INFO-0116(E)

ACNS Advisory Committee on Nuclear Safety

CCSN Comité consultatif de la sûreté nucléaire

ACNS-4

RECOMMENDED GENERAL SAFETY REQUIREMENTS FOR NUCLEAR POWER PLANTS

by the

Advisory Committee on Nuclear Safety

June 1983

An Advisory Committee of the Atomic Energy Control Board of Canada — Secretariat: Ottawa, Canada K1P 5S9

Comité consultatif de la Commission de contrôle de l'énergie atomique du Canada — Secrétariat: Ottawa, Canada K1P 5S9

REPORT ACNS-4 - RECOMMENDED GENERAL SAFETY REQUIREMENTS FOR NUCLEAR POWER PLANTS

ABSTRACT

This report presents the recommendations of the Advisory Committee on Nuclear Safety for a set of general safety requirements that could form the basis for the licensing of nuclear power plants by the Atomic Energy Control Board. In addition to a number of recommended deterministic requirements the report includes criteria for the acceptability of the design of such plants based upon the calculated probability and consequence (in terms of predicted radiation dose to members of the public) of potential fault sequences. The report also contains a historical review of nuclear reactor safety principles and practices in Canada.

Preface

This report contains the recommendations of the Advisory Committee on Nuclear Safety to the Atomic Energy Control Board on general safety requirements for CANDU nuclear power plants in Canada. To develop these requirements, following its normal procedure, the ACNS appointed a Working Group of its members, at its the fifth meeting, Jan. 20, 1981. The Working Group, in developing the requirements, took into consideration the historical background to reactor safety regulation in Canada; consulted members of the AECB staff, the Advisory Committee on Radiological Protection of the AECB and representatives of AECL and the utilities; examined approaches to reactor safety requirements in other countries; and studied recent developments in the field of risk assessment, analysis, perception and management.

The Working Group also had the benefit of the views of the other members of the ACNS. The ACNS endorsed the report at its meeting of June 27, 1983, for submission to the Atomic Energy Control Board.

The members of the Working Group were:

J.T. Rogers, Chairman
N. Lind
O.R. Lundell
W. Paskievici
A. Pearson

The Working Group was assisted by F.C. Boyd, Science Adviser to the AECB.

EXECUTIVE SUMMARY

ACNS-4 Recommended General Safety Requirements for Nuclear Power Plants

Advisory Committee on Nuclear Safety

INTRODUCTION

This report presents the recommendations of the Advisory Committee on Nuclear Safety to the Atomic Energy Control Board (AECB) on general safety requirements for CANDU type nuclear power plants in Canada.

The objectives of this statement of requirements are:

a) to provide a basis for assuring that the safety objectives defined in reference 1 can be met for nuclear power plants in Canada;
b) to provide a comprehensive and consistent basis for AECB licensing regulations for nuclear power plants in Canada;
c) to provide a unified statement of the safety requirements for nuclear power plants in Canada for the information of all interested parties.

The proposed requirements embody many fundamental principles of nuclear reactor safety that have been developed over several decades of Canadian design and licensing practice. Among the foremost of these principles are:

a) the use of separation, independence, redundancy and diversity in the design;
b) the recognition that the prevention of process system failures is a fundamental element in the achievement of reactor safety;
c) the judicious use of probability arguments in which values of system unavailability or failure frequency must be based on direct experience or reasonable extrapolations therefrom.

In the development of the proposed requirements, the Committee recognized that the primary responsibility for the safety of a nuclear power plant rests with the owner. As a corollary, the Committee considers that a major role of the AECB is that of review and audit to ensure that the requirements which it has established are being met. The recommended requirements reflect this approach. They do not represent a major departure from past practice but are a stage in the development of that practice.

BACKGROUND

The first specific criteria for reactor safety and licensing in Canada were enunciated in the early 1960's by Laurence [2] who proposed that the probability of a "disastrous" accident should be less than 10^{-5} per reactor year, based on actual experience with component reliability. To ensure that such a low frequency could be achieved, it was required that "protective devices" and "containment features" be provided which were separate from the process systems and from each other. The separation was to be sufficiently complete that the probability of cross-linked or common-mode failures would be very small.

The above approach, using the categories of "single" process failures and "dual" combinations of process failures and failure of a safety system, was incorporated into the Siting Guide adopted by the AECB's Rector Safety Advisory Committee in 1964 and is still essentially in use today [3]. Thus, from the beginning, the reactor safety and licensing approach in Canada, while basically a deterministic procedure, has also incorporated a risk concept, i.e., the probability of a "disastrous" accident was to be low enough that the corresponding risk would be very small.

While this approach provided a reasonable basis for the systematic review of the safety aspects of CANDU nuclear power plants, its simplicity resulted in some difficulties in interpretation and application. These difficulties became increasingly important with growth in reactor size, fuel element power rating and system complexity, and the simultaneous growth in knowledge of system behavior, experimental data and analytical methods. The need for a more comprehensive approach lead to the formation in 1977 of an Inter-Organizational Working Group (IOWG), composed of representatives of AECB, the Reactor Safety Advisory Committee, Atomic Energy of Canada Limited and the three provincial utilities with nuclear power programs. The IOWG proposed general principles and safety requirements which retained the traditional deterministic defence-in-depth approach by requiring certain special safety systems and criteria, but expanded the probabilistic basis of the previous approach by defining six categories of events according to their probability, with increasing individual dose reference values permitted as the probability decreased.

Certain of the recommendations of the IOWG were incorporated by the AECB into its Consultative Document C-6[4]. This document retained the concept of several categories of accidents (5 instead of 6) for which reference individual doses were proposed ranging from 5×10^{-4} to 0.25 Sv. However, these categories were not defined on a probabilistic basis but in a deterministic way by grouping together, from a pre-determined list, postulated accidents.

PROPOSED REQUIREMENTS

The proposed general safety requirements for nuclear power plants are grouped under the following headings:

A. Radiological Dose Limits for Normal Operation
B. Siting
C. Design
D. Safety Analysis
E. Construction
F. Commissioning
G. Operation
H. Effluent and Waste Management
I. Decommissioning

The proposed requirements include use of the ALARA principle for normal operation[1].

Since the design is such an important factor in the safety of a nuclear power plant most of the recommended requirements apply to design and the analysis necessary to demonstrate the adequacy of a proposed design.

While the proposed safety requirements incorporate more comprehensive risk criteria than those of the Siting Guide, certain deterministic design requirements, such as those for the special safety systems, are retained to assure defence-in-depth against potential accidents.

