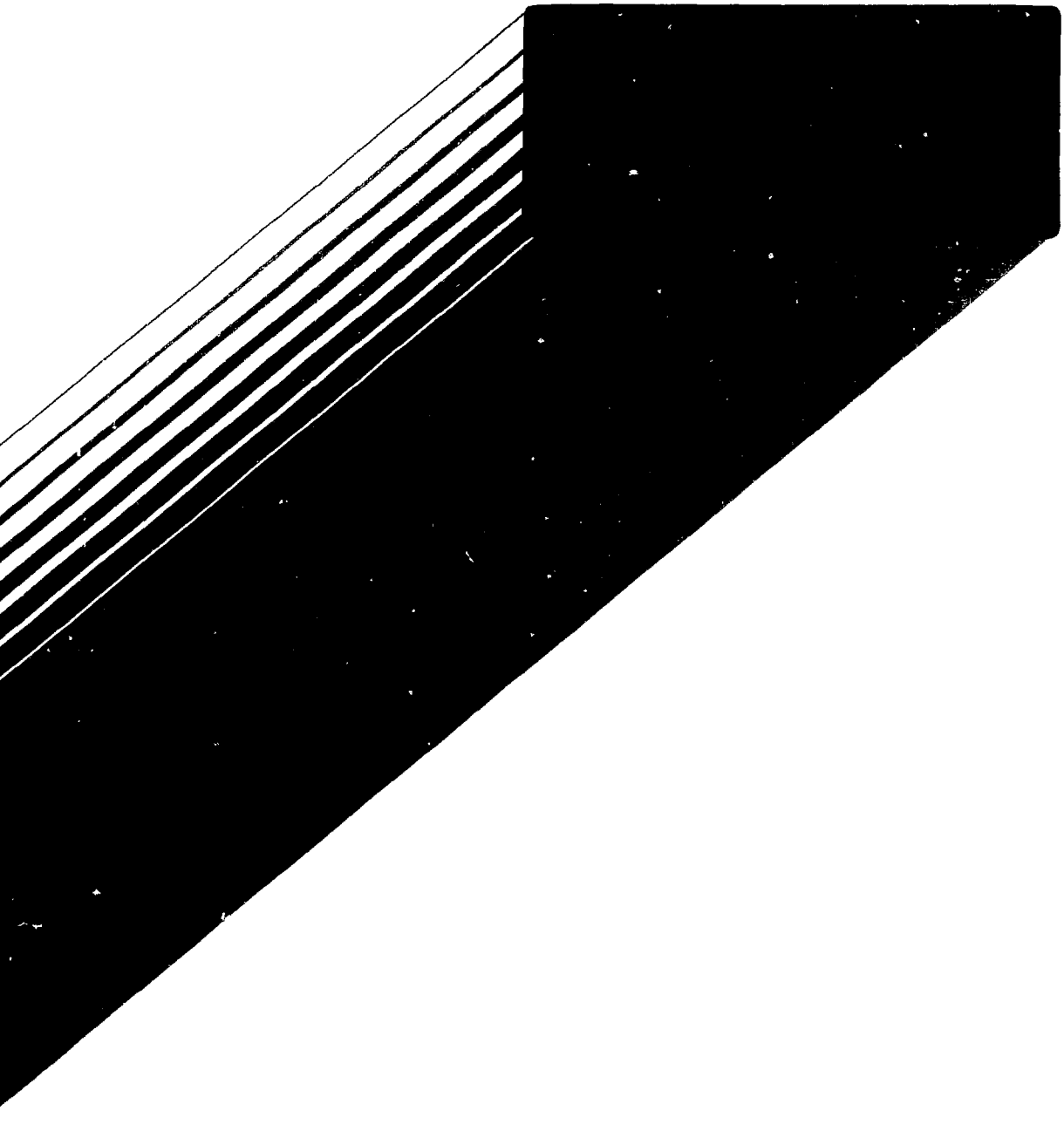
Publication

INFO 0104

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

CA8507857



Atomic Energy Control Board
P.O. Box 1046
Ottawa, Canada
K1P 5S9

Commission de contrôle de l'énergie atomique
C.P. 1046
Ottawa, Canada
K1P 5S9

INFO-0104

THE CANADIAN APPROACH TO NUCLEAR POWER SAFETY

by

R.J. Atchison, F.C. Boyd and
Z. Domaratzki

Atomic Energy Control Board
Ottawa, Canada

Article published in the
July-August 1983 issue of
"Nuclear Safety"

PAPER

July 1983

RÉSUMÉ

On peut retracer les principes et les pratiques de sûreté nucléaire au Canada depuis leurs origines au Centre d'études nucléaires de Chalk River jusqu'à la délivrance de permis des réacteurs actuels. Comme un des principes de base stipule que la responsabilité première d'atteindre un haut niveau de sûreté incombe au titulaire de permis, les exigences réglementaires ont insisté davantage sur certains buts et objectifs numériques et minimisé les caractéristiques de conception ou les règles d'exploitation. Le rapport décrit le processus canadien de délivrance de permis, rend compte de certaines difficultés auxquelles il doit faire face et fournit notamment des exemples de considérations particulières à la délivrance de permis de chaque étape d'un projet.

The Canadian Approach to Nuclear Power Safety

by R.J. Atchison[+], F.C. Boyd[*] and Z. Domaratzki[#]

ABSTRACT

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

BIOGRAPHICAL SKETCHES

+ Robert J. Atchison received the B.A.Sc. degree in engineering physics from the University of Toronto in 1953. Following reactor physics and operating experience with the NRX experimental reactor at the Chalk River Nuclear Laboratories, he joined the design team working on the Douglas Point prototype power station in 1958, carrying out reactor physics studies and accident analyses. In 1965, he joined Hydro-Quebec to work on the Gentilly-1 boiling light water (BLW) station in various technical capacities. In 1970, he joined Ontario Hydro as a Supervising Design Engineer in the Nuclear Concepts Department to carry out technical assessments of various nuclear plant designs and to assist with licensing documentation for the Pickering and Bruce plants then under construction. In 1974, he joined the Atomic Energy Control Board (AECB) and is currently Director of the Assessment Branch.

* Fred C. Boyd received the B.A.Sc degree in engineering physics from the university of Toronto in 1949. He was part of the original design team for the NPD demonstration plant, subsequently joining the AECB in 1959 and becoming Head of the Facilities Licensing Group. In 1972, he joined the Energy Policy Sector of the Ministry of Energy, Mines and Resources. After serving a year as an IAEA adviser in Korea, he rejoined the AECB in 1978. He is currently Science Advisor, and Director of the Orientation Centre which provides advice to foreign regulatory agencies. As Science Advisor, he is responsible for the support and operation of the Board's advisory committees.

Zigmund Domaratzki graduated from the University of Manitoba in 1959 with a degree in mechanical engineering. He spent the next 10 years at the Chalk River Nuclear Laboratories engaged chiefly in R & D work on fuel for CANDU reactors. In 1969, he joined the Atomic Energy Control Board as one of its two resident project officers at the Pickering Generating Station where his responsibilities included review of safety evaluation and commissioning work, and subsequently, operational compliance monitoring. He is currently the Director General of the Directorate of Reactor Regulation and has responsibility for all regulatory functions dealing with power and research reactors.

