from: IAEA Containment + Siting Conf. 1967

# CONTAINMENT AND SITING REQUIREMENTS IN CANADA

F. C. BOYD
ATOMIC ENERGY CONTROL BOARD,
*OTTAWA, ONTARIO, CANADA*

**Abstract**

CONTAINMENT AND SITING REQUIREMENTS IN CANADA. The present early stage of development of large nuclear power reactors has led to a requirement in Canada for siting restrictions and "containment" provisions. The latter, in conjunction with reliable operating and protective equipment, are intended to reduce to an acceptable level the probability of a serious release of fission products to the public.

In considering the suitability of a site and the adequacy of the containment provisions, the Atomic Energy Control Board, which is the regulating agency, has developed siting criteria which consider: (1) normal releases of radioactive material from the plant, (2) the size of potential accidental releases, (3) the probability of accidents, and (4) the density of the surrounding population. Design guide values are given for the radiation exposure both of individuals and the total population at risk for three conditions: (1) normal operation, (2) failures of operating or "process" equipment only, (3) combined failures of process and protective equipment. From the application of known or stated meteorological conditions an "acceptable" release from the plant can be determined. When combined with predicted releases from the reactor for various accidents within the last two categories above, this will give the total "allowable" fractional release from the containment.

The exposure limits for normal operation follow the recommendations of the ICRP. The limits for whole-body exposure for accidents are:

| *Accident type* | *Individual* | *Total population* |
|---|---|---|
| Process failure only | 0.5 rem | $10^4$ man-rem |
| Process plus protective failure | 25 rem | $10^6$ man-rem |

Limits have also been specified for exposure of the thyroid and other critical organs.

These criteria have been used in evaluating the site and containment for the large multi-unit Pickering Generating Station and the 250 MW(e) Gentilly Station. Although the former is only 30 km from the centre of Toronto, a city of about two and one-half million, the exposure limit for an individual at the 1-km boundary was the deciding factor.

It is hoped that operating experience will give assurance of the low probability of equipment failure so that the requirements for containment and siting can be reduced.

## 1. *INTRODUCTION*

As in many other countries the regulatory agency for atomic energy in Canada, the Atomic Energy Control Board, has been faced with requests to locate large nuclear power plants close to heavily populated centres. This has resulted in the review by the Board's Reactor Safety Advisory Committee during the past two to three years of its prior criteria for judging the safety of nuclear plants and the acceptability of sites, and has led to the establishment of certain siting and design guides.

Before discussing the siting guides it is necessary to review first some of the concepts of reactor safety which have been developed in Canada, since the siting criteria presume that a plant meets the general standards of safety that have been proposed. In addition the guides are expressed partly in the context of these reactor safety concepts.

## 2. REACTOR SAFETY CRITERIA

### 2.1. General

The basic principles of reactor safety have been published [1, 2, 3] and still apply. Most important is the separation of a nuclear plant into three divisions for the purpose of the safety evaluation. These divisions are:

(1) The process equipment which includes all the equipment and systems necessary for the normal functioning of the reactor and plant;
(2) The protective devices which include all the systems or devices designed to prevent damage to the fuel from any failure in the process equipment or any operating error;
(3) The containment provisions which include any structures or other provisions which are intended to limit or restrict the release of any radioactive material that might escape from the process equipment.

It is a basic principle in the Canadian approach to reactor safety that the three divisions of the plant be structurally and operationally independent. The independence of the divisions from each other is essential if it is to be assumed that the rate of cross-linked faults, i.e. faults affecting more than one division resulting from the same cause, can be kept less than the probable rate of coincidence of independent faults. In other words, the divisions must be sufficiently independent of one another that the probable occurrence of faults in, say, both the process equipment and protective devices can be determined by the product of the independent probability of faults in each division.

### 2.2. Reliability

The standards of reliability that have been quoted [3] for these divisions are:

(1) The frequency of dangerous faults in the process equipment should not exceed one per three years
(2) The unreliability of the protective devices should not exceed 0.003
(3) The unreliability of the containment provisions should not exceed 0.003.

(Unreliability is the fraction of time that a particular system is unable to perform adequately its intended function.)

In actual fact the process and protective systems would not be accepted unless their designs gave promise of a much better performance than these proposed standards. The Committee requires that there be no doubt that the limit can be achieved and allows a considerable margin for uncertainty. There is not sufficient experience to date to indicate whether the required low unreliability of the containment provisions can actually be achieved but the most recent designs give promise that they will meet the requirements.

These standards have been chosen because they are large enough that they may be confirmed by actual observation in a few years and yet are small enough that the probability of the three divisions (assuming their independence from one another) failing simultaneously from independent faults is acceptably small.

A requirement of the siting criteria, as will be seen later, is that proper operation of either the protective devices or the containment

provisions in the event of a dangerous fault in the process equipment will prevent any significant harm to persons outside the required exclusion area. Therefore it would only be through a coincident failure in all three divisions that any widespread injury of the public would be expected.

While these reliability standards serve as a guide to the designer, they also form a standard of performance which the operator must maintain and demonstrate through a test programme.

### 2.3. Design principles

In addition to the general design principle of the subdivision of the plant, a number of more specific design principles and guides have evolved which must be followed to give assurance that the desired reliabilities actually will be achieved. A few of the more important principles are as follows:

(1) All protective and all containment systems shall be designed so that they may readily be tested at a frequency sufficient to demonstrate the required reliability

(2) The reactor protective system (automatic shutdown system) shall be independent of the reactor regulating (control) system. It shall provide the reliability at least equivalent to that expected for a two out of three channel coincident system using proven equipment and shall be designed such that it can readily be tested to demonstrate this reliability. The shutdown system shall have sufficient speed to prevent significant fuel failure in the event of any regulating system failure and sufficient shutdown capacity to overcome the maximum positive reactivity that might be added

(3) The primary cooling system shall be designed and built to the best applicable piping and vessel codes

(4) An emergency cooling system shall be provided, capable of limiting the fuel temperature such that no more than 1% of the fuel is likely to fail in the event of the failure of the largest pipe or vessel in the primary system.

## 3. SITING CRITERIA

### 3.1. General

The siting criteria were developed as a basis for judging the suitability of a site for a given reactor. Alternatively, they may be used for specifying the required effectiveness of the containment provisions and protective devices for a plant at a particular site. While the criteria are expressed in terms of radiation dose, in effect, they set limits on the release of fission products to the environment in the event of assumed large accidents. Hence they impose requirements on the effectiveness of the safety provisions in terms of total leakage from the plant under these assumed conditions.

The criteria give design guide values for the radiation exposure of both individuals and the total population at risk for normal operation; failures of the process equipment; failures of a process equipment coincident with failures of either the protective devices or the containment provisions.

No attempt has been made to set limits for the event of a coincident failure in all three divisions. By dividing the plant as outlined above and taking care to obtain and maintain the independence of the divisions it is felt that it is possible to achieve a sufficiently low probability of the simultaneous failure of the entire plant as to be acceptable.

The design exposure limits for individuals are based on the recommendations of the International Commission on Radiological Protection and the United Kingdom Medical Research Council [4, 5]. The values for the population dose, which are expressed in man-rem, were chosen from a consideration of somatic as well as genetic effects, assuming a linear dose-effect relationship as suggested in the UNSCEAR report [6]. For the particular case of radioiodine, the work of Beach and Dolphin [7] was originally used for the effect of thyroid irradiation and privately obtained information was used [8] for the normal incidence of thyroid carcinoma. This has subsequently been confirmed with more recent information such as the ICRP report on the evaluation of risks from radiation [9].

## 3.2. Normal operation

The values for whole-body exposure chosen for the siting guide for normal operation are 0.5 rem/yr to any individual and $10^4$ man-rem. Since radioiodine has been recognized as being a critical isotope in reactor safety studies, specific limits have also been stated for the thyroid dose, namely 3 rem/yr to an individual or $10^4$ thyroid-rem to the population.

An appreciation of the significance of these population limits may be obtained by noting that the references in section 3.1 indicate that $10^6$ man-rem can lead to 10 to 20 cases of leukaemia and $10^6$ thyroid-rem can lead to 20 to 30 cases of thyroid carcinoma. Hence the chosen dose limits would lead to a very small increase over the natural incidence of leukaemia of about 60 per $10^6$ people per year and of thyroid carcinoma of about 10 to 20 per $10^6$ per year.

For computing the effect of gaseous effluents from the plant in normal operation, applicants are permitted to use the weighted average weather for the particular area. The average weather using Pasquill's equations [10] as applied by Bryant [11] has been accepted. In another paper at this Symposium [12] Barry refers to his measurements and statistical evaluation of the dilution factor at the Chalk River Nuclear Laboratory. This type of approach is preferred and effluent limits based on Barry's data are being considered.

Since the design dose limits are for all aspects of operation of the plant, liquid as well as gaseous effluents must be taken into account and any concentrating factors through the food chain must be included.

## 3.3. Process failure only

It is the intention that the effects of failures which occur only in the process equipment should be averaged with those from normal operation and should meet the same overall criteria. Of concern here are 'dangerous' failures which, in the absence of protective devices, could lead to significant fuel failures. For design purposes, it has been assumed that dangerous process failures will not occur more often than

once per three years and therefore the yearly permitted dose for normal operation may be used as the design basis for a single process failure provided reasonable margin has been provided in normal operation. In this case, for any gaseous or liquid effluents, the most pessimistic dilution factor must be used. For atmospheric dilution this has been set as Pasquill F or the worst weather existing, at the most, 10% of the time. Here again data similar to that obtained by Barry would be the most desirable for use at any particular site.

For a typical exclusion zone of about 1 km radius, this criterion leads to an acceptable release from the plant in the event of a process equipment failure of about 2.5 Ci of iodine-131. This very small release sets the required combined effectiveness of the protective and containment provisions. In essence it means that the protective system shall prevent any significant fuel failure in the event of any process equipment failure.

### 3.4. Coincident process and protective equipment failures

The design dose limits for coincident process and protective equipment failures also apply to coincident process and containment failures. In this paper the limits will be considered for coincident process and protective failures and the application of these limits in specifying the required containment effectiveness for any given site will be shown.

The following design dose limits were chosen for this event which is assumed to have a probability of less than $10^{-3}$ per year:

(a) To any individual, 25 rem whole-body and 250 rem to the thyroid
(b) To the population, $10^6$ man-rem or $10^6$ thyroid-rem.

The individual dose limits were chosen to be values at the lower limit of possible early somatic damage. The population dose limits, which were chosen subjectively using the data noted [6-9], could result in ten cases of leukaemia or thirty cases of thyroid carcinoma over a number of years. These values are comparable to the normal annual incidence (assuming a population at risk of $10^6$) and hence the assumed probability of the event (less than $10^{-3}$/yr) could be increased by a factor of 10 and still not cause an inordinate increase in the normal incidence.

Again, for a release into the atmosphere, the worst weather conditions occurring 10% of the time are assumed; or if this is not known, Pasquill F weather is assumed. Using Pasquill F and an exclusion zone of 1-km radius, the individual dose limit leads to an allowable release of about 200 Ci of iodine-131. The calculation for the population dose is integrated down to the level at which an individual receives the allowable yearly dose.

### 3.5. Exposure to dose relationship

Since the siting criteria are stated in terms of dose, methods of relating the release (in curies) to the dose received by exposed members of the public have been suggested. As mentioned above, in the case of releases to the atmosphere the dilution may be computed by the methods of Pasquill or by applying the data of Barry. For the dose due to inhalation the conversion figures of Beattie [13] are considered convenient and applicable. The situation for the food chain is less precise. Barry [14] has computed "allowable" concentrations and time-integrated concentrations for $^{131}I$, $^{90}Sr$, $^{137}Cs$, and $^{3}H$ over agricultural land using the recom-

mendations of the United Kingdom Medical Research Council [5] and assuming reasonable values for deposition velocities, plant uptake, and, in the case of radioiodine, the transfer from herbage to milk. Stewart and Simpson [15] have reviewed the situation from the assumption of an accidental release.

### 3.6. Accident assumptions

The particular failures that must be assumed for the purpose of applying the siting guide depend upon the particular design. In general the worst failures of process equipment that must be considered are:

(a) Failure of the reactor regulating system such as to drive the power up at the maximum physical rate
(b) Failure of the largest pipe or vessel in the primary system.

From experience in other fields it is likely that the latter, assuming the system is built to the required standards, has a probability of failure much less than the once per three years assumed for the purpose of the guide. However, to date, it has been considered prudent to apply this high probability and thereby require highly effective protective and containment provisions to meet the siting guide limits.

The failures of the protective systems that must be assumed for the case of coincident failure of process equipment and protective devices are primarily either, (1) the reactor shutdown system does not function, or (2) the emergency cooling system does not operate. It has not been required to assume that both the shutdown and emergency cooling fail simultaneously if adequate independence has been provided. Although multiple channel shutdown systems have been commonly used the assumed failure of the reactor protective system, required to date for the safety analysis, is simply that the reactor will not shut down when the normal safety limits are exceeded. As improvements are made in shutdown system design it may be possible to relax this requirement.

For failure of the reactor regulating control the worst coincident failure is normally failure of the reactor shutdown system. For a large failure of the primary system the coincident failure of either the reactor shutdown system or the emergency cooling system may lead to the worst postulated release of fission products.

When considering failures of the containment provisions it is usually required to assume that they fail completely. For actual designs it may be accepted that some, perhaps appreciable, effectiveness remains even if, say, large doors of a containment building were left open, in which case the required assumption may be modified.

Unless reasonable analysis and data are submitted otherwise, it is assumed that all the volatile and 10% of the non-volatile fission products are released from fuel that melts and that 10% of the volatile fission products are released from fuel that overheats to the extent that the sheathing fails but the fuel does not melt.

## 4. OTHER CONTAINMENT REQUIREMENTS

### 4.1. General design

As well as the general exposure criteria given above, which set the effectiveness of the containment, other design requirements have evolved.

The containment must be designed to withstand the total energy release possible from the contained systems. If the primary system is subdivided and the subdivisions are sufficiently independent of one another in connections and physical location it may be possible to claim that the release is only that in one segment of the circuit. Credit may also be taken for energy-absorbing systems, such as water sprays or air coolers, provided these are designed to perform with the required reliability.

The containment and all auxiliary provisions must be designed to permit testing of the state or quality of the containment whenever it is deemed necessary. Containment buildings must have any openings, such as for ventilation ducts or steam mains, designed with adequate closing mechanisms arranged to operate automatically on a predetermined increase of pressure or radioactivity within the structure. At least two airlock openings for personnel, separated from one another as far as practicable, should be installed. In addition, an equipment airlock must be provided, suitable for the largest piece of equipment likely to be required to be moved in or out.

### 4.2. Containment reliability

In section 2.1 it was stated that a required general safety criteria was that the containment provisions have an unreliability of less than 0.003. The design must therefore be such as to give confidence that such a low unreliability can be achieved. This requires simple, basically inherent or self-operating systems together with provisions for testing. It is unlikely that a moderate or high pressure containment building would be required to be tested to full design pressure after operation begins but it would be required to be tested periodically at lower pressures. In this case the initial testing must establish the likely relationship between pressure and leakage.

Although the reliability requirements have been referred to as design requirements they are actually an operating requirement. The operators must demonstrate, through testing, that the unreliability specification is actually achieved and maintained. This in turn, of course, implies that the design provides the required initial quality and, in addition, provides arrangements for testing which are adequate to enable the operator to control the reliability by varying the test frequency and repair time.

## 5. CONCLUSION

The reference dose limits which have been quoted as the criteria for siting and containment are quite conservative when the probability of their actually occurring is considered. In the case of the coincident failure of process equipment and protective devices, the limits for the dose to the individual would lead, according to the recent ICRP report [8], to only third-order risks in the case of the thyroid dose limits or fourth-order risks in the case of the whole-body dose limits. (That is, these doses would cause injury in 1 per $10^3$ to $10^4$ people.) The population limit is more conservative, i.e. it will limit the injuries to about 1 per $10^5$ people. Despite this, it can be shown that the population density beyond the exclusion zone must exceed $10^4$ persons per square kilometre before a

release which gives the individual dose limit at 1 km would give the population dose limit. This population density may be compared with the average density of metropolitan Toronto of about $3 \times 10^3$ per square kilometre.

Since the probability of a coincident failure in both the process equipment and the independent protective devices is taken to be less than $10^{-3}$ per year, the risk to the public is less than 1 carcinoma per $10^6$ people per year. This may be compared to, say, the risk of death from respiratory diseases to which airborne contamination undoubtedly contributes, which in 1959 in North America was about 400 per $10^6$ per year and in the United Kingdom about 1600 per $10^6$ per year [16].

For the Pickering station near Toronto several 500 MW(e) units are planned. Undoubtedly the multiplication of units increases the probability of an accident and therefore the risk to the public. However, there is little difference in total risk to the population between several units at one site and the same number distributed at various sites in the same region. The siting guide dose limits were chosen bearing in mind that there might be about 1000 MW(e) of nuclear power per $10^6$ people, this being approximately the ratio of total electrical generation per capita in Canada a few years ago.