In addition to the safety objectives referred to earlier, the Committee adopted the criterion that the total estimated radiological risk to the public from all accident conditions should not exceed significantly the risk from normal operation. To ensure that this objective is achieved, analyses of the consequences of potential failures must be done. The Committee proposes that the acceptability of the risks estimated from these accident analyses be determined by a set of risk categories, given in Table 1 and depicted graphically in Fig. 1.

These accident categories were established by considering the fundamental risk criterion stated above, the existing single-failure/dual-failure criteria of the Siting Guide and the recommendations of the IOWG as well as other information. The definitions of the categories take into account risk aversion for higher-consequence failures.

Each category has an upper limit value for the permitted sum of the probabilities of mutually exclusive failure sequences within the effective dose-equivalent interval. The acceptability of the predicted results of accident sequences is to be judged as follows:

a) if the sums lie below the limit values in all the categories, the estimated total risk is acceptable;

b) if the sum in any category lies above the upper limit value, the estimated risk is generally not acceptable.

c) In the case described in item b) above, the AECB may accept the situation, provided that the maximum expected value of risk to an individual member of the public from all the accident sequences to be analyzed is equal to or less that that corresponding to the summation of the limiting risks of all the accident categories of Table 1. (See Table 2). In making this judgement, the AECB should consider the consequence level of the particular interval or intervals involved, uncertainties in physical data, adequacy of analytical models, uncertainties in probabilistic models and data, conservatisms in the analysis, economic and social factors and any other factors which might affect the analysis.

The proposed risk categories are shown plotted in the form of a histogram in Fig. 1 which compares them with the criteria of the Siting Guide.

The maximum value of the overall risk for the six categories is given in Table 2, where it is compared to the values of the risk given by the IOWG recommendations and those corresponding to the AECB Siting Guide, as well as the risks associated with normal operation at the regulatory limit and the ALARA target. It can be seen that the proposed accident sequences risk is of the same magnitude as the risk from normal operation at the regulatory limit.

If the probability of a postulated event or sequence of events is 10^{-7} or less per reactor year the Committee recommends that it be accepted whatever the potential dose equivalent. Arguments for the justification of the cut-off at a probability of 10^{-7} per year are given in the report.

CONCLUSION

The ACNS believes that the recommendations in this report will continue to ensure adequate safety of nuclear power plants in Canada for the public and workers, while permitting the economic and social benefits of nuclear power to be obtained.

TABLE 1

Proposed Risk Categories for Accident Analysis

Category	Individual Effective Dose Equivalent Interval, Sieverts	Sum of the Probabilities of Occurrence of Failures within the Corresponding Effective Dose Equivalent Interval (Per Reactor Unit per year)
1	$> 0 - 10^{-2.5}$	3.33×10^{-1}
2	$10^{-2.5} - 10^{-2}$	10^{-1}
3	$10^{-2} - 10^{-1.5}$	10^{-2}
4	$10^{-1.5} - 10^{-1}$	10^{-3}
5	$10^{-1} - 10^{-0.5}$	10^{-4}
6	$10^{-0.5} - 1$	10^{-5}

TABLE 2

Calculated Maximum Values of Risk to

Most Highly Exposed Individual in the Population

ACCIDENT SEQUENCES

Criterion	Risk,* Sieverts/Reactor year
ACNS-4:	2.5×10^{-3}
IOWG Recommendation	1.6×10^{-4}
AECB Siting Guide (Single Failure/Dual Failure)	1.8×10^{-3}**

NORMAL OPERATION

Criterion	Risk, Sieverts/Reactor year
ALARA Target	5.0×10^{-5}
Regulatory Limit	5.0×10^{-3}

BACKGROUND RADIATION

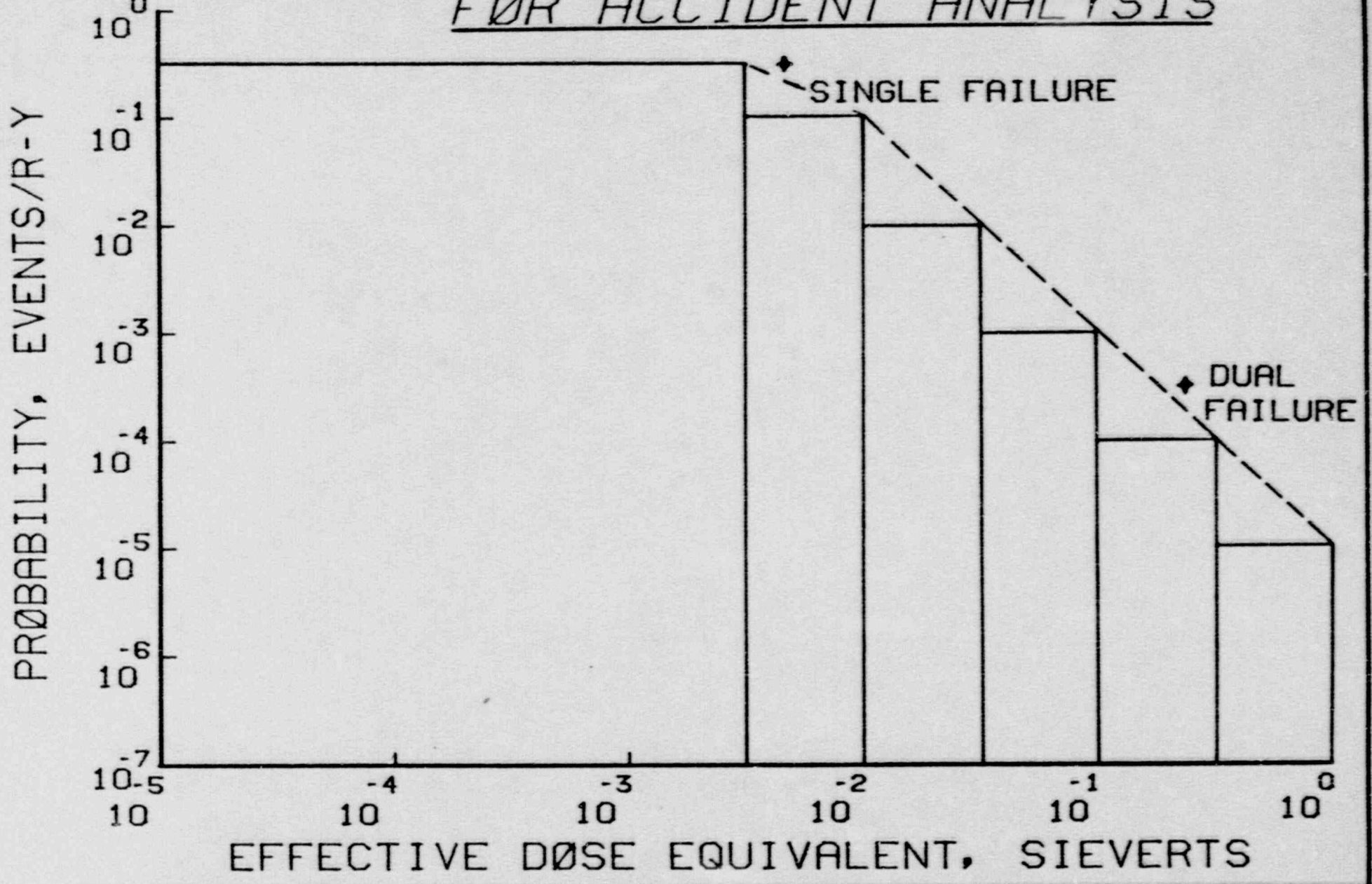
Source	Risk, Sieverts/Year
Natural Sources (indoor and outdoor) (Ref. 4)	10^{-3}