INTRODUCTION

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 while the regulatory authority (the Atomic Energy Control Board) 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.

The conclusion is one of confidence that the approach to achieving safety of nuclear power plants which has been followed over the years in Canada is both flexible and effective. This approach could be adopted by any country wishing to develop indigenous regulatory rules which could be applicable to more than one design of nuclear power plant.

BACKGROUND

The philosophy of nuclear safety in Canada reflects the political structure of the country, the history and organization of the nuclear industry, and the evolution of a distinctive, indigenous nuclear power plant design (CANDU). The following sections outline briefly this important context.

Historical

Canada is a confederation, with ten provinces and two territories administered by the central or federal government. The Canadian constitution is expressed in the Constitution Acts 1867 to 1982.

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

Canada entered the nuclear field during World War II when the Montreal Laboratory was established to pursue the heavy water reactor route to plutonium production. At the end of the war, the government decided to continue, for peaceful purposes, the research and development which was underway.

In 1946, the Parliament of Canada passed the Atomic Energy Control Act[1], declaring atomic energy a matter of national interest and creating the Atomic Energy Control Board (AECB) to administer the Act. The

Act, which was subsequently amended in 1954, is a short document authorizing and defining the powers of the AECB, a body with five members, one of whom is appointed President and chief executive officer. Under the provisions of the Act, the Board is empowered to make regulations governing all aspects of the development and application of atomic energy.

The 1954 amendment to the Act transferred the responsibility for research and the exploitation of atomic energy from the Board to a Minister designated by the government. As a result of this transfer of responsibility, Atomic Energy of Canada Limited (a crown 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 which gives extensive discretionary power to the AECB. The Board 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 with respect to 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, e.g. if the claims are likely to exceed $75 million.

Structure of the Industry

When Atomic Energy of Canada Limited (AECL) was formed in 1952 it took over the operation of the Chalk River Nuclear Laboratories which had been set up in 1944/45 as an outgrowth of the wartime program of the Montreal Laboratory. 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

---

* A government-owned company

functions.

Ontario Hydro, the electrical utility owned by the Province of Ontario (and the largest in the country), became interested in nuclear power in the early 1950's 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 which started up in 1962. Today Ontario Hydro is its own architect-engineer for all but the nuclear reactor and also acts as its own prime contractor.

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-management functions in the balance-of-plant systems. AECL has provided conceptual design and safety assessment for the overall plant, and engineering and procurement services for the nuclear steam supply system (NSSS).

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 which, in effect, decide whether or not nuclear-electric power generation should be part of the provincial energy program. Once 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 Atomic Energy Control Board have a supporting staff of 270 (as of April 1983). This staff is organized in the functional units of: the President's office, Secretariat, Reactor Regulation Directorate, Fuel Cycle and Materials Regulation Directorate, Regulatory Research Branch, and the Planning and Administration Branch. (See FIGURE 1). There are two

regional offices, primarily for compliance functions associated with radioiosotope 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 1960's 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 about mid-point 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, 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 Board 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] employs pressurized heavy water as the coolant, plus pressure-tubes and on-power fuelling. All nuclear power plants built or planned in Canada are of this CANDU-type design except for the Gentilly 1 BLW (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. The operator is therefore 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 which 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], 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.

The safety characteristics of the CANDU design have had, inevitably, an influence on the safety criteria developed by the AECB although 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 Board endorsed a statement[6] on the safety objectives for nuclear activities which had been developed by its Advisory Committee on Nuclear Safety to express the historical understanding. For hazards due to ionizing radiation the objectives are that:

(i) all early detrimental effects should be avoided and the risk of deferred effects should be minimized in accordance with the ALARA principle, and

(ii) 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 to the NRX research reactor at Chalk River in 1952 was the catalyst for much of the Canadian reactor safety approach which still prevails today. The essential principles which evolved were derived from the recognition that even well designed and built systems fail and, therefore, there was a need for separate, independent safety systems which could 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 Nuclear Power Demonstration (NPD), Canada's first nuclear power plant which began operation in 1962[4]. The target proposed for NPD from the above approach was a frequency of 10^{-5} per year for serious accidents, based upon an overall risk of 1 death per 100 reactor years (10^{-2} deaths/year).

Concurrently, G.C. Laurence, who had been named chairman of the Reactor Safety Advisory Committee (RSAC) which the AECB had created in 1956, also proposed[8], on similar arguments, that the likelihood of a "disastrous" accident at a nuclear power reactor should be less than 10^{-5} per year. Laurence further proposed that this target could be achieved with realistic

designs if there was 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 less than 10^{-1} per year and the probability that the protective devices would be inoperative or the containment provisions ineffective should be each less than 10^{-2}.

In the mid-1960's, 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", or normally operating equipment; and what later came to be known as the "special safety systems", designed to prevent or mitigate the consequences of failures of the process systems. The "special safety systems" include the reactor shutdown systems, emergency core cooling systems, and the containment provisions. Although modified over the years, these criteria still constitute the basic safety requirements for nuclear power plants.

The basic requirements, as last modified in 1972[10], set limits on the frequency of "serious process failures"* 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"). 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 I) were determined on the basis of the assumed maximum frequencies of the events. The maximum frequency of any "single failure" was taken as once per three years and the reference dose limits for individuals were chosen as equal to the one-year regulatory dose limits. For a "dual failure", with an assumed

---

* 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.

maximum frequency of once per three thousand reactor-years, 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 a million people.

Associated with these reference dose limits there are 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 an independent audit;

- the quality and nature of the essential process equipment shall be such that the total of all serious failures should not exceed 1 per 3 years;

- the special safety systems shall be physically and functionally separate from the process systems and from each other;

- each special safety system shall be readily testable as a system and shall be tested at a frequency which demonstrates that its unavailability is less than 10^{-3}.

In the early 1970's, the difficulty in analysing a reactor "runaway" accident, i.e. 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 that the above criterion for "cross-linked" failures will be met. With the additional shutdown system a reactor transient without scram 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. Provided the requirements for separation and

unavailability are met, such a major event would have a probability of the order of 10^{-7} per year.

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 emergency core cooling system (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 failure"/"dual failure" approach, as practised, adequately defined the required effectiveness of the special safety systems, some concerns in coverage became evident. Among the concerns were:

i) the inability to take into account the great variation in rates of occurrence and in the consequences of different single and dual failures;
ii) 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;
iii) the need to consider the necessary continuing operation of safety systems after an accident;
iv) the need to design for, and analyse, 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 which 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 FIGURE 2. The use of SDM's has contributed significantly to a better understanding of system behaviour and system 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, it 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 above 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 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 which have been developed over the years and the judicious use of fault trees and "safety design matrices", 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 licence. 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 which they normally control, such as non-radiological 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 provincial department join in conducting quality assurance 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, emergency core cooling system, and containment (16,17,18).

The policy has been that while 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 developed.

The first is a long-standing one which 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. While these features are not formally identified as requirements, 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 in evidence.

The second way 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 which 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 Association 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, while 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 U.S.A. Most noteworthly is the CSA N285 series which adopts most of the ASME nuclear 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 reach agreement on the content of each document, each new CSA nuclear standard contains a warning in its preface to the effect that the AECB may have requirements differing from those in the standard. In only one case so far have additional regulatory requirements been stipulated.