It may be noted, as shown by Hake in another paper to this Symposium [17], that the building of several moderate-size units at Pickering, rather than one extremely large unit or several scattered ones, has permitted the design of an extremely effective containment system. In this case it can be argued that the risk is not proportional to the number of units if these are considered separately, but less.

The assumptions that have been made regarding the failures of the process equipment and protective devices, the release of fission products and the diffusion in the atmosphere are all pessimistic. It is anticipated that experience and experimental work will supply the basis for more accurate estimates and thereby provide confidence to relax the requirements.

There has long been in Canada the attitude that the risk must be related to the benefit derived. The present siting criteria being applied by the Atomic Energy Control Board applies this principle by, in essence, setting the risk proportional to the number of nuclear power units. Even with many units this risk remains extremely small and very much less than other accepted risks.

## ACKNOWLEDGEMENTS

The author would like to acknowledge the helpful comments of members of the Reactor Safety Advisory Committee and of members of the Board staff.

## REFERENCES

[1] LAURENCE, G.C., et al., Proc. 3rd UN Int. Conf. PUAE 13 (1964) 317.
[2] LAURENCE, G.C., Reactor siting criteria and practice in Canada, ANS Topical Meeting, Los Angeles, 18 Feb. 1965.
[3] BOYD, F.C., Reactor licensing in Canada, CNA Annual Meeting, Winnipeg, 1 June 1966.
[4] Recommendations of the International Commission on Radiological Protection, ICRP Publication 6, Pergamon Press, London (1964).

[5] U. K. MEDICAL RESEARCH COUNCIL, The hazards to man of nuclear and allied radiations, Cmnd 1225 (1960).
[6] Report of the United Nations Scientific Committee on the Effects of Atomic Radiation (1964).
[7] BEACH, S. A., DOLPHIN, G. S., A study of relationship between x-ray delivered to the thyroids of children and the subsequent development of malignant tumours, UKAEA Rep. AHSB(RP)R 13 (1962).
[8] TAYLOR, R. M., National Cancer Institute, private communication, 1964.
[9] The Evaluation of Risks from Radiation, A report to Committee I of the International Commission on Radiological Protection, Health Phys. 12 (1966) 239.
[10] PASQUILL, F., Atmospheric Diffusion, D. Van Nostrand, N. Y. (1962).
[11] BRYANT, P. M., UKAEA Rep. AHSB(RP)R42 (1964).
[12] BARRY, P. J., "Concept of a standard site" (SM-89/5) these Proceedings.
[13] BEATTIE, J. R., UKAEA Rep. AHSB(S)R-64 (1963).
[14] BARRY, P. J., Rep. AECL-1624 (Rev) (1964).
[15] STEWART, C. G., SIMPSON, S. D., Protection of the Public in the Event of Radiation Accidents (Proc. of a Seminar) WHO, Geneva (1965) 183.
[16] WORLD HEALTH ORGANIZATION, Technical Report 246, WHO, Geneva (1962).
[17] HAKE, G., "The relation of reactor design to site approval and containment in Canada" (SM-89/4), these Proceedings.

## DISCUSSION

C. SENNIS: Does your first assumption – that the reactor shutdown system does not function (section 3.6.) – imply that no external shutdown mechanism is available to terminate any power excursion that might accompany the loss of coolant? If so, how is the excursion terminated?

F.C. BOYD: Yes, that is the assumption. The excursion is terminated by melting through of the pressure tubes, which allows coolant to enter the moderator, thus displacing the moderator from the core by over-riding the pressure balance system.

T. ITAKURA: Is the 250-rem thyroid dose limit for children or adults?

F.C. BOYD: For children.

E.W. STAUBER: You have given (section 3) the man-rem concept as an additional limit for whole-body exposure in the event of accidents. On the other hand, you also specify limits for the accidental exposure of critical organs. I assume therefore that the $10^6$ man-rem, for example, are received only as external radiation. Is this correct?

F.C. BOYD: Yes, $10^6$ man-rem refers to external radiation. I indicated a value of $10^6$ thyroid-rem and we are working on limits for other organs also.

P.M. GERINI: Is extensive analytical and/or experimental work required to demonstrate that containment (section 3.6.) is not affected by the energy release from the primary system in the event of a nuclear excursion, with particular reference to shock waves and missile generation phenomena?

F.C. BOYD: Yes, and such analytical and development work has been carried out. Some of it is reported in a Canadian paper by I.J. Billington [Developments in the analysis of reactor containment requirements, NUCLEX, Basle, Switzerland (1966)].

# General Safety Considerations

Edited by J. R. Buchanan

## Canadian Approach to Nuclear Power Safety

By R. J. Atchison,* F. C. Boyd,† and Z. Domaratzki‡

[Editor's Note: This is the first in a series of articles on the nuclear safety philosophies of the world's major nuclear power countries. The series will continue with articles in successive issues of *Nuclear Safety* for at least the next year. The editors of *Nuclear Safety* have initiated this series in the belief that nuclear safety in all countries will be enhanced by a better understanding of different and frequently sophisticated approaches that are used in other countries. We are pleased to initiate this series with the following article on the Canadian approach to nuclear power safety.]

**Abstract:** *The development of the Canadian nuclear power safety philosophy and practice is traced from its early roots at the Chalk River Nuclear Laboratories to the licensing of the current generation of power reactors. Basic to the philosophy is a recognition that the licensee is primarily responsible for achieving a high standard of safety. As a consequence, regulatory requirements have emphasized numerical safety goals and objectives and minimized specific design or operating rules. In this article the Canadian licensing process is described with a discussion of some of the difficulties encountered. Examples of specific licensing considerations for each phase of a project are included.*

The approach to nuclear power safety in Canada has evolved in a continuous manner over almost three decades. From the outset the safety objective has been to ensure that the risk to the public presented by nuclear power plants is substantially lower than that from alternative sources of electrical energy. Although the expressed criteria have changed somewhat with experience over the years, this basic objective has remained. An underlying principle has been that the licensee (owner/operator) bears the basic responsibility for safety, whereas the regulatory authority [the Atomic Energy Control Board (AECB)] primarily sets safety objectives and some performance requirements and audits their achievement. As a consequence, regulatory requirements have emphasized numerical safety goals and objectives and minimized specific design or operational rules.

This article traces the evolution of this approach and its application with some specific examples illustrating not only the overall effectiveness of the approach but also some of the practical difficulties encountered.

*Robert J. Atchison received the B.A.Sc. degree in engineering physics from the University of Toronto in 1953. His experience includes service at Chalk River Nuclear Laboratories, the Douglas Point prototype power station, Hydro-Quebec's Gentilly 1 boiling light-water station, and Ontario Hydro as a supervising design engineer. In 1974 he joined the Atomic Energy Control Board (AECB) and is currently Director of the Assessment Branch. Current address: AECB, P. O. Box 1046, Ottawa, Canada, K1P 5S9.

†Fred C. Boyd received the B.A.Sc. degree in engineering physics from the University of Toronto in 1949. Part of the original design team for the Nuclear Power Demonstration Plant, he subsequently joined the Atomic Energy Control Board (AECB) in 1959 and became head of the Facilities Licensing Group. After serving 1 yr as an International Atomic Energy Agency advisor in Korea, he is currently AECB Science Advisor and Director of the Orientation Centre, which provides advice to foreign regulatory agencies. Current address: AECB, P. O. Box 1046, Ottawa, Canada, K1P 5S9.

‡Zigmund Domaratzki graduated from the University of Manitoba in 1959 with a degree in mechanical engineering. After 10 yr at the Chalk River Nuclear Laboratories engaged chiefly in research and development work on fuel for CANDU reactors, he joined the Atomic Energy Control Board (AECB) as one of its two resident project officers at the Pickering Generating Station. He is currently the Director General of the Directorate of Reactor Regulation. Current address: AECB, P. O. Box 1046, Ottawa, Canada, K1P 5S9.

The conclusion is one of confidence that this pproach to achieving safety at nuclear power lants, which has been followed over the years in anada, is both flexible and effective. The pproach could be adopted by any country wishing o develop indigenous regulatory rules that could e applicable to more than one design of nuclear ower plant.

## ACKGROUND

The philosophy of nuclear safety in Canada eflects the political structure of the country, the istory and organization of the nuclear industry, nd the evolution of a distinctive, indigenous uclear power plant design (CANDU). The follow-ig sections outline briefly this important context.

### istorical

Canada is a confederation with 10 provinces nd 2 territories administered by the central or ederal government. The Canadian constitution is xpressed in the Constitution Acts of 1867 to 1982.

The provinces are self-governing in the areas of egislative power assigned to them by the acts. hese areas include local commerce, working con-itions, education, direct health care, and resources general. However, the acts give the Parliament Canada (i.e., the central or federal government) egislative power over works declared by it to be r the general advantage of Canada.

Canada entered the nuclear field during World ar II when the Montreal Laboratory was es-blished to pursue the heavy-water-reactor route plutonium production. At the end of the war, e government decided to continue, for peaceful rposes, the research and development that was nder way.

In 1946 the Parliament of Canada passed the tomic Energy Control Act,[1] declaring atomic ergy a matter of national interest and creating e AECB to administer the act. The Act, which as subsequently amended in 1954, is a short cument authorizing and defining the powers of e AECB, a body with five members, one of hom is appointed President and Chief Executive fficer. Under the provisions of the act, the AECB empowered to make regulations governing all pects of the development and application of omic energy.

The 1954 amendment to the act transferred the responsibility for research and the exploitation of atomic energy from the AECB to a minister designated by the government. As a result of this transfer of responsibility, Atomic Energy of Canada Limited (AECL) (a government-owned company established in 1952) was made responsible directly to the designated minister, and the AECB was left clearly as the regulatory agency.

The Atomic Energy Control Act is very broad, enabling legislation that gives extensive discretionary power to the AECB. The AECB has chosen to issue only general, skeletal regulations;[2] specific regulatory requirements are applied through the licensing process.

Other than the Atomic Energy Control Act, the only other legislation enacted by Parliament specifically for atomic energy is the Nuclear Liability Act.[3] This act, which entered into force in October 1976, places total responsibility for nuclear damage on the operator of a nuclear installation and requires the operator to carry insurance in the amount of $75 million. It also provides for the establishment of a Nuclear Damage Claims Commission to deal with claims for compensation when the federal government deems that a special tribunal is necessary, for example, if the claims are likely to exceed $75 million.

### Structure of the Industry

When the AECL was formed in 1952, it took over the operation of the Chalk River Nuclear Laboratories, which had been set up in 1944–1945 as an outgrowth of the wartime program of the Montreal Laboratory. The AECL conducted the research and development and eventually the engineering of the CANDU design[4] for nuclear power plants. A major sector of the company was created to carry out the engineering and export functions.

Ontario Hydro, the electric utility owned by the Province of Ontario (and the largest in the country), became interested in nuclear power in the early 1950s and collaborated with AECL in the development of the CANDU design. This early association resulted in the joint building of the Nuclear Power Demonstration (NPD) prototype plant that started up in 1962. Today Ontario Hydro acts as its own prime contractor and is its own architect–engineer for all but the nuclear reactor.

The other two Canadian utilities with nuclear power plants are also provincially owned: Hydro-Quebec and the New Brunswick Electric Power Commission. Both have employed private firms for much of the architect–engineer and management functions in the balance-of-plant systems. The AECL has provided conceptual design and safety assessment for the overall plant and engineering and procurement services for the nuclear steam supply system.

Although there are a large number of component suppliers, the basic industry is concentrated in very few organizations. This has facilitated communication and discussion among key personnel on the interpretation and application of the AECB's safety and licensing requirements.

The decision to construct a nuclear power station in Canada is made by a provincial electric power utility. Thus it is provincial governments that, in effect, decide whether or not nuclear–electric power generation should be part of the provincial energy program. After such a decision is made, the AECB ensures that the facility complies with appropriate health, safety, security, and environmental requirements. The board has chosen not to be involved in social or economic aspects.

### Structure of the AECB

The five members of the AECB have a supporting staff of 270 (as of April 1983). The staff is organized into the functional units of President's Office, Secretariat, Reactor Regulation Directorate, Fuel Cycle and Materials Regulation Directorate, Regulatory Research Branch, and Planning and Administration Branch (Fig. 1). There are two regional offices, primarily for compliance functions associated with radioisotope licensing.

About one-quarter of the staff of 70 of the Reactor Regulation Directorate are at field offices located at each of the nuclear power projects and at AECL's design office. Since the early 1960s, the AECB has followed the practice of having at each nuclear power station resident professionals who serve both as inspectors and project licensing officers. Typically the project offices are opened at about the midpoint of the construction. The presence of AECB personnel on the site facilitates the surveillance of construction and commissioning activities. To date, resident offices have been maintained after the plant has gone into operation, and it is expected that this practice will continue.

The project officers, who are, of necessity, "generalists," are complemented by staff specialists in quality assurance (QA), radiation protection, and a variety of engineering disciplines. A separate division conducts examinations for the licensee staff proposed for positions requiring specific authorization by the AECB, namely, the shift supervisors and control room operators.

Reporting separately to the AECB are two advisory groups, the Advisory Committee on Radiological Protection and the Advisory Committee on Nuclear Safety. Although not involved in licensing, these committees advise the board on generic issues, regulations, general requirements, and specific problems assigned to them.

### CANDU Characteristics

Canada has concentrated on heavy-water-moderated reactors using natural uranium as fuel. The power reactor design[4] uses pressurized heavy water as the coolant, plus pressure tubes and on-power fueling. All nuclear power plants built or planned in Canada are of this CANDU-type design except for the Gentilly 1 boiling light-water prototype.

The combination of expensive heavy water and natural uranium tends to result in reactors having relatively high fuel power rating, high flux, and small excess reactivity. The reactivity constraint, coupled with small temperature–reactivity coefficients, requires constant control and has led to the extensive use of automatic (in recent plants, digital computer) control.

Automatic control relieves the operator of the need to make quick decisions under stressful conditions. Adjustments required by transient conditions are made automatically by the regulating system, which can also bring the plant from shutdown to the demanded power at a safe and controlled rate without intervention by the operator. Therefore the operator is free to make full use of his diagnostic abilities. As a corollary, the training of operating staff has emphasized a sound understanding of the principles involved.

The pressure-tube design presents some safety considerations that are different from those of other designs[4] while obviating any concern about reactor pressure vessel failure. These include such factors as the heat-sink capacity of the moderator,[5]

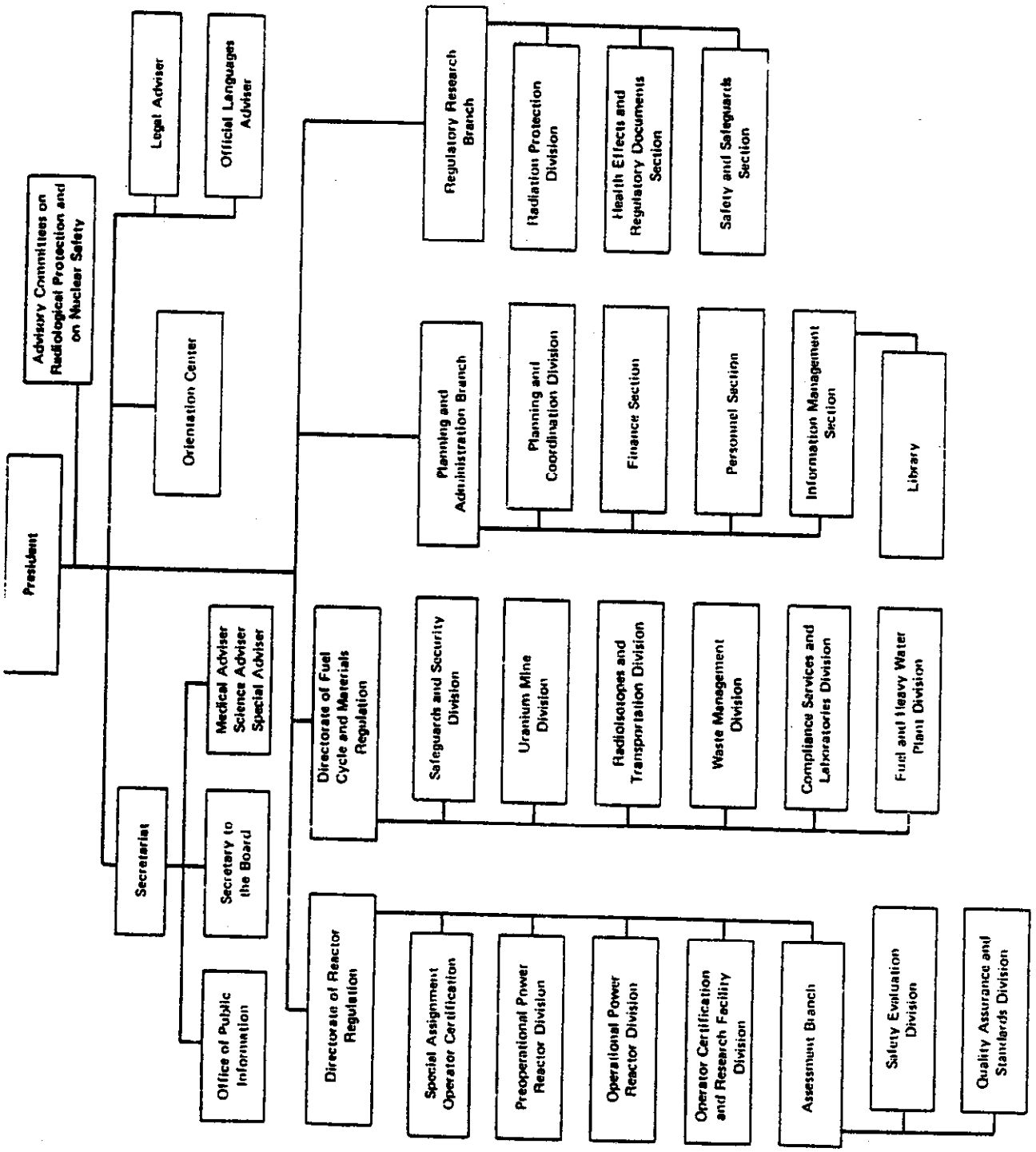



Fig. 1 Organization chart for the Atomic Energy Control Board.

flow stability questions, and the possibility of the fuel coming into contact with the pressure boundary, all of which bear on the requirements for emergency core cooling systems (ECCS).