---

* The risk values given are conservative since they assume that all accident sequences in a given category are at the upper consequence limit of the category.

** The calculated maximum risk corresponding to the AECB Siting Guide criteria is more of a nominal value than that corresponding to the present recommendations because of the greater use of deterministic and arbitrary elements in the Siting Guide.

FIGURE 1 PROPOSED RISK CATEGORIES FOR ACCIDENT ANALYSIS



References

1. Safety Objectives for Nuclear Activities in Canada.
Report of the Advisory Committee on Nuclear Safety.
ACNS-2, June, 1981. Amended, April, 1982.

2. Laurence, G.E.
Reactor Siting in Canada.
AECL-1375, October, 1961.

3. _____
Reactor Siting and Design Guide.
AECB Document, November, 1964.

4. _____
Licensing Guide No. 39. Requirements for the Safety Analysis for CANDU Nuclear Power Plants (Draft).
AECB Consultative Document C-6, June, 1980.

INFO-0116

ACNS Advisory Committee on Nuclear Safety

CCSN Comité consultatif de la sûreté nucléaire

ACNS-4

RECOMMENDED GENERAL SAFETY REQUIREMENTS FOR NUCLEAR POWER PLANTS

by the

Advisory Committee on Nuclear Safety

June 1983

An Advisory Committee of the Atomic Energy Control Board of Canada — Secretariat: Ottawa, Canada K1P 5S9

Comité consultatif de la Commission de contrôle de l'énergie atomique du Canada — Secrétariat: Ottawa, Canada K1P 5S9

Table of Contents

1.0 INTRODUCTION

One of the first tasks assigned to the Advisory Committee on Nuclear Safety (ACNS) following its formation in 1980 was to review and comment on the various licensing guides developed by the AECB staff. As a result of its review and recommendations the ACNS was asked to develop documents defining safety objectives for all nuclear activities in Canada as well as statements of general safety requirements for specific nuclear activities. The safety objectives have now been defined and are given in reference 1.

These safety objectives have been endorsed by the Atomic Energy Control Board and are now incorporated in a basic policy statement of the AECB.

In this report, the ACNS presents a proposed statement of general safety requirements for nuclear power plants* in Canada. The objectives of this statement are:

a) to provide a basis for assuring that the safety objectives defined in reference 1 can be met for nuclear power plants in Canada
b) to provide a comprehensive and consistent basis for AECB licensing regulations for nuclear power plants in Canada
c) to provide a unified statement of the safety requirements for nuclear power plants in Canada for the information of all interested parties.

As discussed later, in developing this statement of requirements, the ACNS has judged that nuclear power plants in Canada, licensed under existing criteria, are adequately safe but that the application of these criteria have presented some problems. Therefore, an important goal of the ACNS in the development of this statement of requirements has been to overcome these problems and to facilitate the licensing process while ensuring that nuclear power plants in Canada continue to be safe.

The requirements proposed in this report embody many fundamental principles of

---

* CANDU nuclear power plants are to be understood in all subsequent references to nuclear power plants in this report, unless otherwise stated.

nuclear reactor safety that have been developed over several decades of design and licensing practice. Foremost among these principles are:

a) the use of separation, independence, redundancy and diversity in the design;
b) the recognition that the prevention of process system failures is a fundamental element in the achievement of reactor safety;
c) the judicious use of probability arguments in which values of system unavailability or failure frequency must be based on direct experience or reasonable extrapolations therefrom.

With the careful application of the proposed requirements, a nuclear power plant in normal day-to-day operation would not subject individuals in its vicinity to more than a small fraction of the radiation exposure limits established by internationally-accepted standards and adopted by the AECB. In addition, the risk to the population in the vicinity of a nuclear power plant resulting from accidents caused by component failure or human error would be very low and comparable to the risk from normal operation.

In developing this statement of general safety requirements, the ACNS accepts that the risk to the health of operators and the public from the entire fuel cycle associated with existing nuclear power plants in Canada is comparable to and probably less than the risks from alternative demonstrated methods of generating electricity (e.g., 2-5). Furthermore, the ACNS recognized the significant direct and indirect economic and social benefits resulting from the operation of nuclear power plants (e.g., 6-10). Considering these factors among others, the ACNS judged that there was no need to reduce the maximum calculated risk to operators and the public from the operation of nuclear power plants in Canada, as deduced from the current Canadian licensing regulations and procedures. The ACNS believes that the recommendations in this report will ensure adequate safety for the public and workers while permitting the economic and social benefits of nuclear power to be obtained.

In the development of the proposed requirements, the ACNS has recognized that the primary responsibility to ensure that a nuclear power plant is designed, constructed, operated and otherwise managed in a safe manner rests with the plant owner. In addition to ensuring that regulatory limits for exposures to radioactivity are met, the plant owner is responsible for ensuring that any

radiation doses* received by the public or workers under normal conditions are as low as reasonably achievable below these limits, social and economic factors being taken into account.**

As a corollary to the recognition of the owner's responsibility, the ACNS considers that a major role of the AECB is that of review and audit to ensure that the requirements it has established are being met in all phases of the activities associated with nuclear power plants.

The ACNS assumes that specific safety requirements and guidelines for the design, analysis and operation of various systems will be issued by the AECB as required to amplify and clarify the general requirements of this document.

It is intended that these recommended requirements will apply to all Canadian power reactors for which construction licenses have yet to be granted.

The requirements proposed here do not represent a major departure from past practice but are a stage in the development of that practice, as described in section 2.0 of this report. In recommending these safety requirements, the ACNS does not imply that the safety of existing nuclear power plants in Canada is inadequate nor that the risks to the public and workers from their operation are unacceptable. The recommendations are made in the light of growing experience and knowledge to assure all concerned that nuclear power plants in Canada are and will continue to be acceptably safe.