Licensing Process

Although the AEC Regulations call for only two formal steps, "construction approval" and "operating licence", in practice the licensing process for nuclear power plants involves a prior step of "site acceptance" and many intermediate sub-steps. The licensing process is described in some detail in reference 19.

The Atomic Energy Control Act does not require public hearings and, to date, the AECB has not held any 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 Board adopted the policy

of making applications for licences 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 proposed station and information on land use, present and predicted population, principal sources and movement of water, water usage, meteorological conditions, seismology and local geology. The AECB, itself, is primarily concerned with the inter-relationship of the site and plant, leaving evaluation of environmental impact to associated federal and provincial environmental agencies.

During this phase, the applicant is required to announce publicly his intentions to construct the facility and to hold public information meetings at which the public can express its views and question applicant officials.

Construction Approval

Prior to granting a Construction Approval the AECB must be assured that the design is such that the AECB safety principles and requirements will be met and that the plant will be built to appropriate quality standards. In order to do this, it is necessary that the design be sufficiently advanced to enable the safety analyses to be performed and their results assessed. The primary documentation required includes a Preliminary Safety Report (which combines the essential information of the Site Evaluation Report, a description of the Reference Design, and the Preliminary Safety Analyses), an overall Quality Assurance Program for the project together with a

specific program for construction quality assurance, and preliminary plans for operation.

Construction will only be authorized once the design and safety analysis programs have progressed to the point that, in the judgment of the AECB, no further 'significant' design changes will be required.

Operating Licence

Before issuing an Operating Licence the AECB must be assured, primarily, that the plant, as built, conforms to the design submitted and approved, and that the plans for operation are satisfactory. The requirements include submission of a Final Safety Report, completion of a previously approved commissioning program, examination and authorization of senior personnel, approval of operating policies and principles, preparation of plans and procedures for dealing with radiation emergencies, and a specific program for operations quality assurance.

Typically, a provisional licence is issued to permit start-up and, subject to AECB staff approval, increases in power to the design rating. Provided all has proceeded satisfactorily, a full Operating Licence is issued for a term not exceeding five years. Among the terms of an Operating Licence is the requirement that the licensee inform the AECB promptly of any occurrence or situation which 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 Licence. Formal approval of the Board 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 quality assurance principles. The AECB requires that an appropriate, formal quality assurance program be in existence for each phase of a nuclear project: design, construction, commissioning, and operation, as specified in the CSA N.286 series of standards[20,21,22,23,24,25].

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 Board 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 on-site 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

(see FIGURE 3) in the early sixties, one aspect received particular attention, namely, the proximity of a large population. The population reference dose limits in the "Siting Guide" (TABLE I) 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 outwards rom 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 out to a point (at about 18 miles) where the dose to an individual would be one percent 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 which 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 ten miles away. Although the Board'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[27] at the École Polytechnique in Montreal to determine what risk the presence of the airport would present to the nuclear power station. A risk map was produced as shown in FIGURE 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 re-location 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[28] to investigate generally the response of a concrete reactor containment building to the impacts of various parts (fuselage, engines) of various types of heavy aircraft (DC-8, B-747, etc.) depending upon the angle of impact.

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 150 feet). From this second control centre the state of several systems important to the safety of the reactor could be monitored and/or controlled, and the centre 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 II.

Design

Strict application of the safety philosophy to the design of a nuclear power plant can pose difficult design and analysis problems. Since 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 FIGURE 5. Maximum physical separation is achieved by having the rod system enter the reactor vertically with all the actuating mechanisms located on top of the reactor. The liquid injection system on the other hand 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 utilizing 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. Since this was a violation of the separation criterion it was not allowed. The final design employs completely separate shutdown rods and regulating rods, albeit of similar design.

The proposal by the Bruce 'A' designers to place major equipment, e.g. main heat transport pump motors and boilers, outside containment (see FIGURES 6 and 7) to facilitate inspection, testing, and maintenance, posed a particularly difficult

situation for the AECB. The interdependence between process equipment and a special safety provision (containment) was obviously being increased, but there were potential gains to be made in the reduction of personnel exposure during maintenance and in the greater freedom to carry out tests on the equipment. The early experience with the single unit, 200 MWe prototype Douglas Point station which had begun operating in 1967 had led to a personnel dose burden as high as 1,935 man-rem in 1971. Although these problems have since been corrected and personnel dose burdens are now running at 200-400 man-rem annually, there was a very strong incentive at the time to improve routine access to equipment. The Board considered the trade-off advantageous and gave its approval. The appropriateness of that decision can be judged by noting that for 1982, the total personnel dose burden for the four unit 3000 MWe Bruce 'A' station was only 370 man-rem.

Commissioning

It is the objective in the commissioning program to test equipment and systems as thoroughly as practical under conditions which simulate 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 those stations which employ a vacuum containment system, an important set of components are the pressure relief valves (see FIGURE 8) which interconnect the reactor buildings with the vacuum building. These valves are 2 to 3 metres 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 per second). 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 rise in pressure in the vacuum building actuates the passive dousing system located in its dome. In the single containment building design, however, with the gravity dousing system located in the dome above the reactor, the AECB has accepted that only the dousing system active components (logic and valves) need be tested, since an actual douse would entail a major clean-up and re-testing of other reactor system components.

Commissioning of the emergency core cooling system, as a system, presents

difficulties. The AECB accepts that it is not practical to simulate a rupture in the heat transport system for the purposes of commissioning. However, operation of the system as a whole can be demonstrated by either injecting water into a partially voided reactor core, or installing valved discharge lines just ahead of the core injection valves to permit commissioning tests at full design flow. Another operation, which is an essential part of the emergency core cooling function, is rapid depressurization of the core by initiating a fast or "crash" cooldown of the steam generators. This feature is tested by opening several of the boiler safety valves simultaneously, with all of systems at temperature.

Under some postulated upset and accident conditions, thermosyphoning may be necessary to keep the core cooled immediately after reactor shutdown. All such postulated events are examined and commissioning tests are done to demonstrate satisfactory cooling capability under various scenarios with full coolant inventory. Clearly, such tests must be done with the reactor operating at several per cent of full power.

Operation

One of the fundamental criteria in the Canadian safety approach is that each special safety system shall be readily testable as a system and shall be tested at a frequency which demonstrates that its unavailability is less than 10^{-3}. In the design of a plant, mathematical models are developed to predict the future unavailability of the special safety systems based on predicted failure rates for each component and a defined testing schedule. Because the required test intervals for most components range from several days to one month, it is evident that components and systems must be testable while the reactor is operating at high power. A further objective of the test program for special safety systems is that as far as practical, the tests should simulate accident 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 of the tests are simply a test of a single component where testing of a system is not practical, e.g. stroking of one of the 2 to 3 metre diameter pressure relief valves which connect 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 which hold up the shut-off 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 shut-off rods will fall. Similarly, for a sub-system which 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 would be 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 N-285.4[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. While 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 I, was adopted in the mid-1960's.

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 short-comings 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, e.g. any serious process failure should be detected by two diverse parameters. The need for, or adequacy of such requirements cannot be rigourously defended in the absence of appropriate component failure data and comprehensive probabilistic risk assessments. However, since 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. RSC 1970 c A-19.