The safety characteristics of the CANDU design have had, inevitably, an influence on the safety criteria developed by the AECB, and the safety criteria have, in turn, strongly influenced the design.

## SAFETY PRINCIPLES AND OBJECTIVES

The basic philosophy of nuclear regulation in Canada and the underlying principles have changed little since the passage of the Atomic Energy Control Act. Although the regulatory process has become appreciably more comprehensive and systematic and is now much more open, the fundamental regulatory principles remain unchanged. The underlying concept is that the primary responsibility for achieving a high standard of safety resides with the licensee.

Recently the AECB endorsed a statement[6] on the safety objectives for nuclear activities that had been developed by its Advisory Committee on Nuclear Safety to express the historical understanding. For hazards caused by ionizing radiation, the objectives are that (1) all early detrimental effects should be avoided and the risk of deferred effects should be minimized in accordance with the as low as reasonably achievable principle and (2) the probability of malfunctions should be limited to small values, decreasing as the severity increases, so that the likelihood of catastrophic accidents is virtually zero.

In the case of nuclear power, the safety objective from the earliest days of the Canadian program has been to ensure that the likelihood of a serious release of fission products is negligibly small. This "risk" approach has pervaded the Canadian safety philosophy throughout the years and from the outset has included numerical safety goals, as discussed in the following sections.

## EVOLUTION OF APPROACH

A serious accident at the NRX research reactor at Chalk River in 1952 was the catalyst for much of the Canadian reactor safety approach that prevails today. The essential principles that evolved were derived from the recognition that even well-designed and well-built systems fail; therefore there is a need for separate, independent safety systems that can be tested periodically to demonstrate their availability.

In 1957 a paper by E. Siddall[7] (which had an extended foreword by W. B. Lewis) proposed setting safety standards for nuclear power plants by comparing their economic and accidental death consequences with those of the coal-fired power plants to be displaced. This approach was taken for the design of the small NPD, Canada's first nuclear power plant, which began operation in 1962 (Ref. 4). The target proposed for NPD from the above approach was a frequency of $10^{-5}$/yr for serious accidents, based on an overall risk of 1 death per 100 reactor-years (RYs) ($10^{-2}$ deaths/yr).

Concurrently, G. C. Laurence, who had been named Chairman of the Reactor Safety Advisory Committee (RSAC), which the AECB created in 1956, also proposed, on similar arguments, that the likelihood of a disastrous accident at a nuclear power reactor should be $<10^{-5}$/yr.[8] Laurence further proposed that this target could be achieved with realistic designs if there were adequate separation between the operating equipment, the protective devices, and the containment provisions. On this basis, he proposed that the rate of failure of equipment that could lead to a serious release of fission products should be $<10^{-1}$/yr and the probability that the protective devices would be inoperative or the containment provisions ineffective should be each $<10^{-2}$.

In the mid-1960s these concepts were formalized for the first time into a set of criteria commonly called the Siting Guide.[9] These criteria were based on the separation of plant systems into two categories: the process systems or normally operating equipment and what later came to be known as the special safety systems, which were designed to prevent or mitigate the consequences of failures of the process systems. The special safety systems include the reactor shutdown systems, ECCSs, and the containment provisions. Although modified over the years, these criteria still constitute the basic safety requirements for nuclear power plants.

The basic requirements,[10] as last modified in 1972, set limits on the frequency of serious process failures* and on the unavailability of the special

*A *serious process failure* is a *failure of a process system or* equipment that, in the absence of special safety system action, could lead to fuel failure or the release of radioactive material to the environment.

Table 1 Operating Dose Limits and Reference Dose Limits for Accident Conditions

| Situation | Assumed maximum frequency | Meteorology to be used in calculation | Maximum individual dose limits, mSv | Maximum total population dose limits, Sv |
|---|---|---|---|---|
| Normal operation | | Weighted according to effect, i.e., frequency times dose for unit release | 5/yr, whole body<br>30/yr, thyroid | 100/yr, whole body<br>100/yr, thyroid |
| Serious process equipment failure (single failure) | 1 per 3 yr | Either worst weather existing at most 10% of time or Pasquill F condition if local data incomplete | 5, whole body<br>30, thyroid | 100, whole body<br>100, thyroid |
| Process equipment failure plus failure of any special safety system (dual failure) | 1 per $3 \times 10^3$ yr | Either worst weather existing at most 10% of time or Pasquill F condition if local data incomplete | 250, whole body<br>2500, thyroid | $10^3$, whole body<br>$10^4$, thyroid |

safety systems. They further stipulated maximum values for the calculated dose of ionizing radiation to members of the public for any serious process failure (single failure) and for any combination of a serious process failure and failure of a special safety system (dual failure). A corollary is that the special safety systems must be sufficiently separate and independent of the process systems and of each other that the likelihood of a cross-linked failure will be less than that calculated for coincident events (dual failure).

The reference dose limits of the basic requirements (Table 1) were determined on the basis of the assumed maximum frequencies of the events. The maximum frequency of any single failure was taken as one per 3 yr, and the reference dose limits for individuals were chosen as equal to the 1-yr regulatory dose limits. For a dual failure, with an assumed maximum frequency of one per 3000 yrs, the reference dose limits for individuals were chosen as those judged tolerable for a "once-in-a-lifetime" emergency dose.

The population reference dose limits for the dual failure situation were chosen to have a very small relative effect.[11] They would lead to about a 0.1% increase in the lifetime incidence of cancer in a population of 1 million people.

Associated with these reference dose limits are some additional criteria: (1) the design, construction, and operation of all components, systems, and structures essential to the safety of the reactor will follow the best applicable codes, standards, or practice and be confirmed by an independent audit; (2) the quality and nature of the essential process equipment will be such that the total of all serious failures should not exceed one per 3 yr; (3) the special safety systems will be physically and functionally separate from the process systems and from each other; and (4) each special safety system will be readily testable as a system and will be tested at a frequency that demonstrates its unavailability as $<10^{-3}$.

In the early 1970s the difficulty in analyzing a reactor "runaway" accident, i.e., an anticipated transient without scram (ATWS), led to the requirement for two shutdown systems.[12] These must be conceptually different and sufficiently separate and independent of each other so that the criterion for cross-linked failures will be met. With the additional shutdown system, a reactor ATWS is no longer a design-basis accident. If the above criteria are met, a serious release of radioactive fission products could occur only if there were a triple failure, i.e., if two special safety systems failed coincident with a serious process failure. If the requirements for separation and unavailability are met, such a major event would have a probability of the order of $10^{-7}$/yr.

The various dual failures define the performance requirements for the special safety systems. For example, a loss-of-coolant accident (LOCA) plus failure of the ECCS will lead to the release of fission products from the fuel (the "source term") that must be accommodated by the containment. Similarly, a LOCA with impaired containment sets the effectiveness required of the ECCS.

Although the single/dual failure approach, as practiced, adequately defined the required effectiveness of the special safety systems, some concerns in coverage became evident. Among the concerns were (1) the inability to take into account the great variation in rates of occurrence and in the consequences of different single and dual failures; (2) the difficulty of dealing with failure of safety support systems, such as electrical supply, instrument air, or service water, whose failure could result in common failure of a process system and a safety system; (3) the need to consider the necessary continuing operation of safety systems after an accident; and (4) the need to design for, and analyze, the consequences of potential common-cause events, such as earthquakes and aircraft crashes, which could result in damage to both process and safety systems. These concerns pointed to a need for a more comprehensive approach to safety evaluation. This was identified not only by staff of the utilities and of the AECB but also by advisory groups set up by the AECB.[13]

In 1975 the designers proposed using a safety design matrix (SDM) to deal with matters of interdependency and longer-term actions requiring operator intervention. In its present form the SDM is a record of a systematic "what-if" investigation. The analyst selects an event that is a potential safety concern, and the possible causes of this event are identified by a fault-tree analysis. Various postulated consequences are then represented by event sequence diagrams accompanied by a narrative. An example of the sequence diagram is shown in Fig. 2. The use of SDMs has contributed significantly to a better understanding of system behavior and interactions under abnormal operating conditions and has the potential to identify proper operator actions, desirable design modifications, and, in certain cases, contradictory design requirements. It still depends, however, on visual inspection by the analyst for identifying interdependencies between systems. Nevertheless, SDM is currently a major tool used for accident analysis.

At the present time this approach is used primarily for two purposes: (1) to ensure that the four concerns identified previously are addressed in the final plant design and (2) to help establish operating procedures for abnormal events based on realistic event scenarios. It could be modified and extended to predict the risk posed by any postulated sequence of events and to permit design and licensing decisions to be based on calculated risk considerations. Such an approach would be consistent with the recent recommendations of the AECB's Advisory Committee on Nuclear Safety.[14]

The application of probabilistic risk assessment techniques and the development of appropriate data bases have not yet reached the state where individual licensing decisions can be resolved purely on the basis of statistical risk considerations; however, progress is being made,[15] and the information obtained by the use of these techniques is having a steadily increasing impact on licensing decisions. In the meantime the single/dual failure approach, supplemented by the other requirements that have developed over the years and the judicious use of fault trees and SDMs, continues to be the basis for the licensing of Canadian nuclear power plants.

## IMPLEMENTATION

### Regulations

As mentioned earlier, the Atomic Energy Control Regulations[2] are primarily procedural with the exception of the basic radiation protection regulations. Specific requirements are imposed through the licensing process.

The current regulations stipulate two formal licensing steps for nuclear facilities, construction approval and operating license. In practice, formal approval is also given for the site.

Although nuclear projects are a federal responsibility, the AECB has chosen to enlist the cooperation of the provinces in areas that they normally control, such as nonradiological occupational safety and pressure-retaining components. For the latter the AECB approves the classification of components and systems (as submitted by the licensee) according to their importance to the safety of the plant, and the appropriate provincial agency oversees the correct application of the relevant codes and standards. The AECB and the

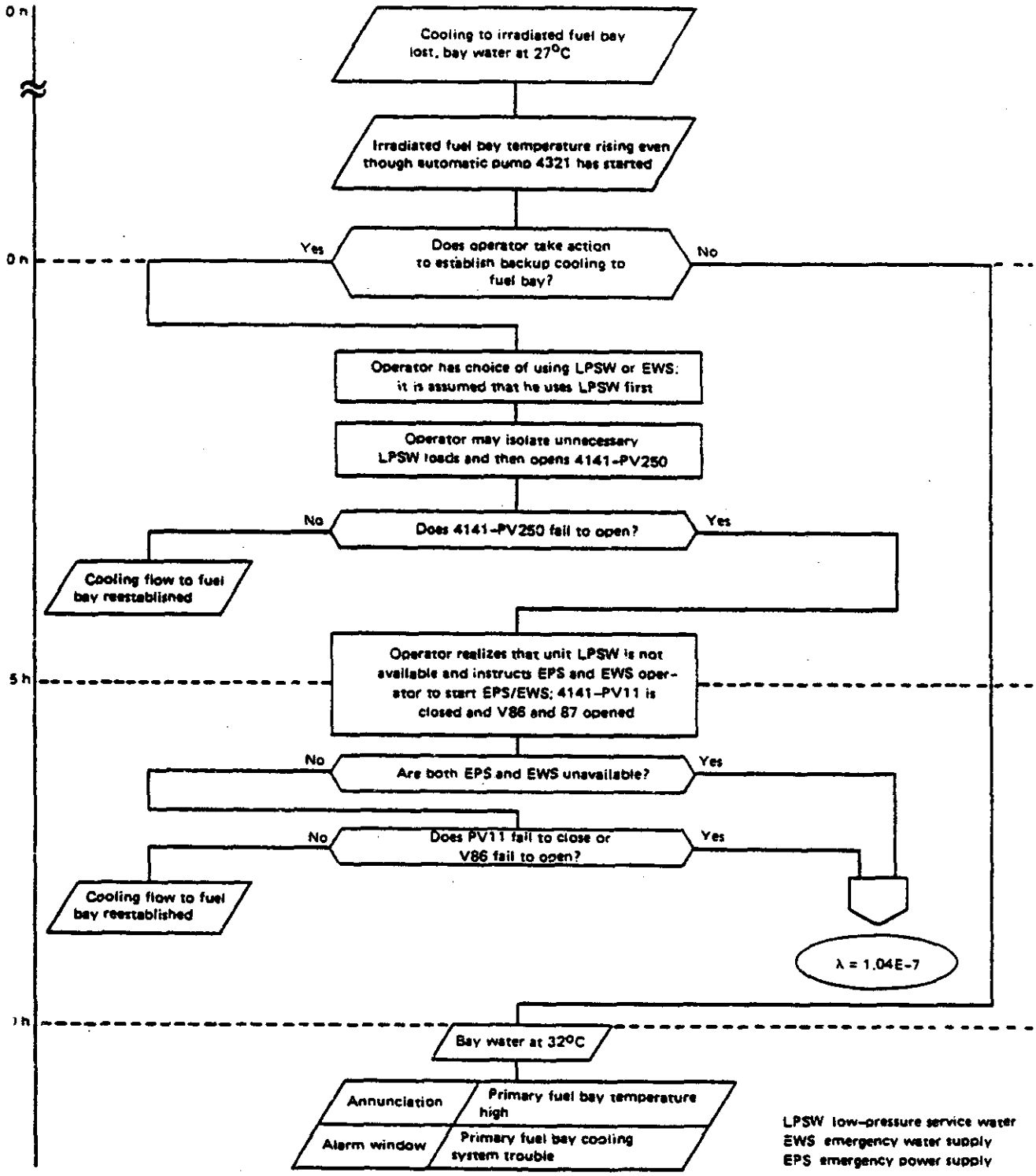



**Fig. 2 Example of event sequence diagram.**

provincial department join in conducting QA audits related to pressure-retaining components.

### Standards

The AECB has issued only a few regulatory documents related to nuclear power plants. Three proposed regulatory guides have been produced, covering the special requirements for the three main safety systems: shutdown system, ECCS, and containment.[16-18]

The policy has been that, although written statements concerning some basic regulatory requirements are necessary and proper for nuclear power plant design, construction, and operation, the establishment of detailed requirements should be handled in other ways. Two methods have been developed.

The first method is a long-standing one that reflects the principle that the primary responsibility for safety rests with the licensee. Nuclear power plant designers have been allowed a very substantial degree of freedom to design plants to meet the basic regulatory criteria. The designs are then submitted to the AECB for approval. This approach has led to the gradual establishment of acceptable safety-related design features. Although these features are not formally identified as requirements, the AECB staff keep them very much in mind in reviewing each new plant design, and further discussions are held with the designers if the features are not evident.

The second method of establishing detailed requirements is the more traditional one of developing consensus nuclear standards for particular topics. Such standards are produced in Canada by the Canadian Standards Association (CSA). The CSA is one of a small number of standards-writing organizations that are officially accredited by the Standards Council of Canada, in accordance with a federal statute, to carry out the preparation and publication of consensus standards. The membership of the CSA is made up almost entirely of organizations and individuals representing the different sectors and industries in Canada. Membership in the CSA is not, however, a prerequisite for participating in the development of CSA standards, and staff members of the AECB have participated in the program since its inception in 1974. At the present time, 22 nuclear standards have been published by the CSA, and some 36 are either in preparation or are undergoing revision.

In recognition of general practice in Canada, some CSA nuclear standards adopt, by reference, certain codes and standards of the United States. Most noteworthy is the CSA N.285 series, which adopts most of the *ASME Boiler and Pressure Vessel Code* and specifies requirements pertinent to a pressure-tube type of reactor not adequately covered by the ASME Code.

Recognizing that regulatory representatives and other participants on the CSA committees might not always be able to agree on the content of every document, each new CSA nuclear standard contains a warning in the preface to the effect that the AECB may have requirements differing from those in the standard. In only one case thus far have additional regulatory requirements been stipulated.

### Licensing Process

Although the AECB regulations call for only two formal steps, construction approval and operating license, in practice the licensing process for nuclear power plants involves a prior step of site acceptance and many intermediate substeps. The licensing process is described in some detail in Ref. 19.