---

* As used in this document, dose means dose-equivalent or effective dose-equivalent, depending on the context. See Glossary of Terms.

** This approach is usually referred to as the ALARA approach.

2.0 HISTORICAL REVIEW AND BACKGROUND OF REACTOR LICENSING PRINCIPLES AND PRACTICE IN CANADA

The first criteria for reactor safety and licensing in Canada were enunciated in the late 1950's and early 1960's by Laurence(11). Significant contributions to reactor safety concepts were also made at this time by Siddall and Lewis (12,13). Laurence stipulated that the probability of a "disastrous" accident should be less than 10^{-5} per reactor year. Furthermore, this probability was to be based on actual experience with component reliabilities. To ensure that such a low probability could be achieved, it was required that "protective devices" and "containment features" be provided which were separate from the process systems and from each other. The separation was to be sufficiently complete that the probability of cross-linked or common-mode failures would be very small.

This approach was incorporated into the first Siting Guide of the AECB in 1964(14). Thus, from the beginning, the reactor safety and licensing approach in Canada, while basically a deterministic procedure, has also incoporated a risk concept, i.e. the probability of a "disastrous" accident was to be low enough that the corresponding risk would be very small.

The development of this approach which is essentially still in use today (15), is summarized in Table 1. It requires that serious process system failures (single failures) are to have a total probability no greater than once in three years and are not to expose an individual in the general public at the site boundary to a total whole body dose exceeding 5×10^{-3} Sieverts, while process system failures combined with a failure of one of the special safety systems* (dual failures) are to have a total probability not greater than 3.3×10^{-4} per year, and are not to expose an individual in the general public to a whole body dose exceeding 0.25 Sieverts. Failures of a process system and the simultaneous unavailability of two special safety systems (triple failures) are ignored on the basis of the very low probability of such event sequences

---

* These include the protective devices and containment features and are:
a) two independent shut-down systems of different designs;
b) emergency core-cooling system;
c) containment system.

TABLE 1

AECB Siting Guide

Reference Dose Limits

Normal Operation and Accident Conditions

Situation	Maximum Probability	Maximum Individual Dose Limits	Maximum Total Population Dose Limits
Normal Operation	--	5×10^{-3} Sv/yr whole body	100 man-Sv/yr whole body
		3×10^{-2} Sv/yr to thyroid	100 thyroid - Sv/yr
Single Failure (Process System)	1 per 3 years	5×10^{-3} Sv whole body	100 man-Sv whole body
		3×10^{-2} Sv to thyroid	100 thyroid - Sv
Dual Failure (Process System and Safety System)	1 per 3×10^{3} years	0.25 Sv whole body	10^{4} man - Sv whole body
		2.5 Sv to thyroid	10^{4} thyroid - Sv

(Based on Ref. 15)

($\leq 3.3 \times 10^{-7}$ per reactor year), considering the independence of the special safety systems.**

In addition to these individual dose limits, corresponding collective dose limits were established for normal operation and the two accident states. The individual and collective dose limits were chosen on the basis of comparative risk, the risk of leukemia, considered as the most significant radiological hazard, should be small compared with its normal rate of occurrence.

This approach has provided a reasonable basis for the systematic review of the safety aspects of a CANDU nuclear power plant. However, these simple requirements have resulted in some difficulties in interpretation and application. These difficulties became increasingly important with growth in reactor size, fuel element power rating and system complexity and the simultaneous growth in knowledge of system behavior, experimental data and analytical methods. Such difficulties became particularly evident in the licensing of the Bruce A reactor units in 1976. These difficulties can be summarized as follows:

i) The approach does not distinguish amongst single failures with differing rates of occurrence and consequences.

ii) It does not distinguish amongst dual failures with differing rates of occurrence and consequences.

iii) It deals in a simplistic fashion with safety system impairment.

iv) It does not deal explicitly with events of such low probability that the consequences could be ignored.

v) It does not treat external events explicitly.

vi) While well-suited to deal with the reactor shut-down function in the event of process system failure, it does not adequately deal with the more complex safety functions of emergency cooling and containment.

The need for a more comprehensive approach lead to the formation in 1977 of an Inter-Organizational Working Group (IOWG), composed of representatives of AECB,

---

** Failure to shut down the reactor following a process system failure is not considered in this analysis. Since two independent and diverse safety shut-down systems are required, the simultaneous random unavailabilities of these two special safety systems following a process system failure would be a triple failure with the very low probability stated above.

the Reactor Safety Advisory Committee*, AECL and the utilities. The objective of the IOWG was to review Canadian reactor safety principles and criteria and to prepare an up-dated statement, supplemented as necessary by broad guidelines explaining their application. It was expected that this up-dated statement would overcome the difficulties which had become evident. The efforts of the IOWG resulted in the issuing of a report which stated proposed safety requirements for licensing CANDU nuclear power plants and provided an explanation of the philosophy underlying those requirements (16,17). The general principles and safety requirements proposed by the IOWG retained the traditional deterministic defence-in-depth approach by requiring certain special safety systems and criteria, but expanded the probabilistic basis of the previous approach by defining six categories of events according to their probability, with increasing individual dose reference values permitted as the probability decreased (See Table 2).

Other elements of the IOWG approach included:

a) a constant risk equal to that of normal operation for the first three event categories, with reduced risk for the last three categories to provide a risk aversion approach to high-consequence accidents;
b) an explicit cut-off limit for the consideration of the consequences of events with probabilities less than 10^{-7}/year;
c) a framework for handling rare single events and multiple coincident failure events, whether of process or safety systems;
d) methods of handling external events such as earthquakes, aircraft impacts and sabotage.

The IOWG proposals were not adopted in full by the AECB. The ACNS understands that there were apparently two main reasons for this decision. First, the increase in the maximum reference-value dose from 0.25 Sv to 1.0 Sv, when combined with the proposed tolerance of a factor of ten on predicted reference-value doses allowed if encountered in the late stages of design, was not considered acceptable. Second, the AECB did not have enough confidence, at that time, in the analytical tools and the statistical data base to provide

---

*The Reactor Safety Advisory Committee, along with a number of other specifically-oriented advisory committees, was disbanded by the AECB in 1978.