2. AEC Regulations CRC 1978 c 365, as amended SOR/78-58, SOR/79-422.

3. Nuclear Liability Act RSC 1970 c 29 (1st Supp.). (came into force 1976).

4. "CANDU Nuclear Power System", AECL TDSI-105, January 1981.

5. D.A. Meneley and W.T. Hancox, "LOCA Consequence Predictions in a CANDU-PHWR", IAEA-CN-42/145, September 1982.

6. "A Proposed Statement on Safety Objectives for Nuclear Activities in Canada", ACNS-2, June 1981, AECB INFO-0055.

7. E. Siddall and W.B. Lewis, "Reactor Safety Standards and Their Attainment", AECL-498, September 1957.

8. G.C. Laurence, "Reactor Siting in Canada", AECL-1375, October 1961.

9. G.C. Laurence, "Reactor Siting Criteria and Practice in Canada", AECB-1010, February 1965.

10. D.G. Hurst and F.C. Boyd, "Reactor Licensing and Safety Requirements", AECB-1059, June 1972.

11. F.C. Boyd, "Containment and Siting Requirements in Canada", AECB-1018, April 1967.

12. J.H. Jennekens, "Recent Developments in Nuclear Plant Licensing in Canada", AECB-1074, June 1974.

13. W. Paskievici, "Proposed Safety Requirements for Licensing of CANDU Nuclear Power Plants - Report of Inter-Organizational Working Group", AECB-1149, November 1978.

14. "Recommended General Safety Requirements for Nuclear Power Plants", ACNS-4 (draft unpublished) 1983.

15. "The Use of Fault Trees in Licensing Submissions", AECB Regulatory Document C-70, April 1983.

16. "Requirements for Containment Systems for CANDU Nuclear Power Plants", AECB Regulatory Document C-7/REV-1, May 1982.

17. "Requirements for Shutdown Systems for CANDU Nuclear Power Plants", AECB Regulatory Document C-8/REV-1, May 1982.

18. "Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants", AECB Regulatory Document C-9/REV-1, May 1982.

19. M. Joyce, "The Licensing Process for Nuclear Power Reactors", AECB-1139/REV-1, November 1979.

20. CSA Standard N286.0, "Quality Assurance Program Requirements for Nuclear Power Plants".

21. CSA Standard N286.1, "Procurement Quality Assurance for Nuclear Power Plants.

22. CSA Standard N286.2, "Design Quality Assurance for Nuclear Power Plants".

23. CSA Standard N286.3, "Construction and Installation Quality Assurance for Nuclear Power Plants".

24. CSA Standard N286.4, "Commissioning Quality Assurance for Nuclear Power Plants".

25. CSA Standard N286.5, "Operations Quality Assurance for Nuclear Power Plants.

26. "Pickering Generating Station Safety Report, Volume 2, 1969, Ontario Hydro-Electric Power Commission of Ontario.

27. 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.

28. 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.

29. CSA Standard N285.4, "Periodic Inspection of CANDU Nuclear Power Plant Components.

30. Z. Domaratzki, "Reactor Safety Requirements in Times of Change", AECB paper INFO-0005, June 1980.

TABLE I

OPERATING DOSE LIMITS AND REFERENCE DOSE LIMITS FOR ACCIDENT CONDITIONS

Situation	Assumed Maximum Frequency	Meteorology to be Used in Calculation	Maximum Individual Dose Limits	Maximum Total Population Dose Limits
Normal Operation		Weighted according to effect, i.e. frequency times dose for unit release	5 mSv/yr whole body 30 mSv/yr to thyroid	100 man-Sv/yr 100 thyroid-Sv/yr
Serious Process Equipment Failure (Single Failure)	1 per 3 years	Either worst weather existing at most 10% of time or Pasquill F condition if local data incomplete	5 mSv whole body 30 mSv to thyroid	100 man-Sv 100 thyroid-Sv
Process Equipment Failure plus Failure of any Special Safety System (Dual Failure)	1 per 3×10^3 years	Either worst weather existing at most 10% of time or Pasquill F condition if local data incomplete	250 mSv whole body 2500 mSv to thyroid	10^4 man-Sv 10^4 thyroid-Sv

TABLE II

THE TWO GROUP CONCEPT FOR

DISTRIBUTION OF SAFETY FUNCTIONS

SAFETY FUNCTION	Group 1 Systems and Equipment	Group 2 Systems and Equipment
Shutdown Reactor	Shutdown System 1	Shutdown System 2
Remove Decay Heat	Normal Electrical Power and Cooling Water Supplies	Emergency Power Supply and Emergency Water Supply
Post-Accident Monitoring	Main Control Room	Secondary Control Area

