical failure of the fuel and (ii) to preventing or minimizing the escape of fission products from the plant if fuel failure occurs. The chance of fuel failure depends upon the ability to ensure that the power produced in the fuel and heat removal from the fuel are properly controlled. The escape of fission products can be prevented by ensuring that there are a number of high integrity barriers, the most important of which is the final containment.

In specifying the requirements to be met by the designer and operator a very useful concept was developed in which the nuclear plant was considered to consist of three systems: the process system, the protective system, and the containment system. If these systems are independent of one another, and if each is of a reasonable reliability, the chance of a significant release of radioactive material to the public domain can be kept extremely small.

For the *process system* the aspect of most concern from the safety viewpoint is the frequency of occurrence of faults which could lead to fuel failure, whereas for each of the *protective* and *containment* systems the important parameter is the unreliability defined as the fraction of time during which the system would not perform its intended function.

Progress was only possible in the application of this philosophy when it was made quantitative. The applicants were required to demonstrate that the frequency of occurrence of significant faults in the process system should be less than 1 per three years, and that the unreliability of the protective devices and of the containment divisions should each be less than $10^{-2.5}$.

The International Commission for Radiological Protection (ICRP) recommends that individual members of the public should not be exposed to more than 0.5 rem/yr to the whole body, not including exposure from natural background or medical procedures, and with ancillary recommendations for special cases. By 1965, the concept of the plant as three systems became associated with dose limits. The 0.5 rem/yr was accepted as the limiting dose to an individual at the boundary of the exclusion zone for normal operation, including releases due to failures of the process system alone, i.e. with the protective and containment systems functioning. In addition to the individual dose a limiting population dose of 10^4 man-rem/yr per site was also imposed. The day-to-day releases must be sufficiently small to allow for consequences of process failures being held within the overall limits.

For the combined failure of a process system and one of the other systems, presumably having a frequency less than once per thousand years, the dose limits were set at 25 rem whole body and 250 rem to the thyroid with a population dose of 10^6 rem.

In seeking to ensure that postulated limits of unreliability for the protective system would not be exceeded, the designers and the Board's advisers have made use of the instrumentation philosophy which developed from the lessons of the 1952 accident to the NRX reactor at Chalk River. The triplication of shutdown circuits and other systems not only enhances the probability of correct operation when needed, without imposing unnecessary shutdowns, but also permits complete testing during operation. This detects faults and gives information on reliability. The need for well-defined protective circuitry and rigid rules for its maintenance have been fully recognised in the safety philosophy. The protective system must be such that it prevents fuel failure in the event of any reactor regulating system failure and the emergency core cooling system must be capable of limiting the fuel and sheath temperature so that no more than a very small fraction of fuel is likely to fail in the event of the failure of any pipe or vessel in the primary system.

Recent Developments

With increasing experience some modifications to the original concept of three simple systems have become desirable. For example, the containment was treated as a single entity whereas it consists of many sub-systems. Also the blanket assumption of complete failure of the reactor shutdown system gave little incentive to the designers to improve beyond what they themselves considered adequate. An approach is being developed, therefore, which treats the various safety systems as somewhat parallel and requires that there be no significant release of radioactive fission products following failure of any one of the safety systems combined with a failure of the process system. One consequence of this approach is the need for analysis of more potential dual accidents than previously, i.e. any conceivable significant failure of the process system must be reviewed in connection with the failure of any of the safety systems to ensure that the resultant release of fission products is acceptable. The basic criterion is the same as before. However, in the face of the larger number of potential combinations and in view of the larger reactors with their larger fission product inventory, the unreliability and failure frequency requirements have been made somewhat more severe. Each safety system is expected to have an unreliability not exceeding 10^{-3}. The combined frequency of all serious failures of the process system should not exceed one per three years.

This approach accepts and gives credit for a second shutdown system, but only if it is shown that either of the shutdown systems will fully meet the requirements for any serious failure and that they are independent in design and operation and free from any operational connection with any of the process systems including the regulating systems.

Where the proper operation or effectiveness of a safety system requires the sequential or simultaneous operation of several sub-components, combined failure of these components shall be examined also and may require that they individually meet a more stringent reliability requirement so that the overall reliability requirement of the systems will be met.