The Atomic Energy Control Act does not require public hearings and, to date, the AECB has not held a hearing for any aspect of its regulatory process, including nuclear power plants. In fact, until recently the licensing process was essentially closed. Two years ago the AECB adopted the policy of making applications for licenses available to the public, as well as the referenced supporting documentation, staff recommendations, and board decision.

Under their environmental legislation, most provinces have a requirement for public hearings on major projects. Despite some possible ambiguities concerning the application of such provincial legislation to nuclear "works," the AECB has supported such hearings.

### Site Acceptance

The basic objectives at the site acceptance stage are to establish the conceptual design of the facility and to determine whether it is feasible to design, construct, and operate the facility on the proposed site to meet the safety objectives and requirements established by the AECB. The primary documentation required is a Site Evaluation Report providing a summary description of the

roposed station and information on land use, resent and predicted population, principal sources nd movement of water, water usage, meteorological conditions, seismology, and local geology. The AECB is primarily concerned with the interrelationship of the site and plant, leaving evaluation of nvironmental impact to associated federal and rovincial environmental agencies.

During this phase the applicant is required to nnounce publicly his intentions to construct the acility and to hold public information meetings at hich the public can express its views and question pplicant officials.

### Construction Approval

Before granting construction approval, the AECB must be assured that the design is such hat the AECB safety principles and requirements ill be met and that the plant will be built to ppropriate quality standards. To do this, it is ecessary that the design be sufficiently advanced o enable the safety analyses to be performed and heir results assessed. The primary documentation equired includes a Preliminary Safety Report which combines the essential information of the ite Evaluation Report, a description of the reference design, and the preliminary safety analyses), n overall QA program for the project together ith a specific program for construction QA, and reliminary plans for operation.

Construction will only be authorized after the esign and safety analysis programs have rogressed to the point that, in the judgment of the ECB, no further significant design changes will e required.

### Operating License

Before issuing an operating license, the AECB ust be assured, primarily, that the plant as built onforms to the design submitted and approved nd that the plans for operation are satisfactory. he requirements include submission of a Final afety Report, completion of a previously approved ommissioning program, examination and authoriation of senior personnel, approval of operating olicies and principles, preparation of plans and rocedures for dealing with radiation emergencies, nd a specific program for operations QA.

Typically a provisional license is issued to permit startup and, subject to AECB staff approval, increases in power to the design rating. Provided all has proceeded satisfactorily, a full operating license is issued for a term not exceeding 5 yr. Among the terms of an operating license is the requirement that the licensee inform the AECB promptly of any occurrence or situation that could alter the safety of the plant. The AECB retains the right to impose additional conditions at any time.

Although the primary responsibility for the safe operation of the plant remains with the licensee, there is continued surveillance by the resident AECB inspectors, annual reviews of operation, and major reviews at times of renewal of the operating license. Formal approval of the AECB would be required for decommissioning, although the situation has not yet arisen.

### Authorization of Operators

The practice to date has been that those members of the operational staff who serve as shift supervisors (SS) and control room operators (CRO) must be specifically authorized by the AECB. In the operating organizations in Canada, these positions bear the prime responsibility for the day-to-day operation. The AECB also must approve appointments to the positions of station manager, production manager, and senior health physicist.

When proposing a person to fill the position of SS or CRO, the station management must provide a written statement of assurance regarding the nominee's capability to carry out the tasks involved. The AECB reviews the training and experience of the nominee and further audits his qualifications by subjecting him to a set of five written examinations.

### Quality Assurance

Like other countries, Canada fully endorses the application of QA principles. The AECB requires that an appropriate, formal QA program be in existence for each phase of a nuclear project: design, construction, commissioning, and operation, as specified in the CSA N286 series of standards.[20–25]

Following the Canadian philosophy, the primary responsibility for establishing the appropriate QA program rests with the owner. The AECB does periodic audits of both the overall programs and specific key parts. In the particular case of

pressure-retaining components, the QA audit is conducted jointly by the AECB and the relevant provincial agency.

### Emergency Planning

From the start of the Canadian nuclear power program, the AECB has set as a condition for licensing a nuclear power plant the preparation of an emergency response plan. The responsibility for ensuring an effective response outside the plant rests with the provincial government. The licensee bears the responsibility for onsite response, initial action, and continuing support to the provincial response organization.

## EXAMPLES OF APPLICATION OF SAFETY PRINCIPLES

### Siting

When Ontario Hydro proposed siting a major nuclear power station near Toronto (Fig. 3) in the early 1960s, one aspect received particular attention: the proximity of a large population. The population reference dose limits in the Siting Guide (Table 1) provided the criteria for the evaluation.[26]

The projected 1986 population figures for the region around the site were used with a Pasquill F dispersion plume, which was assumed to extend outward from ground level at the reactor building in a direction to include the maximum extrapolated population density. The dose to the population within this plume was then calculated to a point (at 29 km) where the dose to an individual would be 1% of that to an individual at the plant exclusion area boundary (at 1 km). From this it was concluded that, over the expected lifetime of the station, the population dose from postulated accidents would not be a limiting factor. Rather, it was the dose to the individual situated on the exclusion area boundary that was governing.

A short time before operation of the Pickering station had begun, the federal government proposed and began assembling land for a major airport only 16 km away. Although the AECB's criteria at that time did not specifically address external hazards, it was consistent with those criteria to set an acceptable probability of significant consequences to the public at about $10^{-7}$. The AECB initiated work at the École Polytechnique in Montréal to determine what risk the presence of the airport would present to the nuclear power section.[27] A risk map was produced (Fig. 4) showing the contours of rate of crash as a function of distance from the airport for a site of 0.31 km$^2$ and an angle of crash of 10°. This indicated that, had the airport development plans gone ahead (they have not, as yet), some relocation of the airport would have been necessary to keep the probability of a penetrating aircraft crash on the power plant complex to an acceptable level. The aircraft crash study was later extended to investigate generally the response of a concrete reactor containment building to the impacts of various parts (fuselage and engines) of various types of heavy aircraft (such as DC-8 and B-747), depending on the angle of impact.[28]

Concern about the habitability of the main control room (which is located outside containment) if subjected to either internal or external hazards, such as turbine breakup, aircraft crashes, fire, or earthquakes, led to a proposal by the licensees to establish a second control area some distance away (e.g., for the Pickering B station, the separation achieved is of the order of 46 m). From this second control center, the state of several systems important to the safety of the reactor could be monitored and/or controlled, and the center itself was designed to withstand the design-basis earthquake. This arrangement came to be known as the "two-group concept," with the distribution of safety functions as is shown in Table 2.

### Design

Strict application of the safety philosophy to the design of a nuclear power plant can pose difficult design and analysis problems. Because the analysis of ATWS-type events was considered to be too speculative, the solution to the problem proposed by the designers and accepted by the AECB was to reduce the probability of the event by several orders of magnitude by designing another essentially independent and diverse means of rapid reactor shutdown. This led to the requirement for two shutdown systems mentioned earlier.

The layouts of the traditional gravity rod shutdown system and of the high-pressure liquid neutron poison injection system, relative to the reactor core, are shown in Fig. 5. Maximum physical separation is achieved by having the rod system enter the reactor vertically with all the actuating

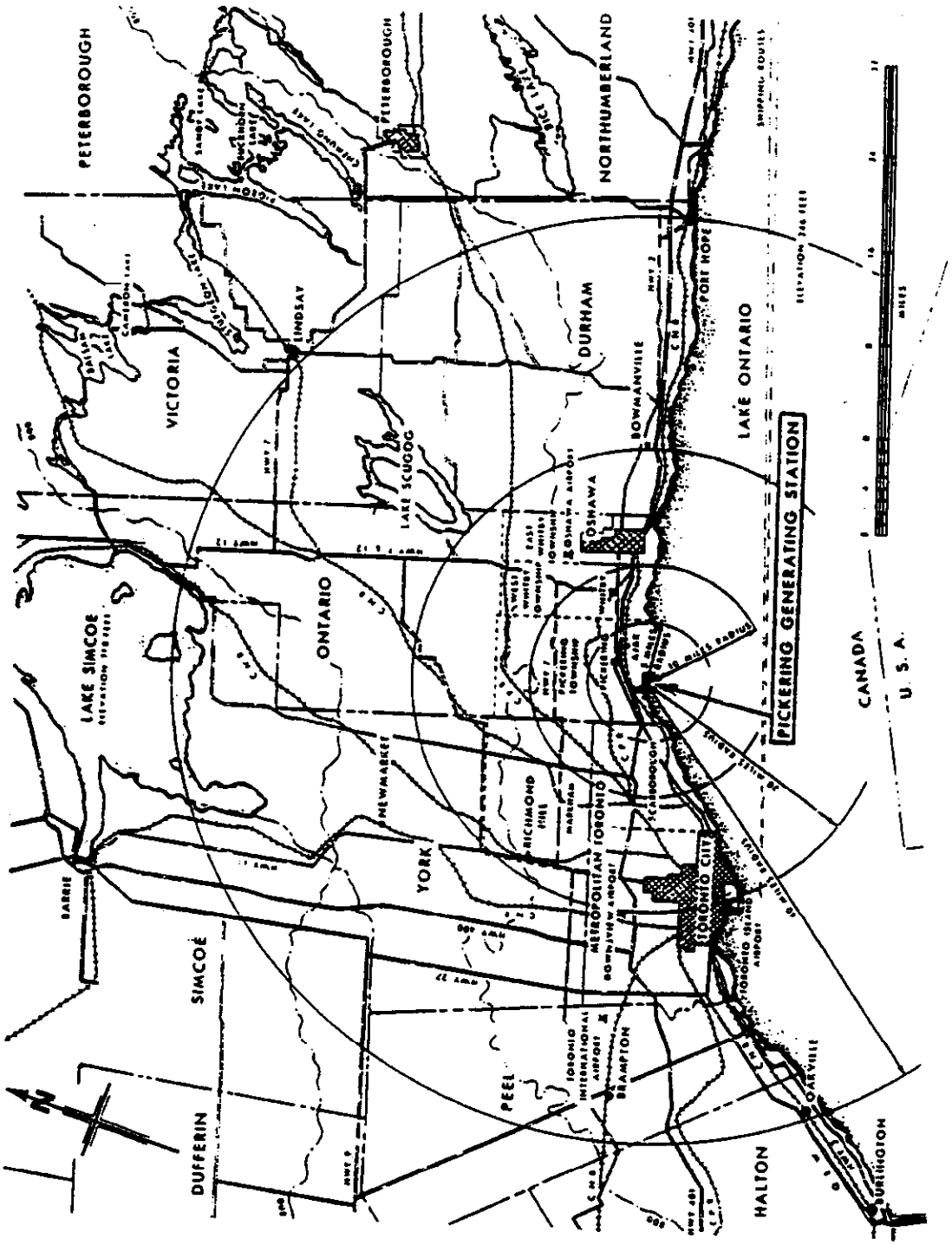



Fig. 3 Site location with 64-km radius.

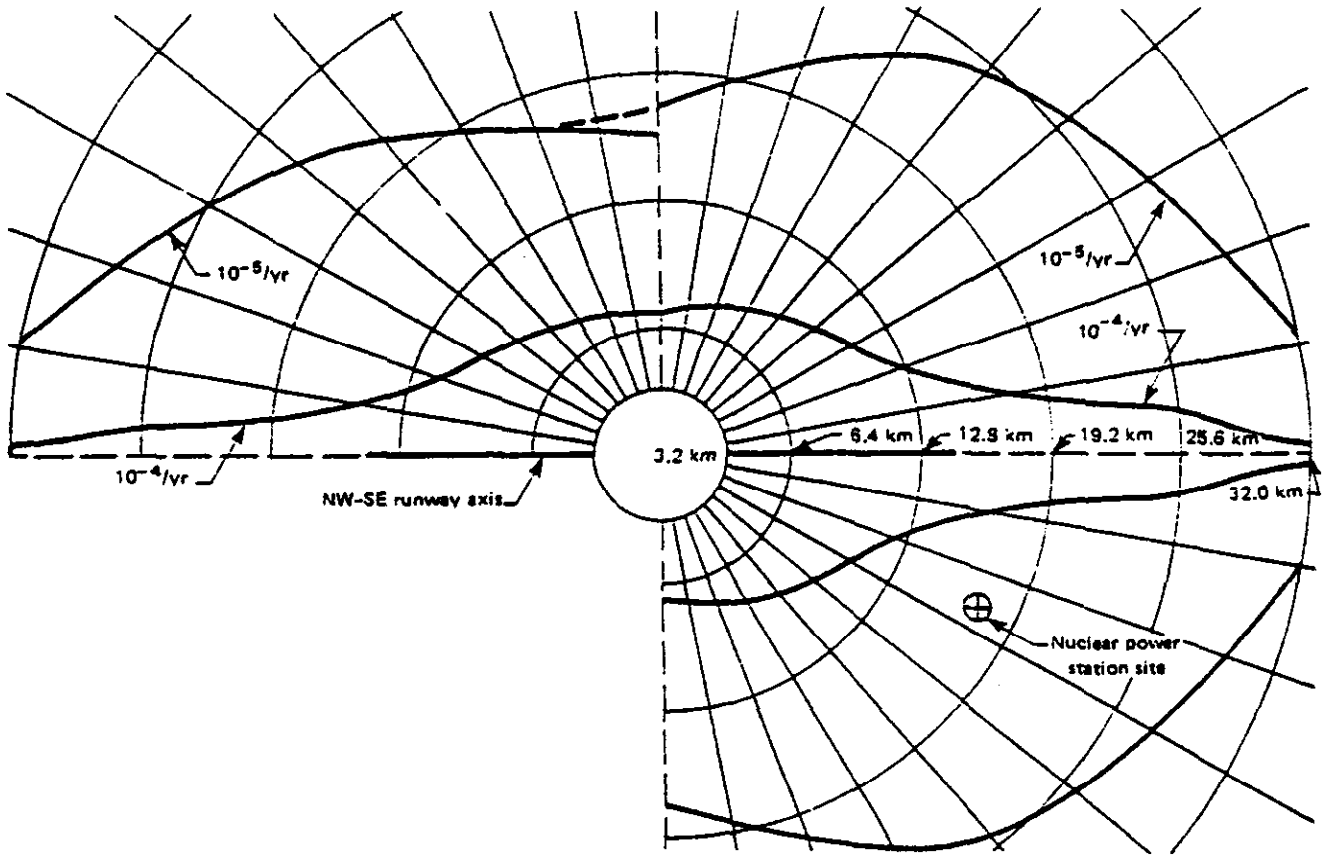



**Fig. 4 Rate of crash contour lines for heavy aircraft traffic—an approximation to the Pickering case (figure is symmetrical about runway axis).**

**Table 2 Two-Group Concept for Distribution of Safety Functions**

| Safety function | Systems and equipment | |
|---|---|---|
| | Group 1 | Group 2 |
| Shut down reactor | Shutdown system 1 | Shutdown system 2 |
| Remove decay heat | Normal electrical power and cooling water supplies | Emergency power supply and emergency water supply |
| Monitor postaccident conditions | Main control room | Secondary control area |

mechanisms located on top of the reactor. The liquid injection system, however, enters the reactor from the side, and all its equipment is located in rooms to one side of the reactor. All sensors and instrumentation for each system are completely separate, as are the cable routes. Maximum diversity is achieved by using different concepts of operation and different pieces of hardware for each system.

Both shutdown systems are completely separate from the regulating system. The designers had first proposed the dual use of some of the rods for both shutdown and regulation. Because this was a violation of the separation criterion, it was not allowed.

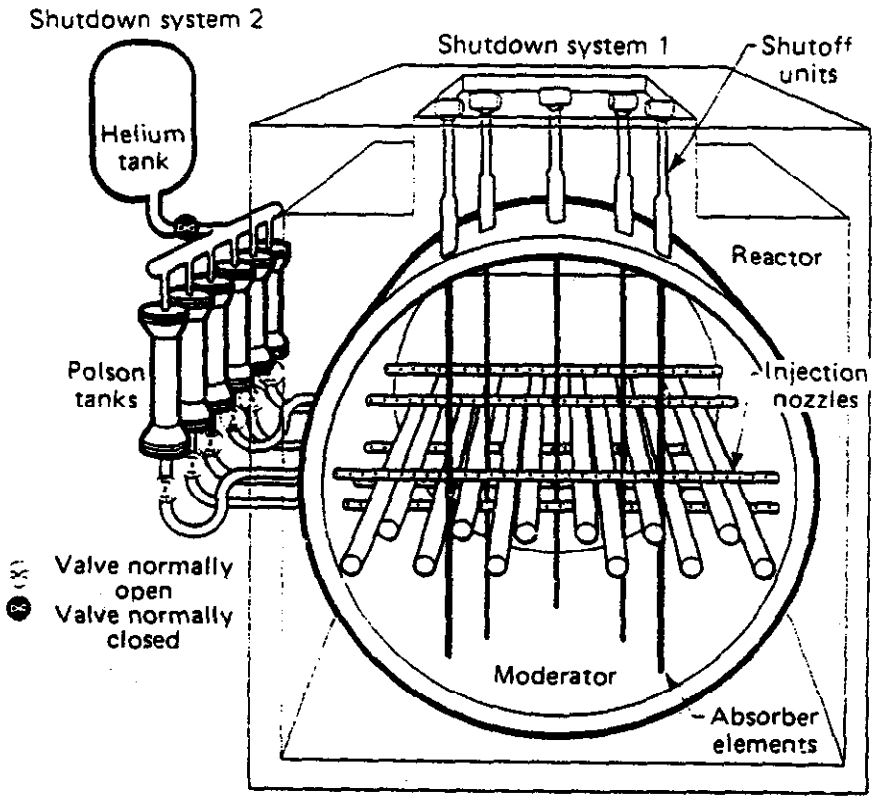



Fig. 5 Safety systems.

e final design uses completely separate shutdown ls and regulating rods albeit of similar design.