TABLE 2

IOWG PROPOSED REFERENCE VALUES(16)

Reference Dose Interval, Sv		Reference Value for the Sum of the Predicted Rates of Occurrence of Failures within the Corresponding Reference Dose Interval (Per Reactor Unit Per annum)
Whole Body	Thyroid	
$0\text{-}5 \times 10^{-4}$	$0\text{-}5 \times 10^{-3}$	10^{-1}
$5\times10^{-4} - 5\times10^{-3}$	$5\times10^{-3} - 5\times10^{-2}$	10^{-2}
$5\times10^{-3} - 5\times10^{-2}$	$5\times10^{-2} - 0.5$	10^{-3}
$5\times10^{-2} - 0.1$	0.5 - 1.0	10^{-4}
0.1 - 0.3	1.0 - 3.0	10^{-5}
0.3 - 1.0	3.0 - 10.0	10^{-6}

reasonably accurate probability estimates. In addition, the ratio of thyroid to whole body dose was not in accord with the most recent estimates (18).

Certain of the recommendations of the IOWG were incorporated by the AECB in its Consultative Document C-6 (19). The document has retained the concept of several categories of accidents (5 instead of 6) for which reference individual doses were proposed ranging from 5×10^{-4} to 0.25 Sv. However, these categories were not defined on a probabilistic basis but in a deterministic way by grouping together, from a pre-determined list, postulated accidents. Nevertheless, the grouping of these accidents represented the judgment of the AECB staff on their probabilities and represented, implicitly, the probability values of the first five IOWG categories (See Table 3). Consultative Document C-6 is being used on a trial basis in the licensing process of the Darlington reactor station.

TABLE 3

Proposed Reference Values in

AECB Consultative Document C-6 (19)

Categories of Postulated Event	Reference Dose Limits, Sv	
	Whole Body	Thyroid
1	5×10^{-4}	5×10^{-3}
2	5×10^{-3}	5×10^{-2}
3	3×10^{-2}	0.3
4	0.1	1.0
5	0.25	2.5

3.0 PROPOSED REQUIREMENTS

The proposed general safety requirements for nuclear power plants are stated in this section of the report under the following headings:

A. Radiological Dose Limits for Normal Operation
B. Siting
C. Design
D. Safety Analysis
E. Construction
F. Commissioning
G. Operation
H. Effluent and Waste Management
I. Decommissioning

The proposed general safety requirements should be read and interpreted in the perspective of the statement of General Safety Objectives for Nuclear Activities in Canada, reference 1, and in the light of the Commentary on Proposed Requirements provided in Section 4.0 of this report.

A. Radiological Dose Limits for Normal Operation

A.1 The siting, design, construction, commissioning, operation and decommissioning of a nuclear power plant shall ensure that the effective dose equivalent and committed effective dose equivalent to an atomic radiation worker or to a member of the public resulting from normal operation of and normal activities associated with the nuclear power plant will not exceed the levels listed in Schedule II of the Regulations (SOR/74-334, Canada Gazette, Part II, Volume 108, No. 12, June 4, 1974, as amended) made pursuant to the Atomic Energy Control Act.

A.2 The siting, design, construction, commissioning, operation and decommissioning of a nuclear power plant shall, as far as practicable, ensure that the effective dose equivalent and committed effective dose equivalent to a member of the public due to normal operation of and normal activities associated with the nuclear power plant will not exceed a target of one percent of the regulatory limit specified in A.1.

A.3 The siting, design, construction, commissioning, operation and

decommissioning of a nuclear power plant shall ensure that the effective dose equivalent and committed effective dose equivalent to an atomic radiation worker at the nuclear power plant will be as low as reasonably achievable below the regulatory limit specified in A.1.

B. Siting

B.1 The siting of a nuclear power plant shall take into account the expectation of meeting the radiological requirements stated in section A, i.e., the site must not present any factors that could place undue requirements or limitations on the design or operation of the plant.

B.2 In considering alternative sites for a nuclear power plant, population (collective) doses should be estimated for both normal operation and accident sequences using accepted approaches and the estimated values should be considered as one factor in the choice of a site.

B.3 At the chosen site for a nuclear power plant, the frequency and severity of natural (other than earthquakes) and man-made external events should be sufficiently low that the estimated risk to the public from the consequential failure of the plant will be a small fraction of the overall risk to the public presented by the plant.

B.4 For earthquakes, at or near the chosen site for a nuclear power plant, of postulated consequences higher than the historical records and for which no sound theoretical model relating frequency and the consequences of the earthquake exists, the estimated risk to the public from the consequential failure of the plant should be small compared to the risk to the public from the earthquake itself.

B.5 The characteristics of the site shall permit practical contingency arrangements for dealing with accidents having potentially hazardous consequences beyond the plant boundary.

C. Design

C.1 The design of nuclear power plants shall follow good engineering principles and practices, shall be in accordance with appropriate recognized codes and

standards and shall employ appropriate quality assurance and quality control methods.

C.2 In the design of a nuclear power plant, all reasonable steps shall be taken to prevent accidents from occurring or to lower their probability of occurrence.

C.3 The design of a nuclear power plant shall ensure by all reasonable means that fission products are retained within the fuel elements under foreseeable operating conditions and that appropriate barriers to their movement from the fuel elements shall be provided.

C.4 The design of a nuclear power plant shall provide for certain safety functions whose purpose is to prevent, or mitigate the consequences of, failures of the process systems. The safety functions are:

a) provision of rapid shut down of the reactor and maintenance of the reactor in a shut down state under anticipated or actual accident conditions
b) provision of adequate cooling of the fuel under accident conditions
c) provision of adequate containment of radioactive materials under accident conditions

C.5 Nuclear power plants shall have special safety systems whose purpose is to assist in the fulfillment of the safety functions.

The special safety systems shall include, at least:

(a) two diverse means for rapidly stopping the nuclear reaction, each capable, acting alone, of shutting down the reactor from all states in which it is likely to be operating. Each shall be capable of maintaining the reactor in a safe shut-down state indefinitely or until another assured means of maintaining the reactor in a safe shut-down state can be employed;

(b) a means for injecting, and, if necessary, re-injecting, a coolant to replace the normal primary coolant in the event that the normal pressure boundary of the primary coolant system is breached.

(c) a means for containing any radioactive substance that may be released from the primary coolant system in the event that the normal pressure boundary of the system is breached.

C.6 Each special safety system shall be designed to have an unavailability of 10^{-3} or less.

C.7 Each special safety system shall:

(a) be designed to provide assurance that the system performance will permit the safety functions in requirement C.4 to be fulfilled;

(b) be sufficiently physically and functionally separate from the other special safety systems and from the process systems and sufficiently diverse to ensure that credible cross-linked, common-cause and common-mode failures do not prevent the requirements of C.6 from being met;

(c) have support systems (electrical, air, water, etc.) with reliability and independence requisite to meet the requirements of C.6, C.7(a) and C.7(b);

(d) be capable of being tested at a frequency adequate to demonstrate the unavailability requirement of C.6 with reasonable confidence;

(e) have sufficient redundancy that, in general, no credible failure of a single component precludes its proper operation.