ORGANIZATION CHART
ATOMIC ENERGY CONTROL BOARD
1 JANUARY 1963

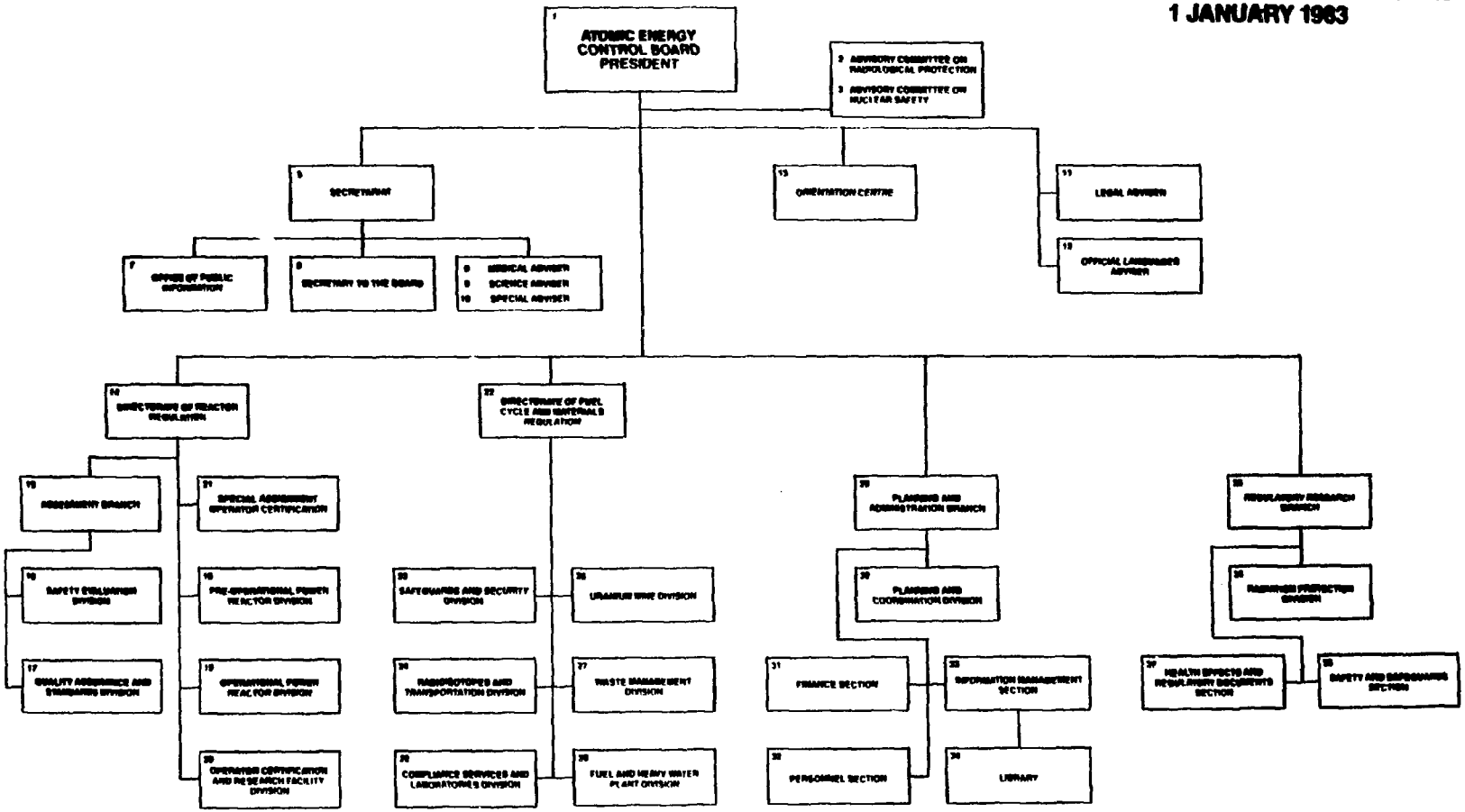
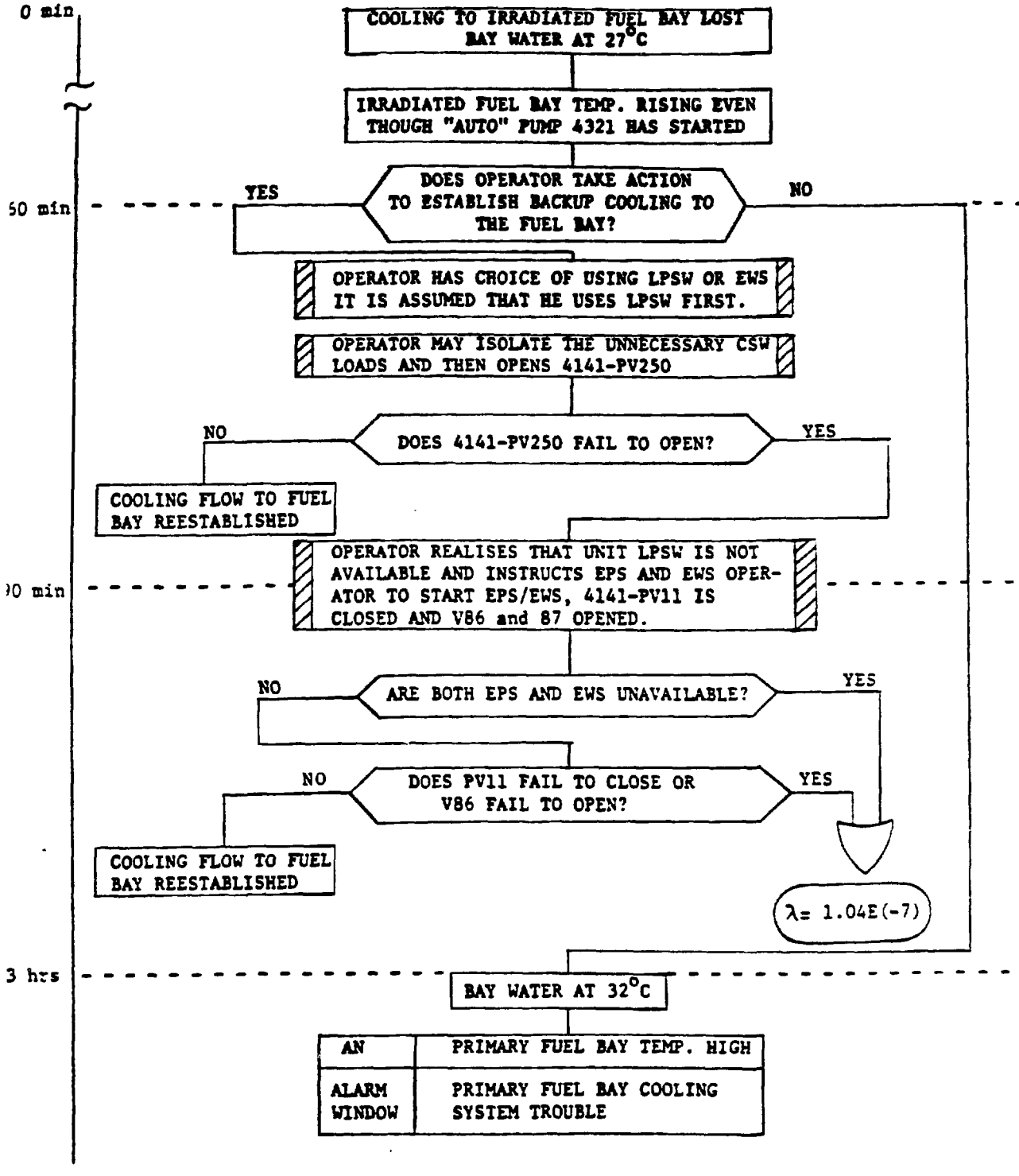
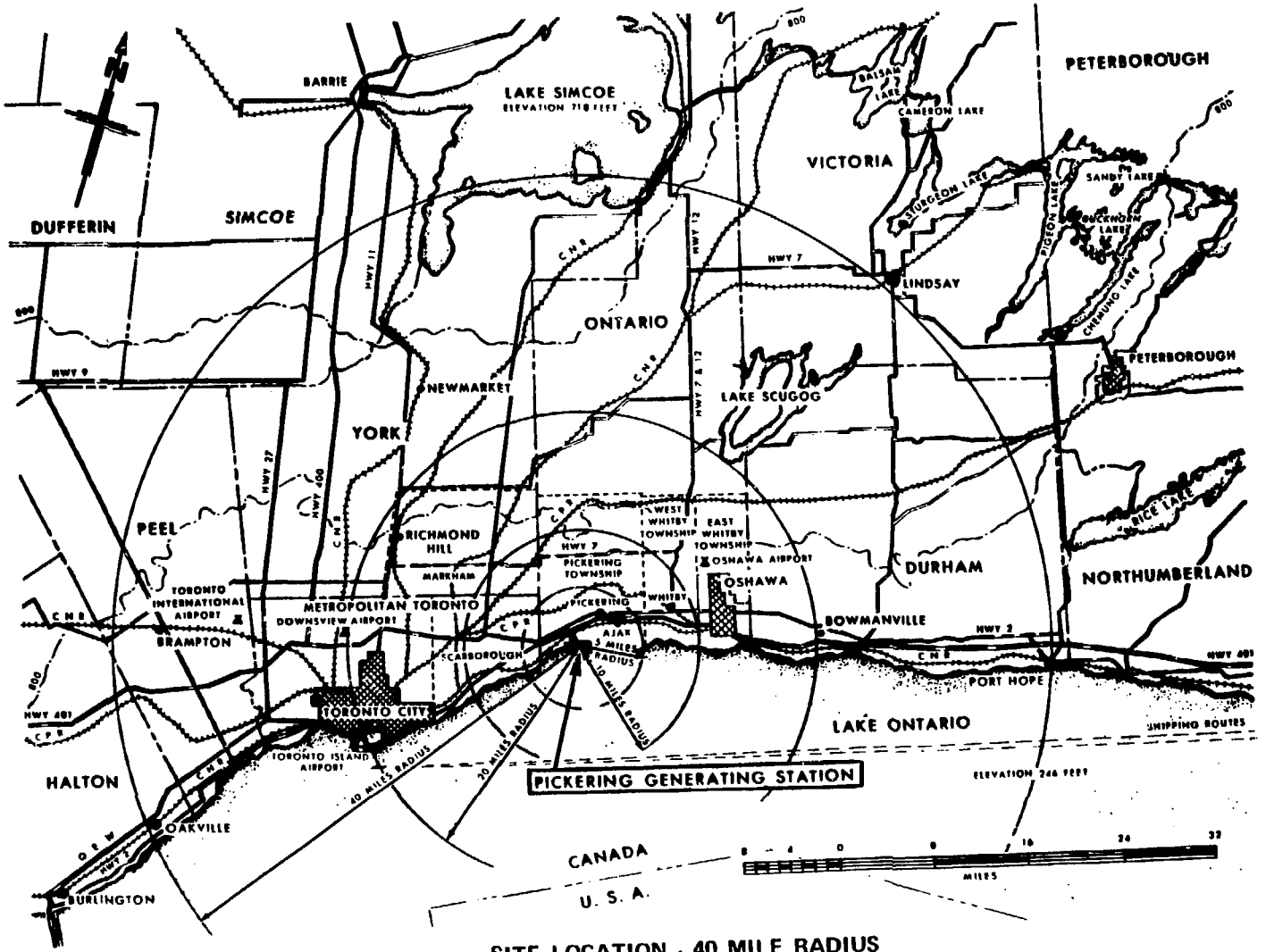