The proposal by the Bruce A station designers place major equipment, such as main heat nsport pump motors and boilers, outside con- nment (Figs. 6 and 7) to facilitate inspection, ting, and maintenance posed a particularly ficult situation for the AECB. The interdepen- ice between process equipment and a special ety provision (containment) was obviously being reased, but there were potential gains to be de in the reduction of personnel exposure during intenance and in the greater freedom to carry tests on the equipment. Early experience with single unit, the 200-MW(e) prototype Douglas nt station that started operating in 1967, had to a personnel dose burden as high as 1935 n-rems in 1971. Although these problems have e been corrected and personnel dose burdens now running at 200 to 400 man-rems annually, re was a very strong incentive at the time to rove routine access to equipment. The AECB sidered the trade-off advantageous and gave its roval. The appropriateness of that decision can be judged by noting that, for 1982, the total personnel dose burden for the four-unit 3000-MW(e) Bruce A station was only 370 man-rems.

### Commissioning

The objective in the commissioning program is to test equipment and systems as thoroughly as practical under simulated normal, upset, and accident conditions. Particular emphasis is placed on testing complete systems to confirm that they will respond as predicted in the safety evaluation.

For stations that use a vacuum containment system, an important set of components are the pressure relief valves (Fig. 8), which interconnect the reactor buildings with the vacuum building. These valves are 2 to 3 m in diameter and would be required to open rapidly under LOCA conditions. To confirm satisfactory operation, these massive valves are stroked at their maximum design rate of opening (25 to 100 cm/s). These tests are followed by testing of the pressure suppression system as a whole. This is achieved by simultaneously opening all the pressure relief valves, thus allowing air to flow into the vacuum building. The resultant

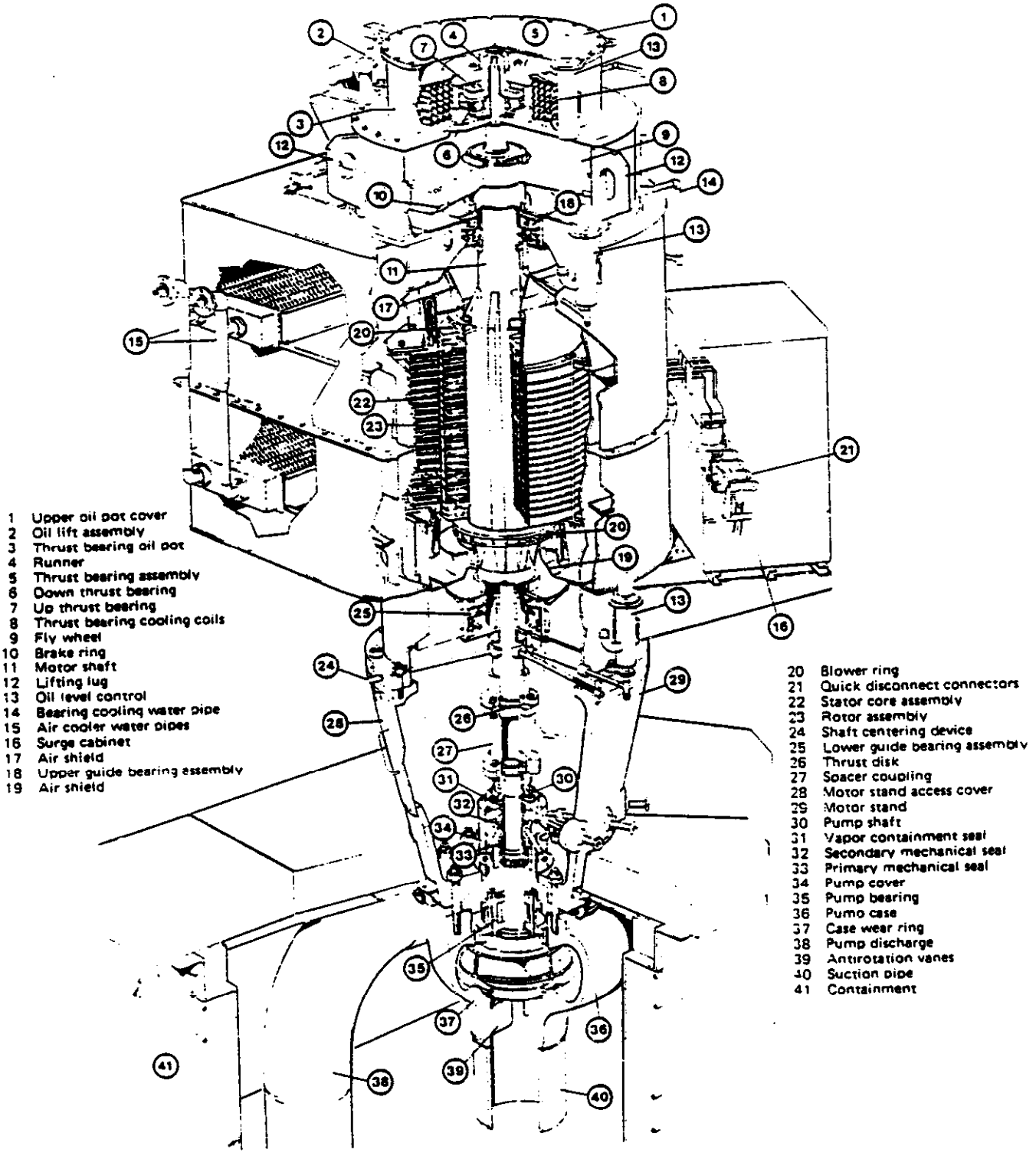



Fig. 6 Heat transport pump.

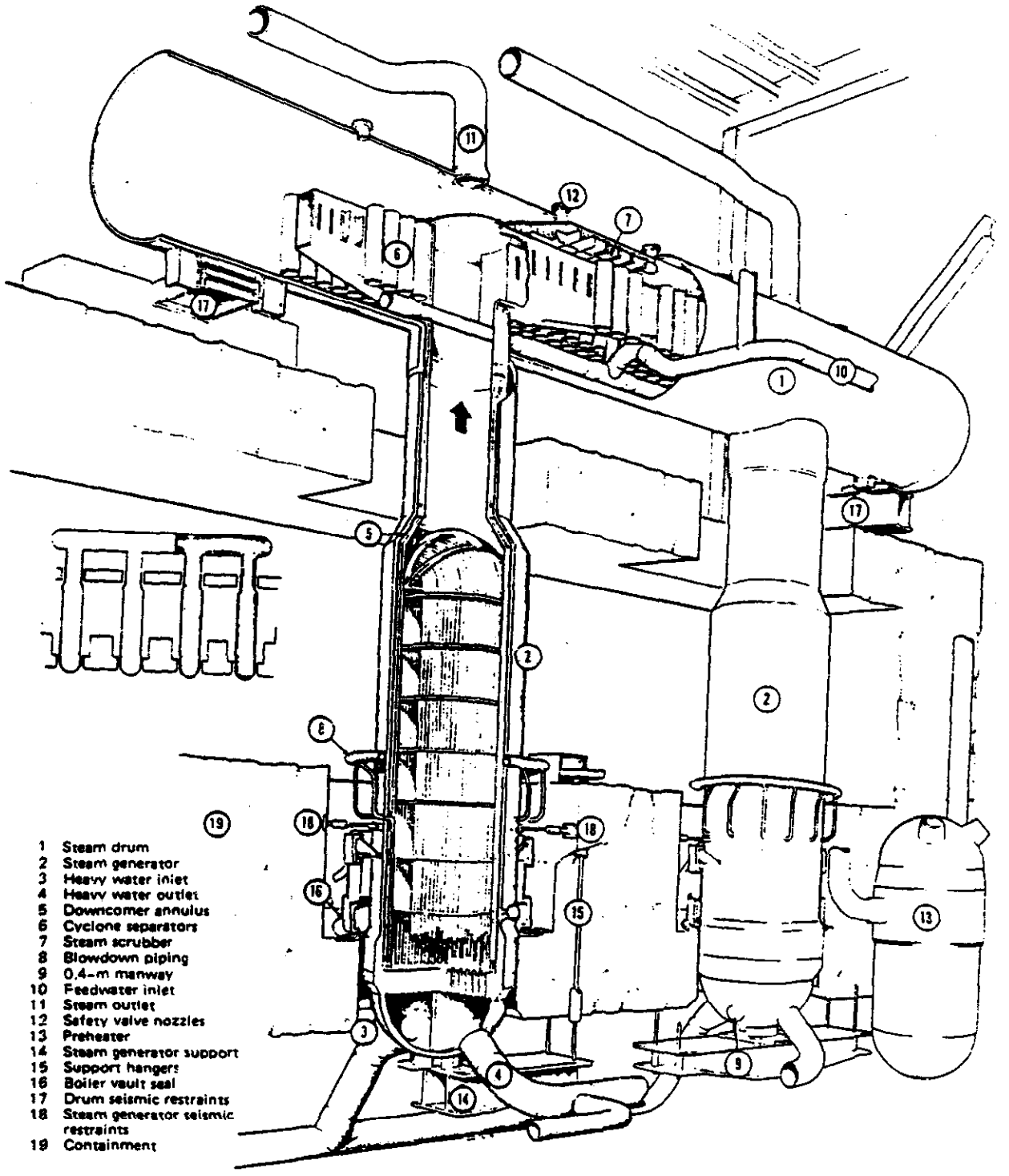
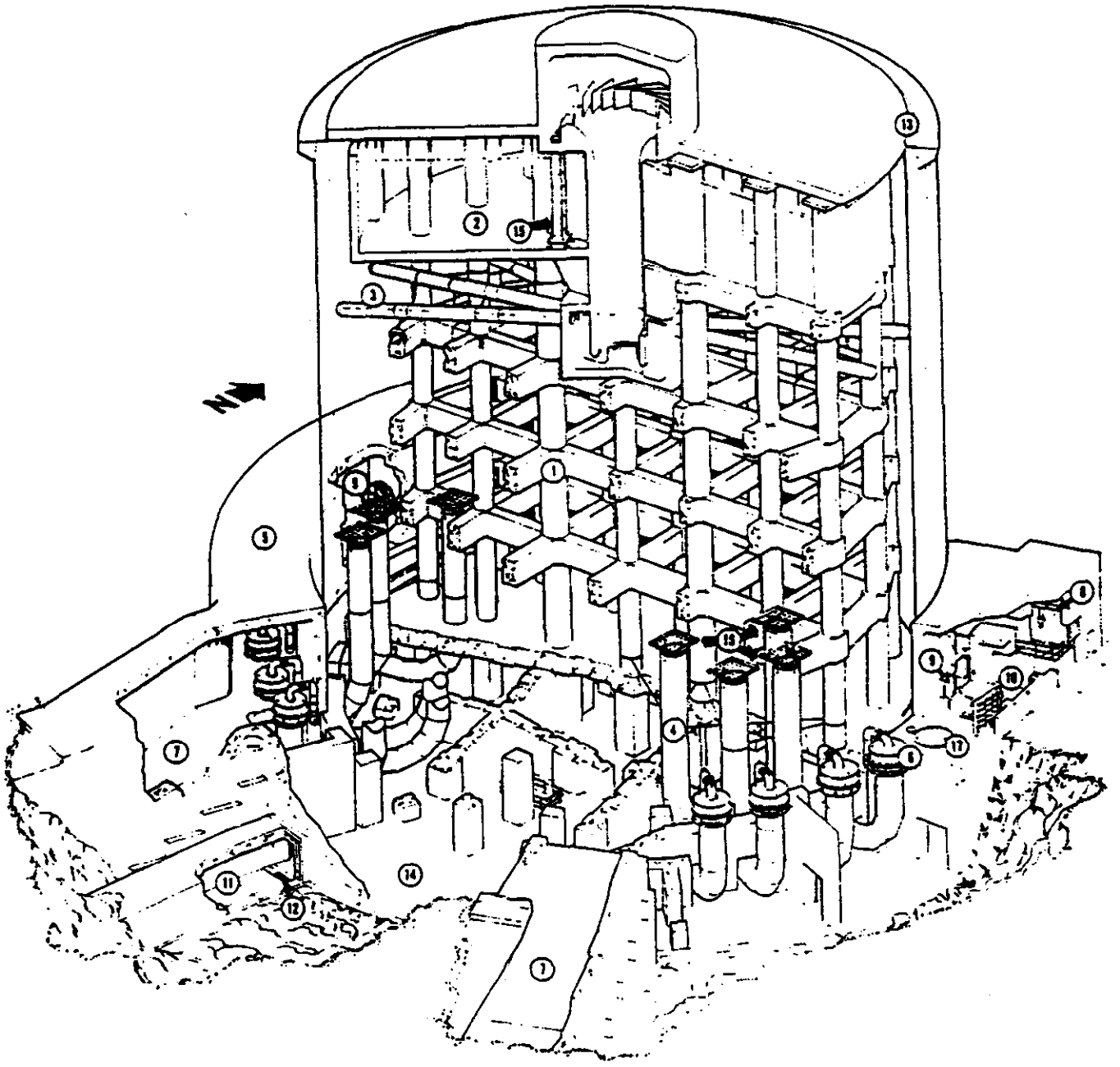



Fig. 7 Bruce A steam generators and preheaters.



1 Internal structure
2 Emergency water storage tank
3 Distribution and spray headers
4 Vacuum duct
5 Valve manifold
6 Pressure relief valve
7 Pressure relief duct
8 Monorail and hoist
9 Personnel airlock
10 Equipment airlock
11 Service tunnel
12 Catch basin
13 Roof/wall seal
14 Basement
15 Suction pipes
16 Diffusing screens
17 Vacuum duct coverplate

Fig. 8 Cutaway view of vacuum building and valve manifold.

se in pressure in the vacuum building actuates ıe passive dousing system located in its dome. In ıe single containment building design, however, ith the gravity dousing system located in the ome above the reactor, the AECB has accepted ıat only the dousing system's active components .ogic and valves) need to be tested because an ctual douse would entail a major cleanup and :testing of other reactor system components.

Commissioning of the ECCS presents difficul-es. The AECB accepts that it is not practical to mulate a rupture in the heat transport system for ıe purposes of commissioning. However, operation the system as a whole can be demonstrated ther by injecting water into a partially voided :actor core or by installing valved discharge lines :st ahead of the core injection valves to permit ɔmmissioning tests at full design flow. Another ɔeration, which is an essential part of the emer-ɛncy core cooling function, is rapid depressuriza-on of the core by initiating a fast or "crash" cool-ɔwn of the steam generators. This feature is :sted by opening several of the boiler safety valves multaneously, with all systems at temperature.

Under some postulated upset and accident con-:tions, thermosyphoning may be necessary to keep ıe core cooled immediately after reactor ıutdown. All such postulated events are examined, ıd commissioning tests are done to demonstrate ıtisfactory cooling capability under various ɛnarios with full coolant inventory. Clearly such sts must be done with the reactor operating at :veral percent of full power.

### peration

One of the fundamental criteria in the Cana-an safety approach is that each special safety stem be readily testable as a system and be sted at a frequency that demonstrates that its ıavailability is $<10^{-3}$. In the design of a plant, athematical models are developed to predict the :ture unavailability of the special safety systems ısed on predicted failure rates for each com-ɔnent and a defined testing schedule. Because the quired test intervals for most components range om several days to 1 month, it is evident that ɔmponents and systems must be testable while the actor is operating at high power. A further objec-ve of the test program for special safety systems that, as far as practical, the tests should simulate ɔcident conditions.

The test program for the safety systems includes literally hundreds of prescribed tests each month and represents a significant manpower expenditure on each operating shift. Some tests are simply of a single component where testing of a system is not practical (e.g., stroking of one of the 2- to 3-m-diameter pressure relief valves connecting a reactor building to a vacuum building).

Where practical, system tests are done. For example, to test a high neutron power trip, a boron shutter at an ion chamber is retracted to increase neutron flux at the ion chamber. A "trip" of one of the triplicated channels should occur, and this, in turn, should result in a reduction in the current to the coils of the clutches that hold up the shutoff rods. To complete the test of the system, a separate test is done on individual rods where the clutch coils are de-energized momentarily to demonstrate that the shutoff rods will fall. Similarly, for a subsystem that isolates the reactor building on an indication of high building pressure, the test involves increasing the pressure at the pressure indicator to ensure that a signal is transmitted to the isolating valves.