Although the limiting rate assumed for serious failure of the process systems may appear high, experience has shown that to achieve it requires a very high standard of quality in large complex plants. To achieve this quality initially and to maintain it during routine operation demands a special effort, particularly for the primary system which is of central importance to safety. The ASME Nuclear Components Code with certain specific exceptions

has been applied for several years by the Board in co-operation with the Ontario and Quebec departments of labour. The ASME Code on In-service Inspection of Nuclear Reactor Coolant Systems is being used as far as practicable with full realisation that this code was developed for light-water reactors. It is hoped that the work of the CNA Codes and Standards Committee will soon lead to a modified standard fully applicable to Canadian reactor designs.

The standard of quality necessary throughout a nuclear plant can be achieved best and most certainly through a program of quality assurance that extends from the conceptual design through to operation. The procedures for controlling quality in manufacture are fairly well established but need more rigorous application. However, the concept of quality assurance, through organization, audit, standards, etc., in the design stage is not yet widely accepted or practised. It is hoped and expected that the industry will move fairly quickly in this direction since the requirement for quality to achieve high operating availability parallels the requirement for quality to achieve high reliability for safety.

The standards and principles developed over the past two decades, especially as applied to safety systems, will continue. The requirement to demonstrate physical and functional separation of the safety systems will be, if anything, now more stringent and special design and maintenance techniques may be necessary to ensure meeting it. The passive safety systems must be testable, at whatever frequency is necessary to ensure the required reliability. It will continue to be necessary that the safety systems are effective without unrealistic requirements that could not be maintained in service.

Final reliance for safety of an operating plant lies mostly in the hands of the operating staff. The examination and authorization of key operating personnel continues, and reviews of total staff training, organizational requirements and the role of other personnel in the safety of the plant will be conducted to determine if further controls would be appropriate.

In appendices A and B the criteria and principles are stated more explicitly. Appendix C contains the definition of exclusion zones for nuclear facilities.

Future Trends

Several of the criteria on which our licensing is based are currently under review and others may be in the near future. The results of these reviews, of course, are difficult to predict with any degree of certainty but the following paragraphs will outline some of the possible directions.

(i) The criteria for man-rem limits, especially those assigned to normal operation, were developed several years ago using available information on the effect of dosage and assuming a linear relation between dose and effect. This subject is under constant review by world authorities such as ICRP, and we shall be guided in our fundamental dose criteria by any modifications in the recommendations.

(ii) Positive void coefficients have been accepted in Canadian power reactors. However, large coefficients impose rather severe demands on the design of the protective shutdown system and accident analysis is then difficult. Future reactors may be required to have a void coefficient within specific limits.

(iii) The need for high quality of the process and safety systems and the growing complexity of the large nuclear power plants is leading to increased emphasis on quality. It is likely that we shall require more organizational control in design and manufacturing of nuclear power plants to oversee, check, and control the safety aspects of the design, procurement, manufacture and installation of important equipment. The quality which is achieved by strict adherence to the pressure vessel codes, the quality assurance programs and the in-service inspection programs will permit an assessment of improved reliability.

(iv) Local investigations may be required to demonstrate the claimed dispersion factors for atmospheric releases and for waterborne releases. While those being used today are believed to be conservative, we may require greater assurance that releases are adding only a small additional radiation dosage to the population.

SUMMARY AND CONCLUSIONS

The Canadian approach to reactor safety, while benefiting from approaches elsewhere, has developed independently. The lesson of the NRX accident and the specific Canadian reactor concept have helped in this distinction. Some of the principles proposed in Canada have been adopted in one form or another elsewhere. These include the basic probability approach, the separation of safety systems from process systems and from one another, the requirement for testing of passive safety systems and the imposition of a limited man-rem population dose as a design and operating criterion. Every effort will be made to keep our standards consistent with the best

approach of other countries and with the requirements of the society in which we live. As the industry develops, it will become essential to express and specify in further detail not only the basic safety criteria but also design manufacturing and operating requirements which will give assurance of meeting the basic criteria. To ensure that the requirements can be met in spite of the complexity of large plants being designed and projected for the future will demand strong organizational control throughout the entire industry, from design and specification through to procurement, manufacture, testing and operation.