FIGURE 1



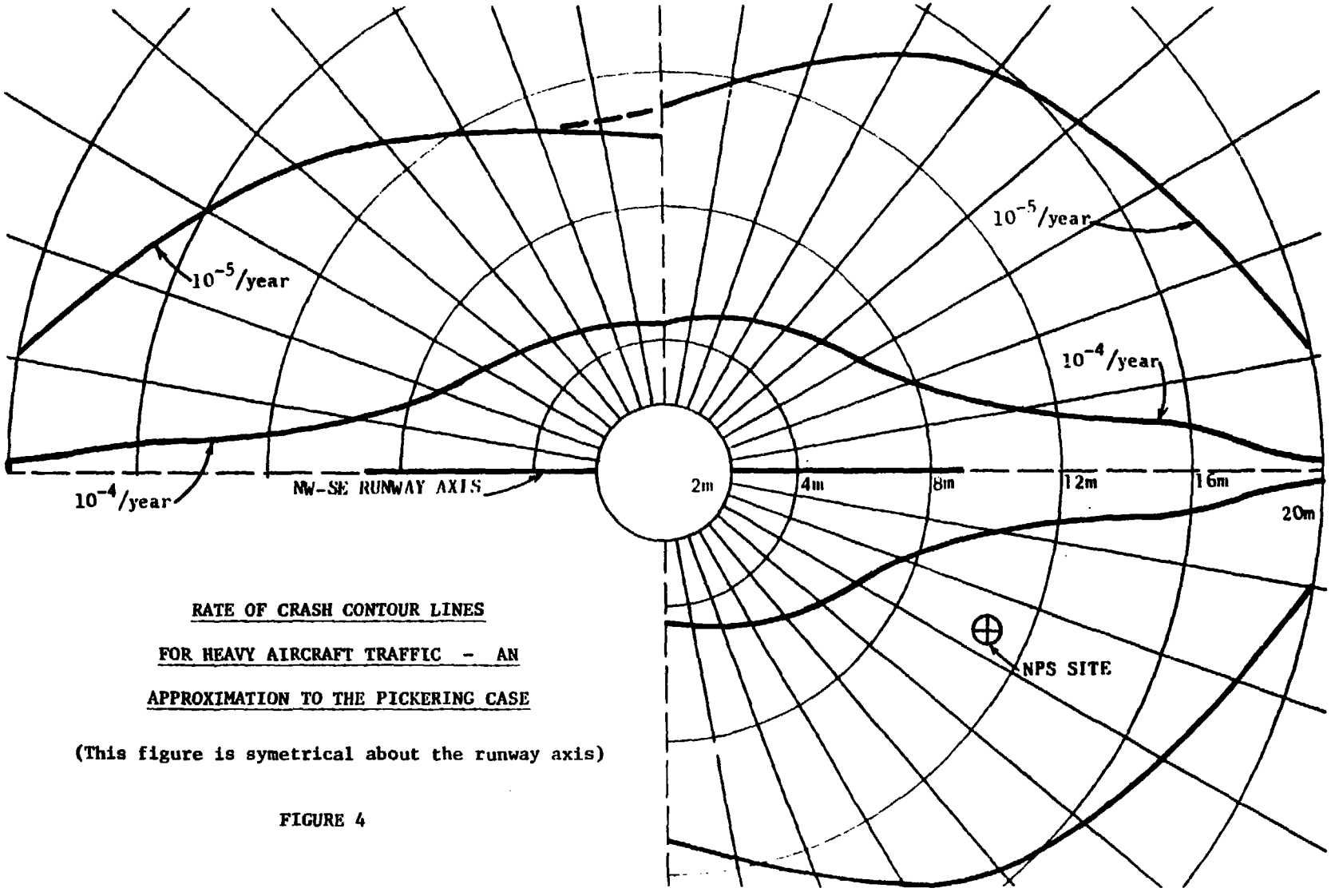
EXAMPLE OF EVENT SEQUENCE DIAGRAM

FIGURE 2



SITE LOCATION - 40 MILE RADIUS

FIGURE 3



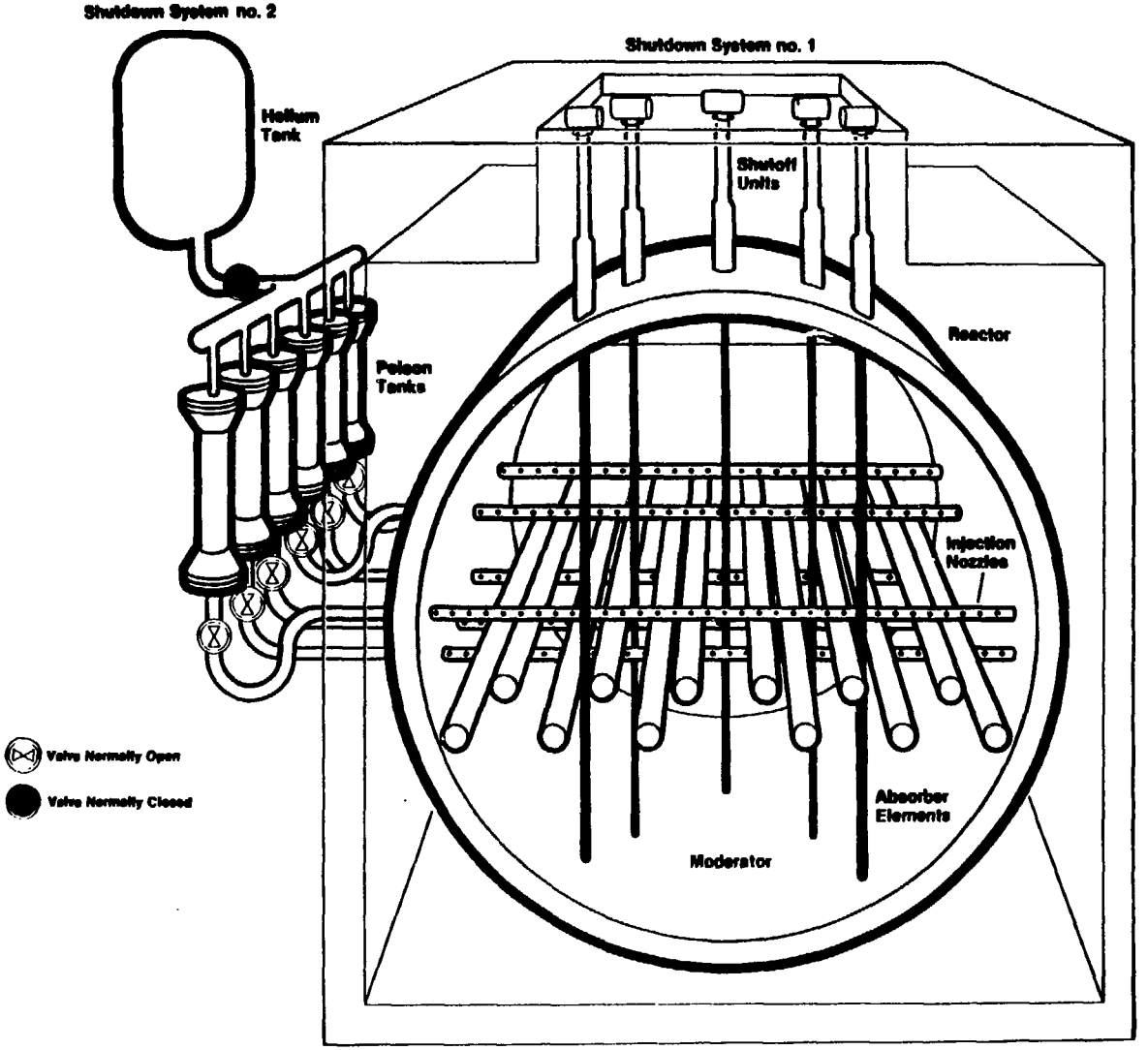