C.8 Where a special safety system employs, or is divided into, sub-systems and these sub-systems are considered to be independent for the purpose of the safety analyses, the design of each sub-system shall meet the requirements of C.7.

C.9 The special safety systems and their support systems shall be designed so that they can reliably perform their designated functions while subject to conditions caused by those failures of the process systems or other special safety systems following which they are required to act.

C.10 The special safety systems shall be designed to be automatically initiated and to require no immediate operator action while permitting operator initiation and operator intervention where necessary to ensure or enhance safety.

C.11 The design shall provide for adequate trip margins, i.e., the interval between initiation of special safety system action and failure points of a system or component shall be based on directly-applicable experimental evidence or a conservative extrapolation of available data.

C.12 A means shall be included in the design for cooling the nuclear fuel in the event that the primary heat sink is unavailable, while the normal pressure boundary of the primary cooling system remains intact.

C.13 The plant shall be designed so that it can continue to operate safely or can be placed and maintained in a safe shutdown state during and after any external or internal event that could credibly be predicted to occur at its particular site. As one of the measures taken, there shall be two physically-separate locations from which the reactor can be shut down, services essential to safety maintained, and the safety state of the plant monitored.

C.14 Appropriate provisions shall be made for the protection of plant personnel in the event of any credible failure. Personnel access to required areas shall not be precluded as a result of conditions caused by a failure.

C.15 The design shall employ sufficient redundancy and diversity so that the radiological dose limits stated in section A and the safety objectives of section D can be met with a high degree of assurance.

C.16 The design should render the plant tolerant to faults, with the response of the plant to postulated faults being in the following order of desirability: (i) no significant, safety-related effect; (ii) change towards safer condition; (iii) safe condition maintained or restored by action of continuously available and operating systems, (iv) safe condition restored by action of a special safety system.

C.17 There shall be sufficient and appropriate instrumentation, with sufficient redundancy and diversity, to provide reliable information needed for the the safe control of the nuclear power plant at all times, including periods following failures, internal or external events.

C.18 The plant shall be designed so as to facilitate periodic inspection and maintenance of process systems and equipment.

C.19 The design of the plant, including the control room, shall take into account ergonomic principles and data.

C.20 The design of the plant shall provide appropriate measures to enable prevention of unauthorized access to, or interference with, safety-related structures, systems or components.

D. Safety Analysis

D.1 All methods, models and data used in safety analysis must be based on sound, relevant theoretical, experimental and/or operational knowledge.

D.2 The designer shall develop a list of potential failure sequences to be analyzed, using a systematic method of identification of such sequences, for the demonstration of conformity with requirement D.4.

D.3 To the extent practical, potential failure sequences shall be analyzed in a realistic manner. Where realistic analysis is not feasible, sets of sequences having similar characteristics should be identified and a bounding case analyzed.

D.4 The risk estimated from analysis of the failure sequences defined according to requirement D.2 shall be judged by reference to Table 4. (Figure 1 shows Table 4 plotted as a histogram.) As indicated in Table 4, the predicted probabilities of failure sequences having consequences within each dose equivalent interval shall be summed.

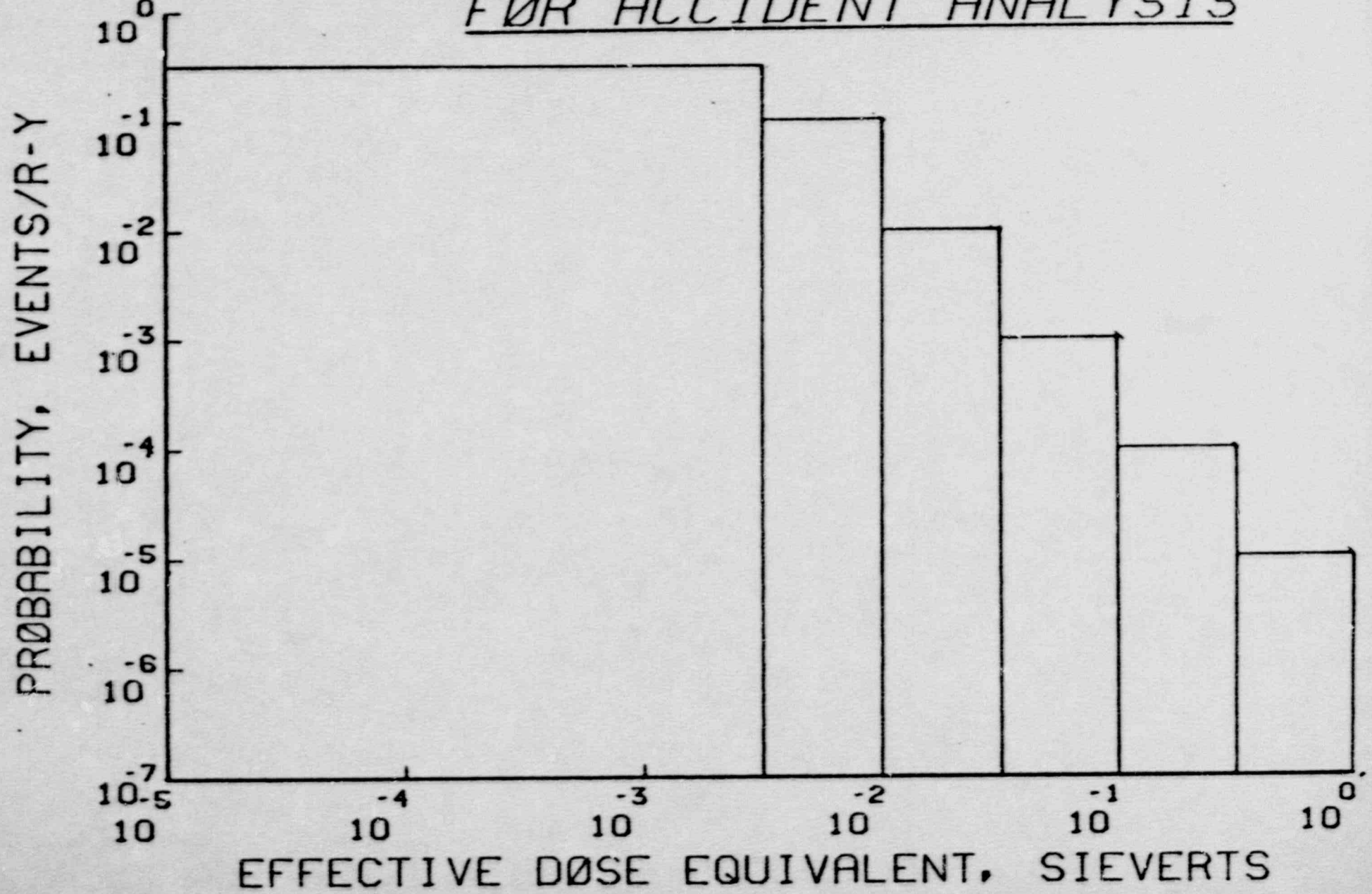
(a) If the sums lie below the limits in all the dose-equivalent intervals, in the third column in Table 4, the estimated risk is acceptable.