By virtue of the redundancy in the special safety systems, some of the maintenance of these systems can be done without any reduction in the demonstrated availability of the systems. Each special safety system incorporates three independent logic channels with safety system action resulting if any two channels are tripped. For maintenance of any equipment, the associated channel is first placed in a safe (tripped) state. In the event of, for instance, a defective ion chamber, the operators must place the associated logic channel in a safe (tripped) state before removing the ion chamber. After repair and replacement, it is thoroughly tested in situ before the logic channel is returned to service.

In common with the rest of the world, in-service inspection of the heat transport pressure boundary is required. The requirements for in-service inspection are documented in Canadian Standard CSA N285.4 (Ref. 29), which has been supplemented by a regulatory requirement for additional inspection of fuel channel feeder pipes, pressure tubes, and boiler tubes.

## SUMMARY AND DISCUSSION

With the lessons learned from the 1952 accident to the NRX research reactor vivid in the

minds of many, the approach to power reactor safety in Canada embodied numerical safety goals from the outset. Although the objective was to limit risk to a defined value, the analytical tools were not available to demonstrate compliance with the objective. Consequently a simplified approach, as summarized in Table 1, was adopted in the mid-1960s.

This approach (single/dual failure) was first used in the design and safety evaluation of the Pickering A Generating Station and has continued to evolve since that time. A comparison of the operation of reactors against these design requirements[30] confirms that the approach has been sound and that only evolutionary, rather than revolutionary, changes were required. The frequency of serious process failures has been consistent with early predictions. Some shortcomings in the availability of special safety systems have been encountered, but the necessary corrective actions have been taken to meet the numerical safety goals.

In the process of applying the single/dual failure approach, a number of additional requirements related to reliability objectives have been adopted: for example, any serious process failure should be detected by two diverse parameters. The need for or adequacy of such requirements cannot be rigorously defended in the absence of appropriate component failure data and comprehensive probabilistic risk assessments. However, because adequate tools for doing such assessments are not yet in common use, such requirements will remain. It is, nonetheless, an objective in Canada to improve the capability to do probabilistic safety evaluations. The primary purpose for using fault trees and event trees at the present time is to aid the design and decision-making process. In the longer term, as analytical capabilities and the data bases improve (particularly for the effects of human intervention), it will be possible to assess better the risk posed by nuclear power plants. This will permit a better comparison with the numerical safety goals adopted almost three decades ago in the Canadian risk philosophy.

## REFERENCES


1. *Atomic Energy Control Act 1946* (as amended 1954), Chap. A-19: Atomic Energy, pp. 153-161, Revised Statutes of Canada, 1970.
2. Atomic Energy Control Regulations CRC 1978, SOR/79-422, Chap. 365, *Canada Gazette, Part II*, 113 (11): 2211-2345 (May 13, 1979).
3. *Nuclear Liability Act* (1st Supplement, 1976), Chap. 29: Nuclear Liability, pp. 907-923, Revised Statutes of Canada, 1970.
4. Atomic Energy of Canada Limited, *CANDU Nuclear Power System*, Report TDSI-105, January 1981.
5. D. A. Meneley and W. T. Hancox, *LOCA Consequence Predictions in a CANDU-PHWR*, presented at the International Conference on Nuclear Power Experience, Vienna, Sept. 13–17, 1982, International Atomic Energy Agency, Preprint IAEA-CN-42/145.
6. Advisory Committee on Nuclear Safety, *A Proposed Statement on Safety Objectives for Nuclear Activities in Canada*, Report INFO-0055, Atomic Energy Control Board, June 1981.
7. E. Siddall, *Reactor Safety Standards and Their Attainment*, Report AECL-498, Atomic Energy of Canada Limited, September 1957.
8. G. C. Laurence, *Reactor Siting in Canada*, Report AECL-1375, Atomic Energy of Canada Limited, October 1961.
9. G. C. Laurence, *Reactor Siting Criteria and Practice in Canada*, presented at the American Nuclear Society National Topical Meeting on Nuclear Power Reactor Siting, Los Angeles, Feb. 18, 1965, Atomic Energy Control Board, Preprint AECB-1010.
10. D. G. Hurst and F. C. Boyd, *Reactor Licensing and Safety Requirements*, Paper AECB-1059, Atomic Energy Control Board, June 11, 1972.
11. F. C. Boyd, *Containment and Siting Requirements in Canada*, presented at the International Atomic Energy Agency Symposium on the Containment and Siting at Nuclear Power Plants, Vienna, Apr. 3, 1967, Atomic Energy Control Board, Preprint AECB-1018.
12. J. H. F. Jennekens, *Recent Developments in Nuclear Plant Licensing in Canada*, Report AECB-1074, Atomic Energy Control Board, June 1974.
13. Inter-Organizational Working Group, *Proposed Safety Requirements for Licensing of CANDU Nuclear Power Plants*, Report AECB-1149, Atomic Energy Control Board, November 1978.
14. Advisory Committee on Nuclear Safety, *Recommended General Safety Requirements for Nuclear Power Plants*, unpublished Draft Report ACNS-4.
15. Atomic Energy Control Board, *Regulatory Guide on the Use of Fault Trees in Licensing Submissions*, Consultative Document C-70, in press.
16. Atomic Energy Control Board, *Requirements for Containment Systems for CANDU Nuclear Power Plants, Proposed Regulatory Guide*, Consultative Document C-7/REV-1, May 21, 1982.
17. Atomic Energy Control Board, *Requirements for Shutdown Systems for CANDU Nuclear Power Plants, Proposed Regulatory Guide*, Consultative Document C-8/REV-1, May 21, 1982.
18. Atomic Energy Control Board, *Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants, Proposed Regulatory Guide*, Consultative Document C-9/REV-1, May 21, 1982.
19. M. Joyce, *The Licensing Process for Nuclear Power Reac-*

*tors*, Report AECB-1139/Rev.1, Atomic Energy Control Board, Nov. 21, 1979.

Canadian Standards Association, *Quality Assurance Program Requirements for Nuclear Power Plants*, Standard N286.0.

Canadian Standards Association, *Procurement Quality Assurance for Nuclear Power Plants*, Standard N286.1.

Canadian Standards Association, *Design Quality Assurance for Nuclear Power Plants*, Standard N286.2.

Canadian Standards Association, *Construction and Installation Quality Assurance for Nuclear Power Plants*, Standard N286.3.

Canadian Standards Association, *Commissioning Quality Assurance for Nuclear Power Plants*, Standard N286.4.

Canadian Standards Association, *Operations Quality Assurance for Nuclear Power Plants*, Standard N286.5

Ontario Hydro and Electric Power Commission, *Pickering Generating Station Safety Report, Volume 2*, 1969.

P. Godbout and A. Brais, *A Methodology for Assessing Aircraft Crash Probabilities and Severity as Related to the Safety Evaluation of Nuclear Power Stations*, École Polytechnique de Montréal, September 1976.

P. Godbout and A. Brais, *A Methodology for Assessing Aircraft Crash Probabilities and Severity as Related to the Safety Evaluation of Nuclear Power Stations, Phase III*, École Polytechnique de Montréal, March 1980.

Canadian Standards Association, *Periodic Inspection of CANDU Nuclear Power Plant Components*, Standard N285.4.

Z. Domaratzki, *Reactor Safety Requirements in Times of Change*, presented at the 20th Annual International Conference of the Canadian Nuclear Association, Montreal, Canada, June 17, 1980, Atomic Energy Control Board, Paper INFO-0005, June 1980.

- 1993 -

# The Canadian Approach to Reactor Safety

## A review of the past and a view of the future

**Fred Boyd**

*Ed. Note: the following is based on a paper presented at the International Nuclear Congress, INC '93, in Toronto, October 1993.*

### Introduction

The origins of the Canadian approach to nuclear safety go back to the work of the pioneers at the Montreal Laboratory during World War II. The Montreal Laboratory was established in late 1942, as a collaborative UK - Canada project including several senior scientists from Europe who had escaped the Nazi invasions. A factor in the decision to locate the project in Canada was the work by G.C. Laurence and B.W. Sargent in building a sub-critical "pile" of graphite and uranium oxide at the National Research Council in Ottawa over the years 1940-41. Laurence, who had studied under Rutherford and had been in charge of radium and X-ray dosimetry, became the senior Canadian at the Montreal Laboratory and subsequently a leader in reactor safety.

Fission had been reported only in early 1939 and after the beginning of World War II later that year the flow of scientific information essentially stopped. The Members of the Montreal Laboratory had, therefore, to develop the theories needed to provide a basis for the design of a heavy-water-moderated, natural-uranium-fuelled research and production reactor which became the focus of the project. Construction of the NRX reactor began at the remote site of Chalk river in late 1944 and it went into operation in 1948. A zero energy facility, ZEEP, was built and operated in 1945, and became the first reactor to operate outside the USA. Originally designed for 20 MW(th) NRX was upgraded to 30 MW(th) by 1952.

Although safety was not identified as a specific topic at the Montreal Laboratory it was inherent in much of the work as evidenced by papers on topics such as, reactor control, reactor dynamics, and radiation protection. In the last area, radiation protection, which is outside the scope of this paper, the concept of "ALARA" (as low as reasonably achievable) was developed, many years before it became the international creed, and dose limits were prescribed which were well below the practice in other countries at the time.

That those pioneers were very aware of the hazards of a nuclear reactor was reflected in the choice of the then remote site of Chalk River, the early atmospheric dispersion tests, and the numerous safety devices installed on the original NRX reactor.

### Context

Although health and safety are normally within the purview of the provinces, the special nature of atomic energy enabled the federal government to pass the Atomic Energy Control Act in 1946, establishing the Atomic Energy Control Board (AECB) with very broad powers. That Act has had only one significant revision, in 1954, to allow for the establishment of the crown corporation Atomic Energy of Canada Limited to operate the nuclear program and to set the AECB as the nuclear regulatory agency.

When power reactors were first proposed, in the early to mid 1950s, the AECB marshalled the most experienced nuclear and conventional power and safety specialists in the Reactor Safety Advisory Committee (RSAC) which it created in 1956, with Laurence as its first chairman, and which, for the next two decades, determined reactor safety requirements. With the growth in numbers and competence of its staff, the AECB, in 1980, dissolved the RSAC and created two generic advisory committees on radiation protection and nuclear safety.

### Origins

Despite the many safety devices incorporated in its design, NRX suffered a serious "runaway" accident in December 1952 which caused major damage to the reactor core. Although the calandria (reactor vessel) was replaced and the reactor repaired, to start up again, at an upgraded power of 40 MW(th), in 1954, the accident served as a catalyst for the development of much of the reactor safety approach that still prevails.

The accident led to incisive reviews of the safety of reactors and, in particular, to consideration of the goals and philosophy for the safety of power reactors on which studies had just begun. Some of this new perspective is implied in the official reports on the NRX accident by W.B. Lewis and D.G. Hurst.[1,2] However, a proposal by E. Siddall, in a seminal report in 1957,[3] to use "risk" as a basic criterion or goal marked the beginning of the Canadian approach to reactor safety.

Siddall looked at the accident death rate from alternative forms of producing electricity, especially coal-fired generating plants, and proposed that nuclear plants be significantly better. On that basis he suggested that a risk of one death per six years for a 200 MW(e) nuclear power plant should be acceptable.

About the same time Laurence was also pursuing the "risk" approach and proposed a design target of $10^{-5}$ serious accidents per year, derived from a goal of less than one death per 100 reactor years and a presumption that a major accident could result in up to 1,000 fatalities.[3] The goal and approach were adopted by the designers of the small (20 MW(e)) Nuclear Power Demonstration (NPD), Canada's first nuclear power plant, which began operation in 1962 and for the prototype, 200 MW(e), Douglas Point generating station. This use of a numerical risk goal became the foundation of Canadian reactor safety philosophy.

Laurence argued that such a low probability could not be achieved, and, particularly, could not be demonstrated, with single systems. He proposed that the target could be achieved, with realistic designs, if there were adequate separation between, and independence of, the operating systems, the protective devices and the containment provisions.

If there were adequate independence of those three divisions of the plant, and if a serious release required failure of all three, the frequency of such a release would be the product of the frequency of the initiating process failure and the unavailabilities of the safety systems. Laurence showed that the desired low frequency of a serious release could, therefore, be achieved with practical, demonstrable, values for process failures and safety system unavailabilities.

In the mid 1960s, at an early stage of the design of the large, four-unit, Pickering (A) plant, these concepts were formalized into a set of criteria that came to be called the "Siting Guide". Subsequently the approach was modified to consider the plant as having two sets of systems; the operating "process" systems, and the "special safety systems" comprising the reactor shutdown systems, the emergency ency cooling systems, and the containment.

The basic requirements, as last formally modified in 1972,[5] set limits on the frequency of serious failures of the process systems* and on the unavailability of the special safety systems. They further stipulated maximum values for the calculated dose of ionizing radiation to members of the public for any serious process failure (single failure) and for any combination of a serious process failure and failure of a special safety system (dual failure). (See Table 1)

It was clearly implied that the special safety systems must be sufficiently separate from and independent of the process systems and of each other that the likelihood of a cross-linked failure will be less than that calculated for coincident events (dual failures).

The reference dose limits of the basic requirements were determined against the assumed maximum frequencies of the events. The maximum frequency for 'single failures" (serious process failures) was taken as one per three years and the reference dose limits for individuals were chosen as equal to the one-year regulatory limits for members of the public. For "dual failures", with assumed maximum frequency of one per 3,000 reactor years, the reference dose limits for individuals were chosen as those judged tolerable at the time, by the UK Medical Research Council, for a "once-in-a-lifetime" emergency dose.

Associated with these reference dose limits were some additional criteria such as:

- the design, construction and operation of all components, systems and structures essential to the safety of the reactor shall follow the best applicable codes, standards or practice and be confirmed by independent audit;
- the quality and nature of the essential process equipment shall be such that the total of all serious failures should not exceed one per three years;
- each special safety system shall be readily testable as a system, and be tested, to demonstrate that its unavailability is less than $10^{-3}$.

To achieve testability as well as reliability many safety systems were triplicated and operated on a two out of three auctioneering arrangement.

* A serious process failure was defined as one that, in the absence of special safety system action, could lead to fuel failure or the release of radioactive material to the environment.

The requirement for separation of systems, the specification of maximum unavailabilities, and the reference dose limits, were all a means towards an end – an appropriately low probability of a significant release of radioactive fission products – in the absence of credible probabilistic analytical techniques.

In the early 1970s, the difficulty in analyzing a "runaway" accident, i.e., an anticipated transient without scram (ATWS), led to the requirement for two shutdown systems. These must be conceptually different and sufficiently separate and independent of each other that they can be considered as distinct "special safety systems". With this requirement an ATWS is not a design-basis accident.

If the criteria of the "Siting Guide" are met a major release of radioactive fission products would occur only if there were a "triple" failure, i.e., if two special safety systems failed coincident with a serious process failure. If the requirements for independence and unavailability are met such an event should have a probability of the order of $10^{-7}$ per year.

The matrix of dual failures defines the requirements for the special safety systems. For example, a loss-of-coolant accident (LOCA) plus failure of the emergency core cooling system will lead to the release of fission products from the fuel (the "source term") that must be accommodated by the containment. Similarly, a LOCA with impaired containment sets the effectiveness required of the ECCS.

## Relationship to Design

Exploiting the successful experience of NRX, and the subsequent larger NRU, research reactors, the heavy-water-moderated, natural-uranium-fuelled reactor concept was pursued for power applications. The original design of the NPD demonstration plant incorporated a pressure vessel but this was abandoned in favour of the pressure tube concept, that became a characteristic of the CANDU design, when zirconium alloys were shown to be suitable.

The large size of CANDU plants resulting from the use of heavy water as a moderator made it easier to incorporate

| Situation | Assumed maximum frequency | Meteorology to be used in calculation | Maximum individual dose limits, mSv | Maximum total population dose limits, Sv |
|---|---|---|---|---|
| Normal operation | | Weighted according to effect, i.e., frequency times dose for unit release | 5/yr, whole body<br>30/yr, thyroid | 100/yr, whole body<br>100/yr, thyroid |
| Serious process equipment failure (single failure) | 1 per 3 yr | Either worst weather existing at most 10% of time or Pasquill F condition if local data incomplete | 5, whole body<br>30, thyroid | 100, whole body<br>100, thyroid |
| Process equipment failure plus failure of any special safety system (dual failure) | 1 per $3 \times 10^3$ yr | Either worst weather existing at most 10% of time or Pasquill F condition if local data incomplete | 250, whole body | $10^4$, whole body<br>$10^4$, thyroid |

**Table 1: Operating Dose Limits and Reference Dose Limits for Accident Conditions**

the separate shut-down systems dictated by the safety philosophy. On-power fuelling, made practicable by the pressure tube design, reduces the need for large reserves of excess reactivity and eases the control problem.

Practical lattice arrangements result in small but positive reactivity power coefficients. This provided added impetus to the development of automatic control systems which have been a feature of all CANDUs. Automatic control also frees the human operators from being a mundane link in the control loop so that they may make full use of their knowledge and judgement.

Canadian expertise and experience in concrete structures influenced the early choice of concrete containment buildings. This, in turn, led to the use of dousing systems and, for the multi-unit stations, attached vacuum buildings, to minimize the containment building pressure in the event of a LOCA. While such designs did not deviate from the safety approach they did complicate the containment provisions which became a set of systems.