Within the past few years public concern for safety of nuclear power plants has at least partially shifted from the question of a major disaster to the effects of normal effluents. While these have always been of great concern to the licensing body, the major concern is and has been to ensure that serious accidents do not occur. Additional requirements may be imposed on radioactive effluents but the major effort of the Board's reactor licensing staff and Reactor Safety Advisory Committee will be in clarifying and strengthening the criteria and in ensuring that the design and operation are such that the probability of a significant accident causing widespread harm is truly negligible.

APPENDIX A

OPERATING DOSE LIMITS AND REFERENCE DOSE LIMITS FOR ACCIDENT CONDITIONS

Situation	Assumed Maximum Frequency	Meteorology to be Used in Calculation	Maximum Individual Dose Limits	Maximum Total Population Dose Limits
Normal Operation		Weighted according to effect, i.e. frequency times dose for unit release	0.5 rem/yr whole body	10^4 man-rem/yr
Serious Process Equipment Failure	1 per 3 years	Either worst weather existing at most 10% of time or Pasquill F condition if local data incomplete	3 rem/yr to thyroid[a]	10^4 thyroid rem/yr
Process Equipment Failure plus Failure of any Safety System	1 per 3×10^3 years	Either worst weather existing at most 10% of time or Pasquill F condition if local data incomplete	25 rem whole body 250 rem thyroid[b]	10^6 man-rem 10^6 thyroid-rem

[a] For other organs use 1/10 ICRP occupational values

[b] For other organs use 5 times ICRP annual occupational dose (tentative)

APPENDIX B

Power Reactor Safety Criteria and Principles

1. Design and construction of all components, systems and structures essential to or associated with the reactor shall follow the best applicable code, standard or practice and be confirmed by a system of independent audit.
2. The quality and nature of the process systems essential to the reactor shall be such that the total of all serious failures shall not exceed 1 per 3 years. A serious failure is one that in the absence of protective action would lead to serious fuel failure.
3. Safety systems shall be physically and functionally separate from the process systems and from each other.
4. Each safety system shall be readily testable, as a system, and shall be tested at a frequency to demonstrate that its (time) unreliability is less than 10^{-3}.
5. Radioactive effluents due to normal operation, including process failures other than serious failures (see #2 above), shall be such that the dose to any individual member of the public affected by the effluents, from all sources, shall not exceed 1/10 of the allowable dose to Atomic Energy Workers and the total dose to the population shall not exceed 10^4 man-rem/year.
6. The effectiveness of the safety systems shall be such that for any serious process failure the exposure of any individual of the population shall not exceed 500 mrem and of the population at risk, 10^4 man-rem.
7. For any postulated combination of a (single) process failure and failure of a safety system, the predicted dose to any individual shall not exceed (i) 25 rem, whole body, (ii) 250 rem, thyroid, and to the population, 10^6 man-rem.
8. In computing doses in 6 and 7 the following assumptions shall be made unless otherwise agreed to:
   (i) meteorological dispersion that is equivalent to Pasquill category F as modified by Bryant[1]
   (ii) conversion factors as given by Beattie[2].

[1] Bryant, P.M. UKAEA report AHSB(RP)R42, 1964.

[2] Beattie, J.R. UKAEA report AHSB(S)R64, 1963.

APPENDIX C

EXCLUSION ZONE

Definition

An Exclusion Zone is an area, specified by the Atomic Energy Control Board, immediately surrounding a nuclear facility and under the control of the licensee or the operator.

Conditions

1. There shall be no permanent habitation within the Exclusion Zone.
2. Use of the land for purposes other than the licensed activities shall require separate AECB approval.
3. Exclusion Zones shall be posted in a manner acceptable to the Board.
4. Radiation safety within the Exclusion Zone is the responsibility of the licensee, or, subject to AECB approval, his designate. Methods and measurement for ensuring radiation safety are subject to review as required by the Board.

NOTE

For all power reactors licensed to date the Exclusion Zones extend from the reactor core to a radius of 3000 feet with the exception of navigable waters and minor other exceptions.