TABLE 4

Proposed Risk Categories for Accident Analysis

Category	Individual Effective Dose Equivalent Interval, Sieverts	Sum of the Probabilities of Occurrence of Failures within the Corresponding Effective Dose Equivalent Interval (Per Reactor Unit per year)
1	$0 - 10^{-2.5}$	3.33×10^{-1}
2	$10^{-2.5} - 10^{-2}$	10^{-1}
3	$10^{-2} - 10^{-1.5}$	10^{-2}
4	$10^{-1.5} - 10^{-1}$	10-3
5	$10^{-1} - 10^{-0.5}$	10^{-4}
6	$10^{-0.5} - 1$	10^{-5}

FIGURE 1 PRØPØSED RISK CATEGØRIES FØR ACCIDENT ANALYSIS



(b) If the sum in any dose-equivalent interval lies above the limit, in the third column of Table 4, the estimated risk is generally not acceptable.

(c) In the case described in D.4(b), the AECB may accept the situation, provided that the total of risk to an individual member of the public from all the accident sequences described in requirement D.2 is equal to or less than that corresponding to the summation of the limiting risks of all the accident categories of Table 4. In making this judgement, the AECB shall consider consequence (dose)intervals, uncertainties in consequence and probability estimates, conservatism and other factors and should ensure that the total calculated risk is as low as practicable.

D.5 The consequences of any single event or of a sequence of events on the list defined by requirement D.2 having a probability estimate less than 10^{-7} per reactor unit per year need not be included in this analysis.

D.6 In calculating dose equivalents for the purpose of requirement D.4, realistic meteorological or dispersion conditions and accepted relationships between exposure or intake and effective dose equivalent shall be used.

E. Construction

E.1 Construction of the plant, including manufacture of all safety-related components, shall employ proven or specifically-approved processes and procedures, and be in accordance with appropriate codes and standards.

E.2 Construction of the plant and manufacture of components shall be in accord with recognized quality assurance and quality control principles and standards.

E.3 Design features which permit periodic inspection and maintenance must not be compromised by the construction methods employed.

F. Commissioning

F.1 A detailed, comprehensive, documented program shall be prepared and followed to demonstrate that all components, systems and structures relevant to safety meet, or can meet, the design intent.

F.2 Prior to the nuclear reactor being made critical for the first time, there shall be documented evidence that the safety systems are fully operable and can meet their design requirements.

F.3 The actual state or behaviour of all components, systems and structures relevant to safety, as determined by the commissioning program, shall be appropriately documented to provide a basis for subsequent tests and inspections during the plant's life.

G. Operation

G.1 The primary responsibility for ensuring safety during the operation of a nuclear power plant shall lie with the licensee and the members of its staff, as appropriate.

G.2 The licensee's organization shall include a group that is responsible for auditing all safety related aspects of the operation of the plant. This group shall be distinct from those primarily responsible for operation and shall report to senior management.

G.3 Members of the operating and maintenance staff shall have qualifications and training appropriate to their functions and there shall be an active system for continually monitoring and up-dating, as necessary, their qualifications and training.

G.4 Notwithstanding requirement G.3, all staff at a nuclear power plant shall receive periodic training in safety and radiological protection.

G.5 The regular operating staff complement shall be sufficient to permit adequate manning of the plant at all times and to preclude the need for temporary additional staff to meet individual dose limits other than in exceptional circumstances.

G.6 Operation shall be governed by pre-determined general written procedures.

G.7 Acceptable operating bounds shall be defined for all important safety-related parameters and clear procedures shall be defined for responding to excursions of such parameters outside these bounds.

G.8 All special safety systems and safety-related components shall be inspected and tested periodically, according to a specified program, to demonstrate continued adherence to requirement C.6.

G.9 Plans shall be in existence for dealing with emergencies having effects inside or outside the plant, and such plans shall be tested periodically in accordance with realistic procedures.

G.10 The licensee shall establish guidelines on maximum radiation exposure to workers in emergency situations for approval by the AECB.

H. Effluent and Waste Management

H.1 Radioactive materials in gaseous or liquid effluents shall only be released under approved conditions and any such release shall be monitored and controlled to ensure compliance with the requirements of section A.

H.2 No radioactive materials shall be disposed of at the plant site except in accordance with requirement H.1 or as specifically approved by the AECB.

H.3 Any arrangements for storage of radioactive waste at a nuclear power plant shall include appropriate provision for shielding, heat removal, physical security and retrievability.

I. Decommissioning

I.1 The design, construction and operation of a nuclear power plant shall be such as to facilitate its decommissioning and dismantling after its useful life with the aim of minimizing the surveillance necessary and the time before the site can be returned to a radiologically-safe condition.

I.2 Plans shall be outlined for the restoration of the site to a radiologically-safe condition following the end of the useful operating life of a nuclear power plant. These outline plans shall be prepared during the design and be up-dated as necessary thereafter.

4.0 COMMENTARY ON PROPOSED REQUIREMENTS

The rationale for, or explanations of, the proposed requirements are provided in this section of the report, organized under the same headings as those used in section 3.0 of the report.

A. Radiological Dose Limits for Normal Operation

Requirement A.1 is a basic statement that the regulatory limits for the effective dose equivalent and committed effective dose equivalent received by an atomic radiation worker at a nuclear power plant or to a member of the public affected by the plant shall be met.

Requirement A.2 states the level, based on experience, of the extent to which doses to a member of the general public can be limited through the application of the ALARA principle to CANDU nuclear power plants. In accordance with the ALARA principle, the statement of this target level does not imply that further methods of reducing exposure should not be taken, where such methods are readily available and not unduly costly. Conversely, if a thorough and conscientious application of the ALARA principle has been made in the design and operation of a plant, levels above the stated target may be acceptable.

Requirement A.3 states the necessity of applying the ALARA principle to radiation doses received by atomic radiation workers at a nuclear power plant. As stated in section 1.0 of this report, it is incumbent on the owner of the plant to establish and enforce the ALARA approach for limiting doses to its workers.