## Developments in Approach

Although this single/dual failure approach provided functional requirements for the special safety systems some concerns and reservations arose. Among these were:

- the difficulty of separating safety support systems or dealing with their failures;
- the fact that some special safety systems must continue to operate for some time after an accident;
- the inability to take into account (provide allowance for) the great variation in frequency of various failure scenarios;
- the problem of common-cause events such as earthquakes.

In the mid 1970s the CANDU designers proposed using a safety design matrix (SDM) concept to deal with matters of inter-dependency through the support systems and long-term actions including operator intervention. The SDM approach, which uses fault-tree and event-sequence analyses of specific systems, has contributed significantly to a better understanding of system behaviour and interaction.

The designers also developed a "two-group" approach to system layout to minimize the dangers from common cause events, wherein key plant functions and the special safety systems are divided into two groups that are kept physically quite separate from each other.[6]

In a desire to extend and improve the safety approach various groups, since the late 1970s, have reviewed the situation and proposed a further evolution of reactor safety requirements. With the development of probabilistic analyses these groups have proposed using such techniques while still retaining the concept of independent special safety systems as a practicable means of achieving the objective.

Reflecting this movement, the AECB issued in 1980, a "consultative document", C-6, "Requirements for the Safety Analysis of CANDU Nuclear Power Plants", which created six categories of accident sequences and assigned reference dose limits to each. However, no frequency was stated for the various categories making it difficult to assign a limit to an unlisted accident sequence. The AECB required that C-6 be applied, on a "trial" basis, in the licensing of the Darlington generating station. In the Darlington "trial", however, the Ontario Hydro analysts proposed frequencies for the categories which were accepted by the AECB. (Darlington also had to meet the single/dual failure criteria.)

Darlington was also the subject of an extensive probabilistic analysis, the Darlington Probabilistic Safety Evaluation (DPSE), which was proposed and conducted by the utility. Although the DPSE was submitted to the AECB, the regulatory agency did not consider it as a "licensing document" and, therefore, did not review it closely.

In 1983 the AECB's Advisory Committee on Nuclear Safety produced their report, ACNS-4, "Recommended General Safety Requirements for Nuclear Power Plants", which continued the requirements for the special safety systems but proposed a set of accident sequence categories with frequency and consequence (dose) ranges. Although this was developed with considerable consultation with both industry and AECB staff it has not been adopted by the AECB.

## Current Situation

AECB staff have been working on a revision of C-6 for some time which they expect to issue for comments in early 1994. The ACNS is working on a revision of ACNS-4.

Meanwhile, industry personnel complain that the AECB is demanding more and more "ad hoc" requirements which do not always appear consistent with one another. The old adage of the AECB staff of, "they propose, we dispose", has been pursued without any obvious overall or underlying philosophy. In fact, there are increasing trends of demanding "absolute" safety.

In the case of off-shore projects, the foreign nuclear regulatory agencies which have agreed to follow the Canadian approach are finding it difficult to do so, partly because of the difficulty of determining the underlying rationale for AECB decisions but largely because of the lack of documentation. Other than the regulatory documents R-7, R-8, R-9, spelling out the requirements (as broadly set out in the "Siting Guide") for containment, shutdown systems, and emergency core cooling systems, respectively, there are very few documented requirements. (See Table 2.)

A number of industry standards have been developed and issued by the Canadian Standards Association (Table 3) but these fall far short of the sets of standards in the USA, France or Germany.

Ironically, the United States Nuclear Regulatory Commission (USNRC), which has a large set of prescriptive regulations, is now seriously examining what it calls "risk-based"

| | | |
|---|---|---|
| R-7 | Requirements for Containment Systems for CANDU Nuclear Power Plants | 1991 |
| R-8 | Requirements for Shutdown Systems for CANDU Nuclear Power Plants | 1991 |
| R-9 | Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants | 1991 |
| R-10 | Use of Two Shutdown Systems in Reactors | 1977 |
| R-77 | Overpressure Protection Requirements for Primary Heat Transport Systems in CANDU Power Reactors | 1987 |
| R-90 | Policy on the Decommissioning of Nuclear Facilities | 1988 |

**Table 2: AECB Regulatory Documents Related to Power Reactors**

regulation for nuclear power plants. The USNRC has a major study underway on this topic with initial objectives being:

- to improve "technical specifications" (the key descriptive part of a nuclear power plant licence) through identification of the most risk significant equipment and procedures;
- to modify existing rules where the requirements are shown [by PRA techniques] not to be commensurate with the safety benefits;
- to develop rules for the future, using a performance based approach.

The USNRC work is being conducted with contributions from, and in cooperation with, many groups representing the industry.

While it is acknowledged that the transition to such a style of regulation will take many years it is intriguing to see that large respected organization pursuing an approach which Canada pioneered three decades ago.

| | |
|---|---|
| CAN3-N285.0,1,2,3,4,6 | Requirements for Pressure Retaining Systems and Components in CANDU Nuclear Power Plants |
| CAN3-N286.0 to N286.5 | Quality Assurance Requirements for Power Plants |
| CAN3-N287.1 to N287.7 | Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants |
| CAN3-N288.1 | Guidelines for Calculating Derives Release Limits for Radioactive Material in Airborne and Liquid Effluents from Normal Operation of Nuclear Facilities |
| CAN3-N289.3.2 | High Efficiency Air Cleaning Assemblies for Normal Operation of Nuclear Facilities |
| CAN3-N289.1 to N289.4 | Requirements for Seismic Qualifications for CANDU Nuclear Power Plants |
| CAN3-N290.1 | Requirements for the Shutdown Systems of CANDU Nuclear Power Plants |
| CAN3-N290.4 | Requirements for the Reactaor Regulating Systems for CANDU Nuclear Power Plants |
| CAN3-N290.6 | Requirements for Monitoring and Display of CANDU Nuclear Power Plant Status in the Event of an Accident |
| CAN/CSA-N293 | Fire Protection for CANDU Nuclear Power Plants |

**Table 3: Canadian / CSA Standards**

## Concluding Observations

As indicated by the USNRC initiative towards "risk-based" regulation, the concept of risk or probabilistic safety goals is gaining wider acceptance throughout the world nuclear community. Canada adopted such a philosophy almost 30 years ago. Given the absence of practical, credible, verifiable probabilistic evaluation techniques at that time the approach of separate, independent, testable safety systems was developed and augmented by risk based criteria.

Unfortunately, the approach was not pursued with sufficient vigour in the evolving CANDU designs nor enforced by the regulator. One consequence is many potential cross-links, especially through the support systems, between the supposedly independent safety systems. The SDM analytical technique and the Two Group design layout only partially compensate for this basic deficiency.

In recent years the regulator has concentrated more and more on details while, apparently, ignoring the basic objective. If the original risk goal is to be abandoned and its attendant criteria and requirements are to be dropped, there must be a logical, comprehensive, approach to replace them. All in the nuclear power industry should be involved, not just the regulator.

## References


1. Lewis, W.B., "The Accident to the NRX Reactor on December 12, 1952." AECL - 232 1953.
2. Hurst, D.G., "The Accident to the NRX Reactor, Part II." AECL - 233 1953.
3. Siddall, E., "Reactor Safety Standards and Their Attainment." AECL - 498 1957.
4. Laurence, G.C., "Required Safety in Nuclear Reactors." AECL - 1923 1961.
5. Hurst, D.G. and Boyd, F.C. "Reactor Safety and Licensing Requirements." AECB - 1045 1972.
6. Snell, V.G., Safety of CANDU Nuclear Power Stations. AECL - 6329 1985.



Reprinted from
CNS Bulletin, Vol. 14, No. 4
Winter 1993/94

INTERNATIONAL ATOMIC ENERGY AGENCY
WAGRAMERSTRASSE 5, P.O. BOX 100, A-1400 VIENNA, AUSTRIA
TELEPHONE: 43 1 2060 21270/21275, TELEX: 1-12645,
CABLE: INATOM VIENNA, TELEFAX: 43 1 2060 29610

**24 October 1996**
**PR 96/22**
**FOR IMMEDIATE RELEASE**

PRESS RELEASE FOR USE OF INFORMATION MEDIA - NOT AN OFFICIAL RECORD

## NUCLEAR SAFETY CONVENTION ENTERS INTO FORCE

**The Convention on Nuclear Safety -- the first international legal instrument on the safety of nuclear power plants worldwide -- enters into force today, 24 October 1996. The Convention commits States Parties to ensure the safety of land-based civil nuclear power plants. This includes a legislative and regulatory framework; general safety considerations such as quality assurance, assessment, and verification of safety; human factors; radiation protection; emergency preparedness; and specific obligations on the safety of nuclear installations; siting; design and construction; and operation. Among its requirements, the Convention obliges Parties to submit reports at periodic review meetings. These reports will focus on the measures each State has taken to implement obligations under the Convention.**

**"The Convention marks a major step forward in strengthening international co-operation in the safety field," said IAEA Director General Hans Blix. "Though the safe use of nuclear energy remains clearly a national responsibility, the Convention signals the growing recognition of the global interdependence of safe nuclear development.We now look forward to finishing work on other legal instruments, notably in the field of radioactive waste management, also being negotiated through the efforts of the Agency and its Member States."**

**Twenty-seven States so far have consented to be bound by the Convention on Nuclear Safety. These are Bangladesh, Bulgaria, Canada, China, Croatia, the Czech Republic, Finland, France, Hungary, Ireland, Japan, the Republic of Korea, Lebanon, Lithuania, Mali, Mexico, the Netherlands, Norway, Poland, Romania, the Russian Federation, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, and the United Kingdom. The Convention has been signed by 65 States.**

**Under terms of the Convention, a preparatory meeting of States Parties will be convened within the next six months. At that meeting, among other matters, guidelines will be established regarding the form and structure of reports that States are required to submit for review at periodic meetings, and the process for reviewing such reports. The Convention calls for the first review meeting to be convened as soon as possible, but no later than 30 months from today's entry into force.**

***Editor's Note: The full text of the Convention on Nuclear Safety and its latest status is accessible through the IAEA's World Atom Internet services on the World Wide Web at http:\\www.iaea.org\worldatom***

International Atomic Energy Agency
INFORMATION CIRCULAR

INFCIRC/449
5 July 1994

GENERAL Distr.
Original: ARABIC, CHINESE, ENGLISH, FRENCH, RUSSIAN, SPANISH



# CONVENTION ON NUCLEAR SAFETY

1. The Convention on Nuclear Safety was adopted on 17 June 1994 by a Diplomatic Conference convened by the International Atomic Energy Agency at its Headquarters from 14 to 17 June 1994. The Convention will be opened for signature on 20 September 1994 during the thirty-eighth regular session of the Agency's General Conference and will enter into force on the ninetieth day after the date of deposit with the Depositary (the Agency's Director General) of the twenty-second instrument of ratification, acceptance or approval, including the instruments of seventeen States, having each at least one nuclear installation which has achieved criticality in a reactor core.

2. The text of the Convention as adopted is reproduced in the Annex hereto for the information of all Member States.

# CONVENTION ON NUCLEAR SAFETY

## PREAMBLE

THE CONTRACTING PARTIES

(i) Aware of the importance to the international community of ensuring that the use of nuclear energy is safe, well regulated and environmentally sound;

(ii) Reaffirming the necessity of continuing to promote a high level of nuclear safety worldwide;

(iii) Reaffirming that responsibility for nuclear safety rests with the State having jurisdiction over a nuclear installation;

(iv) Desiring to promote an effective nuclear safety culture;

(v) Aware that accidents at nuclear installations have the potential for transboundary impacts;

(vi) Keeping in mind the Convention on the Physical Protection of Nuclear Material (1979), the Convention on Early Notification of a Nuclear Accident (1986), and the Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency (1986);

(vii) Affirming the importance of international co-operation for the enhancement of nuclear safety through existing bilateral and multilateral mechanisms and the establishment of this incentive Convention;

(viii) Recognizing that this Convention entails a commitment to the application of fundamental safety principles for nuclear installations rather than of detailed safety standards and that there are internationally formulated safety guidelines which are updated from time to time and so can provide guidance on contemporary means of achieving a high level of safety;

(ix) Affirming the need to begin promptly the development of an international convention on the safety of radioactive waste management as soon as the ongoing process to develop waste management safety fundamentals has resulted in broad international agreement;

(x) Recognizing the usefulness of further technical work in connection with the safety of other parts of the nuclear fuel cycle, and that this work may, in time, facilitate the development of current or future international instruments;

HAVE AGREED as follows:

# CHAPTER 1. OBJECTIVES, DEFINITIONS AND SCOPE OF APPLICATION

## ARTICLE 1. OBJECTIVES

The objectives of this Convention are:

(i) to achieve and maintain a high level of nuclear safety worldwide through the enhancement of national measures and international co-operation including, where appropriate, safety-related technical co-operation;

(ii) to establish and maintain effective defences in nuclear installations against potential radiological hazards in order to protect individuals, society and the environment from harmful effects of ionizing radiation from such installations;

(iii) to prevent accidents with radiological consequences and to mitigate such consequences should they occur.

## ARTICLE 2. DEFINITIONS

For the purpose of this Convention:

(i) "nuclear installation" means for each Contracting Party any land-based civil nuclear power plant under its jurisdiction including such storage, handling and treatment facilities for radioactive materials as are on the same site and are directly related to the operation of the nuclear power plant. Such a plant ceases to be a nuclear installation when all nuclear fuel elements have been removed permanently from the reactor core and have been stored safely in accordance with approved procedures, and a decommissioning programme has been agreed to by the regulatory body.

(ii) "regulatory body" means for each Contracting Party any body or bodies given the legal authority by that Contracting Party to grant licences and to regulate the siting, design, construction, commissioning, operation or decommissioning of nuclear installations.

(iii) "licence" means any authorization granted by the regulatory body to the applicant to have the responsibility for the siting, design, construction, commissioning, operation or decommissioning of a nuclear installation.

## ARTICLE 3. SCOPE OF APPLICATION

This Convention shall apply to the safety of nuclear installations.

## CHAPTER 2. OBLIGATIONS

*(a) General Provisions*

### ARTICLE 4. IMPLEMENTING MEASURES

Each Contracting Party shall take, within the framework of its national law, the legislative, regulatory and administrative measures and other steps necessary for implementing its obligations under this Convention.

### ARTICLE 5. REPORTING

Each Contracting Party shall submit for review, prior to each meeting referred to in Article 20, a report on the measures it has taken to implement each of the obligations of this Convention.

### ARTICLE 6. EXISTING NUCLEAR INSTALLATIONS

Each Contracting Party shall take the appropriate steps to ensure that the safety of nuclear installations existing at the time the Convention enters into force for that Contracting Party is reviewed as soon as possible. When necessary in the context of this Convention, the Contracting Party shall ensure that all reasonably practicable improvements are made as a matter of urgency to upgrade the safety of the nuclear installation. If such upgrading cannot be achieved, plans should be implemented to shut down the nuclear installation as soon as practically possible. The timing of the shut-down may take into account the whole energy context and possible alternatives as well as the social, environmental and economic impact.

*(b) Legislation and regulation*

### ARTICLE 7. LEGISLATIVE AND REGULATORY FRAMEWORK

1. Each Contracting Party shall establish and maintain a legislative and regulatory framework to govern the safety of nuclear installations.

2. The legislative and regulatory framework shall provide for:

(i) the establishment of applicable national safety requirements and regulations;

(ii) a system of licensing with regard to nuclear installations and the prohibition of the operation of a nuclear installation without a licence;

(iii) a system of regulatory inspection and assessment of nuclear installations to ascertain compliance with applicable regulations and the terms of licences;

(iv) the enforcement of applicable regulations and of the terms of licences, including suspension, modification or revocation.

## ARTICLE 8. REGULATORY BODY

1. Each Contracting Party shall establish or designate a regulatory body entrusted with the implementation of the legislative and regulatory framework referred to in Article 7, and provided with adequate authority, competence and financial and human resources to fulfil its assigned responsibilities.

2. Each Contracting Party shall take the appropriate steps to ensure an effective separation between the functions of the regulatory body and those of any other body or organization concerned with the promotion or utilization of nuclear energy.

## ARTICLE 9. RESPONSIBILITY OF THE LICENCE HOLDER

Each Contracting Party shall ensure that prime responsibility for the safety of a nuclear installation rests with the holder of the relevant licence and shall take the appropriate steps to ensure that each such licence holder meets its responsibility.

### *(c) General Safety Considerations*

## ARTICLE 10. PRIORITY TO SAFETY

Each Contracting Party shall take the appropriate steps to ensure that all organizations engaged in activities directly related to nuclear installations shall establish policies that give due priority to nuclear safety.

## ARTICLE 11. FINANCIAL AND HUMAN RESOURCES

1. Each Contracting Party shall take the appropriate steps to ensure that adequate financial resources are available to support the safety of each nuclear installation throughout its life.

2. Each Contracting Party shall take the appropriate steps to ensure that sufficient numbers of qualified staff with appropriate education, training and retraining are available for all safety-related activities in or for each nuclear installation, throughout its life.

## ARTICLE 12. HUMAN FACTORS

Each Contracting Party shall take the appropriate steps to ensure that the capabilities and limitations of human performance are taken into account throughout the life of a nuclear installation.