RATE OF CRASH CONTOUR LINES

FOR HEAVY AIRCRAFT TRAFFIC - AN

APPROXIMATION TO THE PICKERING CASE

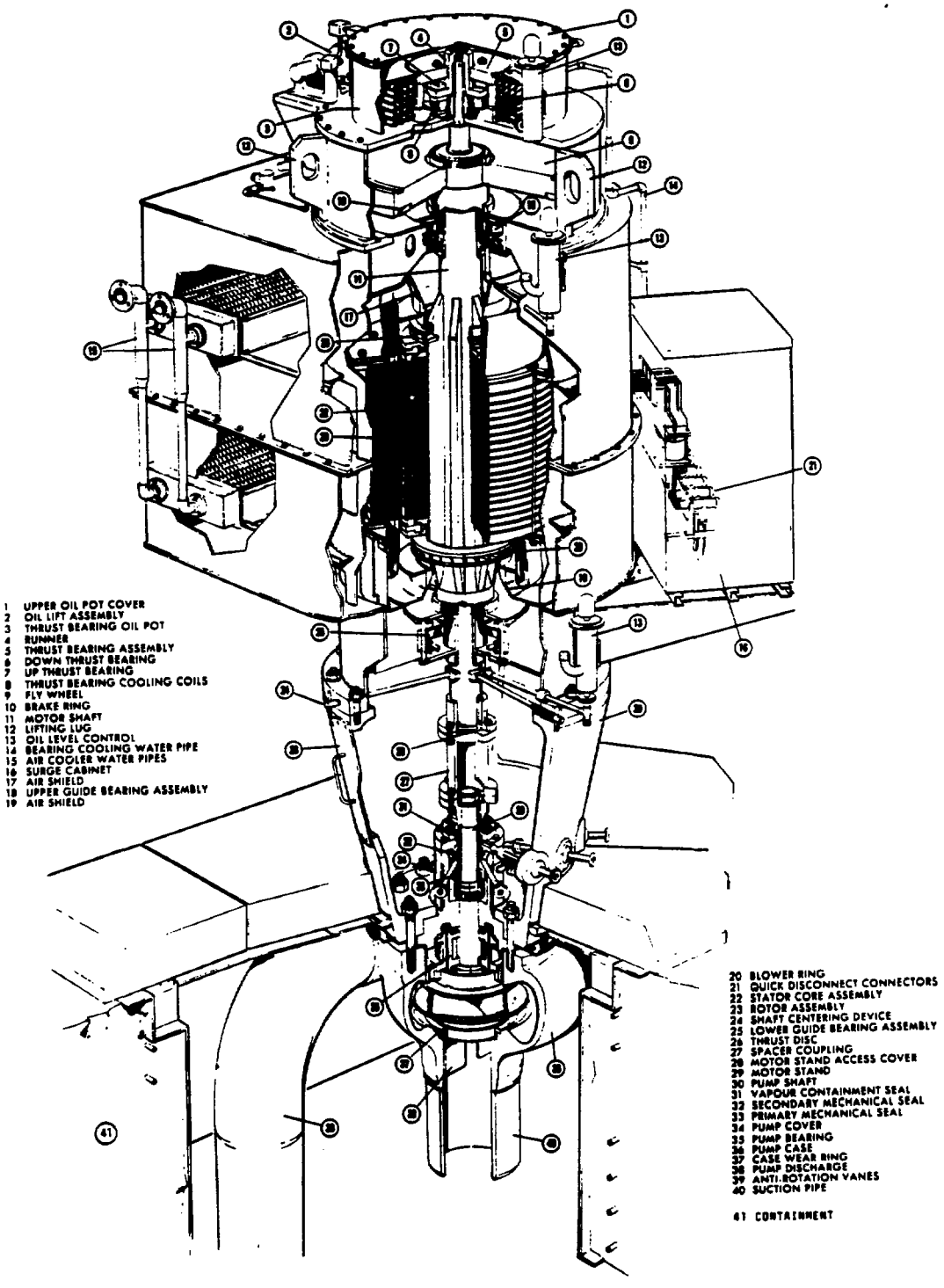
(This figure is symetrical about the runway axis)