## ARTICLE 13. QUALITY ASSURANCE

Each Contracting Party shall take the appropriate steps to ensure that quality assurance programmes are established and implemented with a view to providing confidence that specified requirements for all activities important to nuclear safety are satisfied throughout the life of a nuclear installation.

## ARTICLE 14. ASSESSMENT AND VERIFICATION OF SAFETY

Each Contracting Party shall take the appropriate steps to ensure that:

(i) comprehensive and systematic safety assessments are carried out before the construction and commissioning of a nuclear installation and throughout its life. Such assessments shall be well documented, subsequently updated in the light of operating experience and significant new safety information, and reviewed under the authority of the regulatory body;

(ii) verification by analysis, surveillance, testing and inspection is carried out to ensure that the physical state and the operation of a nuclear installation continue to be in accordance with its design, applicable national safety requirements, and operational limits and conditions.

## ARTICLE 15. RADIATION PROTECTION

Each Contracting Party shall take the appropriate steps to ensure that in all operational states the radiation exposure to the workers and the public caused by a nuclear installation shall be kept as low as reasonably achievable and that no individual shall be exposed to radiation doses which exceed prescribed national dose limits.

## ARTICLE 16. EMERGENCY PREPAREDNESS

1. Each Contracting Party shall take the appropriate steps to ensure that there are on-site and off-site emergency plans that are routinely tested for nuclear installations and cover the activities to be carried out in the event of an emergency.

For any new nuclear installation, such plans shall be prepared and tested before it commences operation above a low power level agreed by the regulatory body.

2. Each Contracting Party shall take the appropriate steps to ensure that, insofar as they are likely to be affected by a radiological emergency, its own population and the competent authorities of the States in the vicinity of the nuclear installation are provided with appropriate information for emergency planning and response.

3. Contracting Parties which do not have a nuclear installation on their territory, insofar as they are likely to be affected in the event of a radiological emergency at a nuclear installation in the vicinity, shall take the appropriate steps for the preparation and testing of emergency plans for their territory that cover the activities to be carried out in the event of such an emergency.

### *(d) Safety of Installations*

### ARTICLE 17. SITING

Each Contracting Party shall take the appropriate steps to ensure that appropriate procedures are established and implemented:

(i) for evaluating all relevant site-related factors likely to affect the safety of a nuclear installation for its projected lifetime;

(ii) for evaluating the likely safety impact of a proposed nuclear installation on individuals, society and the environment;

(iii) for re-evaluating as necessary all relevant factors referred to in sub-paragraphs (i) and (ii) so as to ensure the continued safety acceptability of the nuclear installation;

(iv) for consulting Contracting Parties in the vicinity of a proposed nuclear installation, insofar as they are likely to be affected by that installation and, upon request providing the necessary information to such Contracting Parties, in order to enable them to evaluate and make their own assessment of the likely safety impact on their own territory of the nuclear installation.

### ARTICLE 18. DESIGN AND CONSTRUCTION

Each Contracting Party shall take the appropriate steps to ensure that:

(i) the design and construction of a nuclear installation provides for several reliable levels and methods of protection (defense in depth) against the release of

radioactive materials, with a view to preventing the occurrence of accidents and to mitigating their radiological consequences should they occur;

(ii) the technologies incorporated in the design and construction of a nuclear installation are proven by experience or qualified by testing or analysis;

(iii) the design of a nuclear installation allows for reliable, stable and easily manageable operation, with specific consideration of human factors and the man-machine interface.

## ARTICLE 19. OPERATION

Each Contracting Party shall take the appropriate steps to ensure that:

(i) the initial authorization to operate a nuclear installation is based upon an appropriate safety analysis and a commissioning programme demonstrating that the installation, as constructed, is consistent with design and safety requirements;

(ii) operational limits and conditions derived from the safety analysis, tests and operational experience are defined and revised as necessary for identifying safe boundaries for operation;

(iii) operation, maintenance, inspection and testing of a nuclear installation are conducted in accordance with approved procedures;

(iv) procedures are established for responding to anticipated operational occurrences and to accidents;

(v) necessary engineering and technical support in all safety-related fields is available throughout the lifetime of a nuclear installation;

(vi) incidents significant to safety are reported in a timely manner by the holder of the relevant licence to the regulatory body;

(vii) programmes to collect and analyse operating experience are established, the results obtained and the conclusions drawn are acted upon and that existing mechanisms are used to share important experience with international bodies and with other operating organizations and regulatory bodies;

(viii) the generation of radioactive waste resulting from the operation of a nuclear installation is kept to the minimum practicable for the process concerned, both in activity and in volume, and any necessary treatment and storage of spent fuel and waste directly related to the operation and on the same site as that of the nuclear installation take into consideration conditioning and disposal.

# CHAPTER 3. MEETINGS OF THE CONTRACTING PARTIES

## ARTICLE 20. REVIEW MEETINGS

1. The Contracting Parties shall hold meetings (hereinafter referred to as "review meetings") for the purpose of reviewing the reports submitted pursuant to Article 5 in accordance with the procedures adopted under Article 22.

2. Subject to the provisions of Article 24 sub-groups comprised of representatives of Contracting Parties may be established and may function during the review meetings as deemed necessary for the purpose of reviewing specific subjects contained in the reports.

3. Each Contracting Party shall have a reasonable opportunity to discuss the reports submitted by other Contracting Parties and to seek clarification of such reports.

## ARTICLE 21. TIMETABLE

1. A preparatory meeting of the Contracting Parties shall be held not later than six months after the date of entry into force of this Convention.

2. At this preparatory meeting, the Contracting Parties shall determine the date for the first review meeting. This review meeting shall be held as soon as possible, but not later than thirty months after the date of entry into force of this Convention.

3. At each review meeting, the Contracting Parties shall determine the date for the next such meeting. The interval between review meetings shall not exceed three years.

## ARTICLE 22. PROCEDURAL ARRANGEMENTS

1. At the preparatory meeting held pursuant to Article 21 the Contracting Parties shall prepare and adopt by consensus Rules of Procedure and Financial Rules. The Contracting Parties shall establish in particular and in accordance with the Rules of Procedure:

(i) guidelines regarding the form and structure of the reports to be submitted pursuant to Article 5;

(ii) a date for the submission of such reports;

(iii) the process for reviewing such reports.

2. At review meetings the Contracting Parties may, if necessary, review the arrangements established pursuant to sub-paragraphs (i)-(iii) above, and adopt revisions by consensus unless otherwise provided for in the Rules of Procedure. They may also amend the Rules of Procedure and the Financial Rules, by consensus.

## ARTICLE 23. EXTRAORDINARY MEETINGS

An extraordinary meeting of the Contracting Parties shall be held:

(i) if so agreed by a majority of the Contracting Parties present and voting at a meeting, abstentions being considered as voting; or

(ii) at the written request of a Contracting Party, within six months of this request having been communicated to the Contracting Parties and notification having been received by the secretariat referred to in Article 28, that the request has been supported by a majority of the Contracting Parties.

## ARTICLE 24. ATTENDANCE

1. Each Contracting Party shall attend meetings of the Contracting Parties and be represented at such meetings by one delegate, and by such alternates, experts and advisers as it deems necessary.

2. The Contracting Parties may invite, by consensus, any intergovernmental organization which is competent in respect of matters governed by this Convention to attend, as an observer, any meeting, or specific sessions thereof. Observers shall be required to accept in writing, and in advance, the provisions of Article 27.

## ARTICLE 25. SUMMARY REPORTS

The Contracting Parties shall adopt, by consensus, and make available to the public a document addressing issues discussed and conclusions reached during a meeting.

## ARTICLE 26. LANGUAGES

1. The languages of meetings of the Contracting Parties shall be Arabic, Chinese, English, French, Russian and Spanish unless otherwise provided in the Rules of Procedure.

2. Reports submitted pursuant to Article 5 shall be prepared in the national language of the submitting Contracting Party or in a single designated language to be agreed in the Rules of Procedure. Should the report be submitted in a national language other than the designated

language, a translation of the report into the designated language shall be provided by the Contracting Party.

3. Notwithstanding the provisions of paragraph 2, if compensated, the secretariat will assume the translation into the designated language of reports submitted in any other language of the meeting.

## ARTICLE 27. CONFIDENTIALITY

1. The provisions of this Convention shall not affect the rights and obligations of the Contracting Parties under their law to protect information from disclosure. For the purposes of this Article, "information" includes, inter alia, (i) personal data; (ii) information protected by intellectual property rights or by industrial or commercial confidentiality; and (iii) information relating to national security or to the physical protection of nuclear materials or nuclear installations.

2. When, in the context of this Convention, a Contracting Party provides information identified by it as protected as described in paragraph 1, such information shall be used only for the purposes for which it has been provided and its confidentiality shall be respected.

3. The content of the debates during the reviewing of the reports by the Contracting Parties at each meeting shall be confidential.

## ARTICLE 28. SECRETARIAT

1. The International Atomic Energy Agency, (hereinafter referred to as the "Agency") shall provide the secretariat for the meetings of the Contracting Parties.

2. The secretariat shall:

(i) convene, prepare and service the meetings of the Contracting Parties;

(ii) transmit to the Contracting Parties information received or prepared in accordance with the provisions of this Convention.

The costs incurred by the Agency in carrying out the functions referred to in sub-paragraphs i) and (ii) above shall be borne by the Agency as part of its regular budget.

3. The Contracting Parties may, by consensus, request the Agency to provide other services in support of meetings of the Contracting Parties. The Agency may provide such services if they can be undertaken within its programme and regular budget. Should this not be possible, the Agency may provide such services if voluntary funding is provided from another source.

# CHAPTER 4. FINAL CLAUSES AND OTHER PROVISIONS

## ARTICLE 29. RESOLUTION OF DISAGREEMENTS

In the event of a disagreement between two or more Contracting Parties concerning the interpretation or application of this Convention, the Contracting Parties shall consult within the framework of a meeting of the Contracting Parties with a view to resolving the disagreement.

## ARTICLE 30. SIGNATURE, RATIFICATION, ACCEPTANCE, APPROVAL, ACCESSION

1. This Convention shall be open for signature by all States at the Headquarters of the Agency in Vienna from 20 September 1994 until its entry into force.

2. This Convention is subject to ratification, acceptance or approval by the signatory States.

3. After its entry into force, this Convention shall be open for accession by all States.

4. (i) This Convention shall be open for signature or accession by regional organizations of an integration or other nature, provided that any such organization is constituted by sovereign States and has competence in respect of the negotiation, conclusion and application of international agreements in matters covered by this Convention.

(ii) In matters within their competence, such organizations shall, on their own behalf, exercise the rights and fulfil the responsibilities which this Convention attributes to States Parties.

(iii) When becoming party to this Convention, such an organization shall communicate to the Depositary referred to in Article 34, a declaration indicating which States are members thereof, which articles of this Convention apply to it, and the extent of its competence in the field covered by those articles.

(iv) Such an organization shall not hold any vote additional to those of its Member States.

5. Instruments of ratification, acceptance, approval or accession shall be deposited with the Depositary.

## ARTICLE 31. ENTRY INTO FORCE

1. This Convention shall enter into force on the ninetieth day after the date of deposit with the Depositary of the twenty-second instrument of ratification, acceptance or approval, including the instruments of seventeen States, each having at least one nuclear installation which has achieved criticality in a reactor core.

2. For each State or regional organization of an integration or other nature which ratifies, accepts, approves or accedes to this Convention after the date of deposit of the last instrument required to satisfy the conditions set forth in paragraph 1, this Convention shall enter into force on the ninetieth day after the date of deposit with the Depositary of the appropriate instrument by such a State or organization.

## ARTICLE 32. AMENDMENTS TO THE CONVENTION

1. Any Contracting Party may propose an amendment to this Convention. Proposed amendments shall be considered at a review meeting or an extraordinary meeting.

2. The text of any proposed amendment and the reasons for it shall be provided to the Depositary who shall communicate the proposal to the Contracting Parties promptly and at least ninety days before the meeting for which it is submitted for consideration. Any comments received on such a proposal shall be circulated by the Depositary to the Contracting Parties.

3. The Contracting Parties shall decide after consideration of the proposed amendment whether to adopt it by consensus, or, in the absence of consensus, to submit it to a Diplomatic Conference. A decision to submit a proposed amendment to a Diplomatic Conference shall require a two-thirds majority vote of the Contracting Parties present and voting at the meeting, provided that at least one half of the Contracting Parties are present at the time of voting. Abstentions shall be considered as voting.

4. The Diplomatic Conference to consider and adopt amendments to this Convention shall be convened by the Depositary and held no later than one year after the appropriate decision taken in accordance with paragraph 3 of this Article. The Diplomatic Conference shall make every effort to ensure amendments are adopted by consensus. Should this not be possible, amendments shall be adopted with a two-thirds majority of all Contracting Parties.

5. Amendments to this Convention adopted pursuant to paragraphs 3 and 4 above shall be subject to ratification, acceptance, approval, or confirmation by the Contracting Parties and shall enter into force for those Contracting Parties which have ratified, accepted, approved or confirmed them on the ninetieth day after the receipt by the Depositary of the relevant instruments by at least three fourths of the Contracting Parties. For a Contracting Party which subsequently ratifies, accepts, approves or confirms the said amendments, the amendments will enter into force on the ninetieth day after that Contracting Party has deposited its relevant instrument.

## ARTICLE 33. DENUNCIATION

1. Any Contracting Party may denounce this Convention by written notification to the Depositary.

2. Denunciation shall take effect one year following the date of the receipt of the notification by the Depositary, or on such later date as may be specified in the notification.

## ARTICLE 34. DEPOSITARY

1. The Director General of the Agency shall be the Depositary of this Convention.

2. The Depositary shall inform the Contracting Parties of:

(i) the signature of this Convention and of the deposit of instruments of ratification, acceptance, approval or accession, in accordance with Article 30;

(ii) the date on which the Convention enters into force, in accordance with Article 31;

(iii) the notifications of denunciation of the Convention and the date thereof, made in accordance with Article 33;

(iv) the proposed amendments to this Convention submitted by Contracting Parties, the amendments adopted by the relevant Diplomatic Conference or by the meeting of the Contracting Parties, and the date of entry into force of the said amendments, in accordance with Article 32.

## ARTICLE 35. AUTHENTIC TEXTS

The original of this Convention of which the Arabic, Chinese, English, French, Russian and Spanish texts are equally authentic, shall be deposited with the Depositary, who shall send certified copies thereof to the Contracting Parties.

# ANNEX TO THE FINAL ACT OF THE DIPLOMATIC CONFERENCE SOME CLARIFICATION WITH RESPECT TO PROCEDURAL AND FINANCIAL ARRANGEMENTS, NATIONAL REPORTS AND THE CONDUCT OF REVIEW MEETINGS, ENVISAGED IN THE CONVENTION ON NUCLEAR SAFETY

## 1. Introduction

1.1 This document contains some clarification with respect to procedural and financial arrangements, national reports and the conduct of review meetings. It is understood that this document is not exhaustive and does not bind the Contracting Parties to the Convention on Nuclear Safety.

1.2 The basic principle underlying this clarification is that all provisions in the Rules of Procedure and the Financial Rules should be in strict conformity with the provisions of the Convention.

1.3 Nothing in the implementation of the Convention should dilute the national responsibility for nuclear safety.

## 2. National reports

In accordance with Article 5 of the Convention, national reports should, as applicable, address each obligation separately. The reports should demonstrate how each obligation has been met, with specific references to - inter alia - legislation, procedures and design criteria. When a report states that a particular obligation has not been met, that report should also state what measures are being taken or planned to meet that obligation.

## 3. Conduct of review meetings

the purpose of review meetings referred to in Article 20 of the Convention is the review by experts of national reports. The review process should:

* include in-depth study of all national reports, to be conducted by each party before the meeting, as it deems appropriate;

* be carried out through discussion among experts at the meeting;

* take into consideration the technical characteristics of different types of nuclear installation and the likely radiological impact of potential accidents;

* identify problems, concerns, uncertainties, or omissions in national reports, focusing on the most significant problems or concerns in order to ensure efficient and fruitful debate at the meetings; and

* identify technical information and opportunities for technical cooperation in the interest of resolving safety problems identified.

4. Rules of Procedure for the meeting of the Parties

4.1 Equitable representation: Paramount importance should be given to technical competence in the election of chairmen and officers. Consideration should also be given to the overall membership of the Convention, including the geographical distribution of the Contracting Parties.

4.2 Decision-making: Every effort should be made to take decisions by consensus.

4.3 Confidentiality: The Rules of Procedure should be formulated so as to ensure that the provisions of Article 27 are applied to all participants.

5. Financial rules

5.1 Costs to the secretariat: All costs to the secretariat, referred to in Article 28 of the Convention, should be kept to a minimum. The Agency should be requested to provide other services in support of the meeting of the Contracting Parties, only if such services are deemed essential.

5.2 · Costs to the Contracting Parties: In order to encourage the widest possible adherence to the Convention, the costs of preparing for and participating in review meetings should, while maintaining the effectiveness of the review, be limited by - inter alia - the following means:

* limiting the frequency of review meetings; and

* limiting the duration of the preparatory meeting and of review meetings.