FIGURE 4



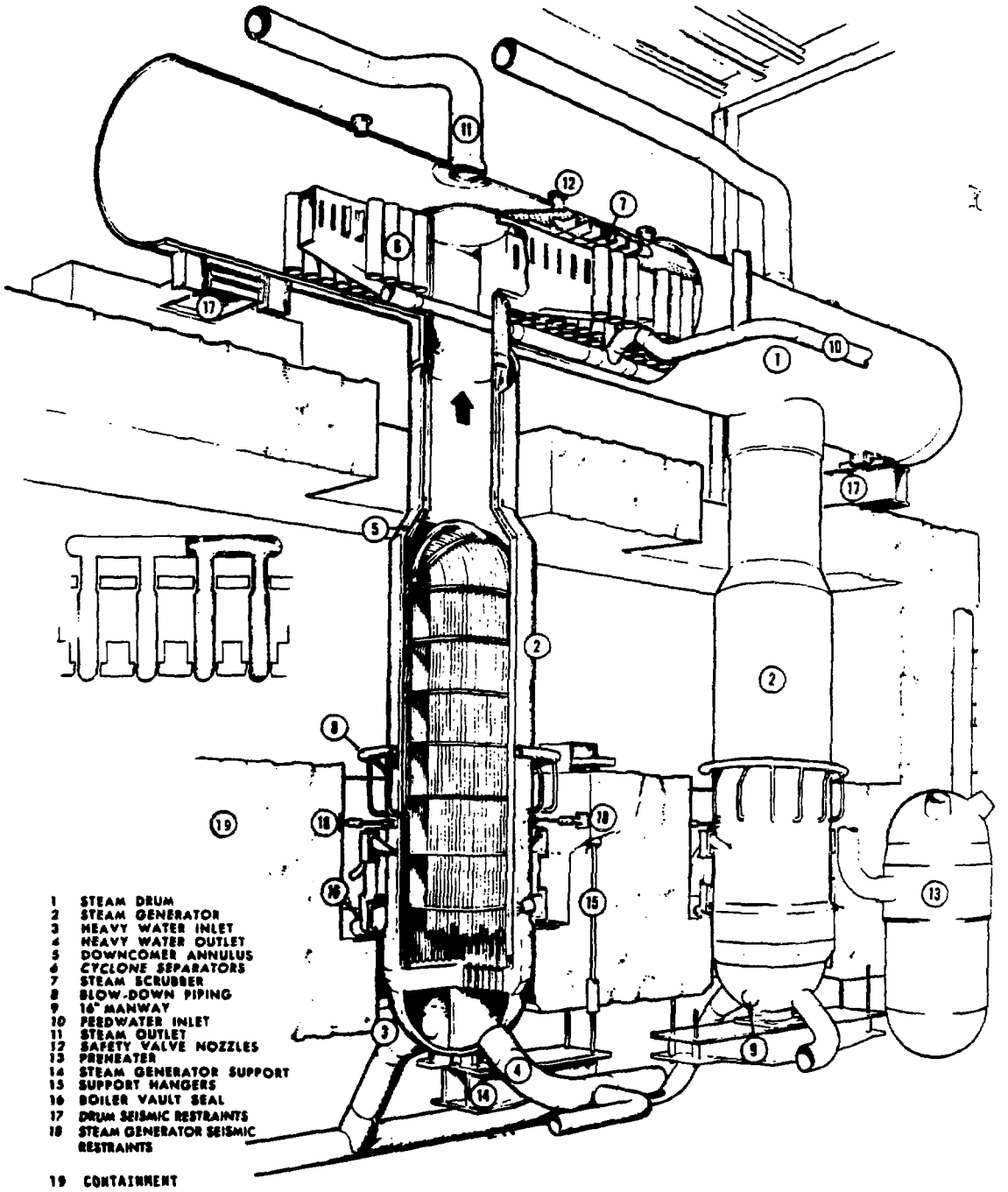
SAFETY SYSTEMS

FIGURE 5



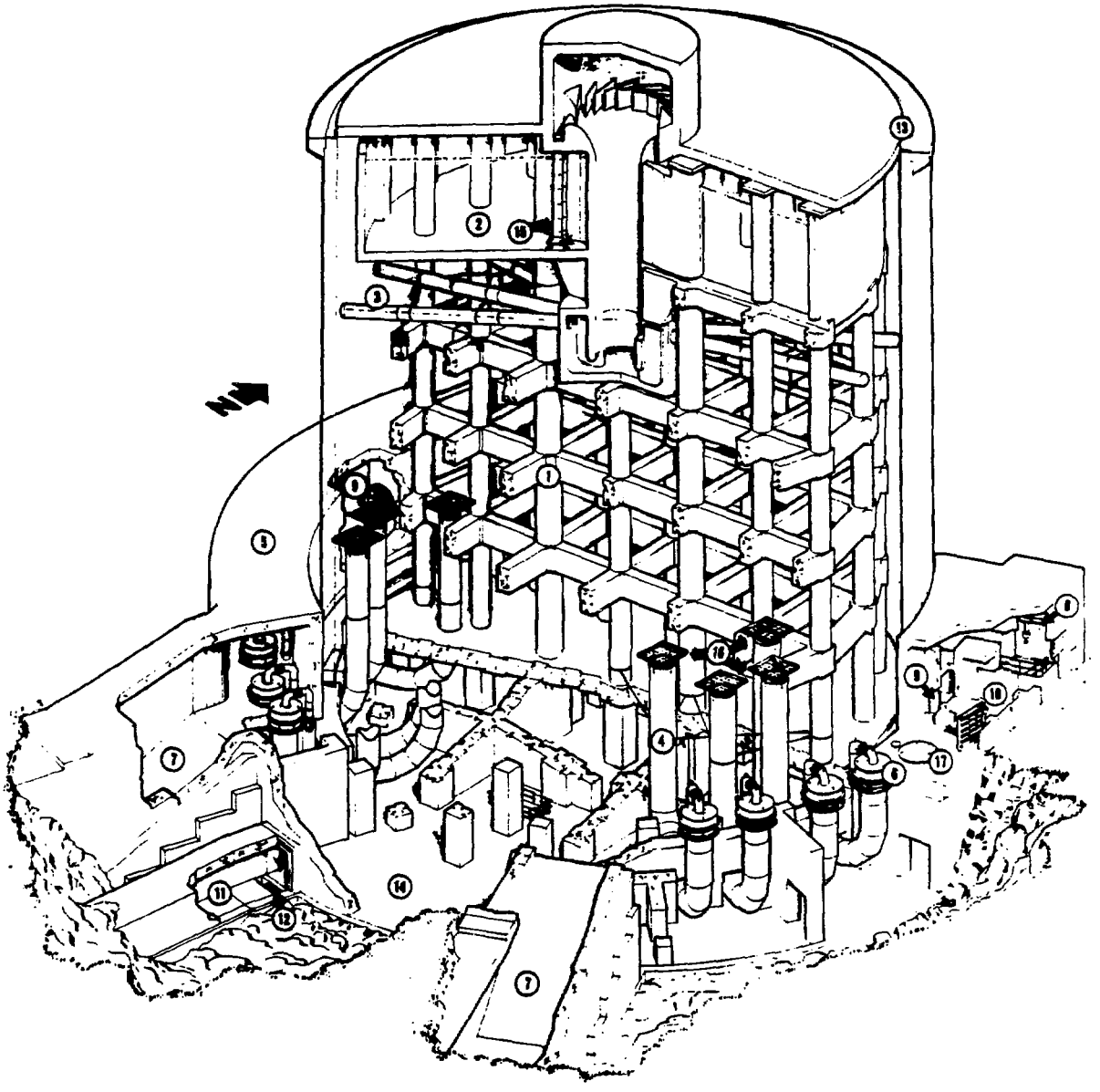
HEAT TRANSPORT PUMP

FIGURE 6



BRUCE "A" STEAM GENERATORS & PREHEATERS

FIGURE 7



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

CUTAWAY VIEW OF VACUUM BUILDING AND VALVE MANIFOLD

FIGURE 8