In applying requirements A.1 to A.3, accepted methods (18) should be used in estimating effective dose equivalents and committed effective dose equivalents to the members of the public and to atomic radiation workers.

Population (collective) dose limits are not stated in the proposed requirements, recognizing that, in general, conformity with individual dose limits will ensure that population doses are acceptable and that the difficulty of calculating total population doses in a reliable manner during normal operation precludes the meaningful specification of their limits. However, proposed requirement B.2 specifies that estimated population or collective doses are to be considered on

a relative basis in the process of site selection.

Radiological dose guidelines for accident conditions are given in section D.

B. Siting

While the location of a nuclear power plant may not affect its safety directly, the characteristics of a site can influence the design, affect the consequences of an accident and constrain mitigating actions.

The proposed requirements of section B are intended to ensure that the selected site is appropriate for a nuclear power plant and that the site itself does not impose excessive design requirements on the plant. As noted above, requirement B.2 stipulates that population doses shall be considered as one of the factors in the selection of a site. Other factors being equal, the site with the lowest population dose commitment shall be favored.

Requirements B.3 and B.4 are intended to ensure that anticipated natural and man-made external events, including earthquakes, at the chosen site will not preclude or make unduly difficult the safe design and operation of the plant. It is not intended that an exhaustive analysis of the effects of an earthquake on the entire region in which a nuclear power plant is sited will be required, but that reasonable efforts will be taken to ensure that the site will not make it unduly difficult to meet this requirement.

The principle stated in requirement B.4 should not be taken to imply that plants should be located in densely populated areas rather than in those remote from population centres.

It is assumed that many other requirements than those relating directly to safety considerations, such as environmental and socio-economic effects, will be taken into account in the selection of a nuclear power plant site.

Obviously, the actual design of a nuclear power plant must take into consideration the effects of man-made and natural external events at the chosen site. This necessity is covered in requirement C.13.

C. Design

The safety of a nuclear power plant depends on a number of factors, a most important of which is design. The proposed design requirements in section C reflect safety concepts that have evolved in Canada and elsewhere and represent well-established and prudent practice, as called for in requirement C.1

Requirement C.2 recognizes that the best means of assuring the safety of the public and workers is to ensure that accidents do not occur or that their probability of occurrence is made as low as reasonably possible.

Requirement C.3 recognizes that there will be no significant hazards to workers or the public if the fission products are retained within the fuel elements and explicitly calls for the "defence-in-depth" provided by multiple barriers to the release of fission products.

Requirement C.4 recognizes that it is essential that certain safety functions be provided in a nuclear power plant to cope with failures of the plant process systems.

While the proposed safety requirements incorporate, in section D, more comprehensive risk criteria than those of the Siting Guide (14,15), certain deterministic design requirements are retained to assure defence-in-depth against potential accidents. Foremost among these requirements are those for the special safety systems listed in requirement C.5 whose purpose is to ensure that the safety functions can be fulfilled with adequate effectiveness and reliability. Requirement C.5 states the need for two independent shut-down systems, an emergency coolant injection and re-injection system and a containment system. The reference to re-injection of the emergency coolant covers provision for recovery from the building sumps of the discharged emergency coolant and its re-injection into the primary heat transport system in the "re-circulation" phase of the emergency cooling function.

Requirement C.6 retains the present unavailability criterion for special safety systems. It is recognized that this unavailability criterion is an operational target value. For reporting purposes, a special safety system is usually considered as unavailable when it is not 100 per cent effective, although it may still be able to fulfill its safety function adequately. Such considerations should be taken into account in determining whether the special safety system is

actually meeting its unavailability target and in the safety analysis process, as described in section D. The target unavailability must be capable of being demonstrated as specified in requirement C.7 (d).

Requirement C.7 (a) shall be interpreted to mean that the design of each special safety system will ensure that it can meet its required performance, when called upon to do so, with adequate reliability.

It is important to recognize the distinction between a safety function as described in requirement C.4 and a special safety system as described in requirement C.5. It is recognized that special safety systems will require support systems and that safety functions will, in some cases, require the use of process system components, such as the use of headers, feeders and coolant circulating pumps in the overall emergency cooling function. The design requirement in these cases is specified in requirements C.6 and C.7 (a), (b) and (c).

The general design requirements for the special safety systems, as stated in C.7 (a) to C.7 (e), are consistent with present practice.

Requirement C.8 recognizes that a special safety system may be composed of separate sub-systems, such as various parts of the containment system, e.g., ventilation dampers, dousing system, etc. When such a separate sub-system is considered to be independent for the purpose of safety analysis, the design of the sub-system must meet the criteria for special safety systems as stated in requirement C.7. It is recognized, of course, that certain sub-systems form an integal part of the special safety system concerned, and they cannot really be "physically separate" from it, as stipulated in C.7 (b). However, the intent of C.7 (b) in this case is to ensure that the unavailability criterion of C.6 can be met.

The purpose of requirement C.9 is to ensure that a special safety system can perform its required function under conditions that may result from failures of process systems or other special safety systems for which the special safety system in question is designed to cope.

Requirement C.10 specifies that special safety system action be automatically initiated in response to appropriate signals as called for in requirement C.17.

However, requirement C.10 does not preclude operator intervention under appropriate conditions, such as manual trip actuation or the initiation of the recirculation phase of the emergency core-cooling function.

Requirement C.11 states the necessity of setting appropriate trip points for various reactor measurements which have safety roles. The trip points shall be set so as to reduce the probability of damage to any system or component which could lead to radioactive releases.

Requirement C.12 states that an auxiliary or stand-by cooling system is required to ensure that a heat sink is available should the normal heat sinks for the primary coolant system, the steam generators, be unavailable.

Requirement C.13 is intended to ensure the safety of the nuclear power plant under foreseeable internal and external events such as earthquakes, fires, etc. It embodies, in the requirement for two separate control locations, the Two-Group Concept now used in CANDU reactor power plant design (e.g., 20).

Requirement C.14 emphasizes the need to ensure the safety of power plant personnel and to ensure that workers can have access to all areas required to ensure plant safety following a component or system failure.

Requirements C.15 to C.19 represent good engineering practice and are consistent with present approaches to reactor design in Canada.

Requirement C.20 states the need to take into account at the design stage the necessity of making nuclear power plant sabotage as difficult as reasonably possible. An attempt at sabotage would generally require a detailed knowledge of plant design and layout which is difficult to obtain by an outsider. Staffing the plant with suitable personnel should be effective in reducing the probability of success in an attempt at sabotage. The ACNS believes that nuclear power plant safety requirements, as specified in this report, coupled with reasonable security measures, will limit the risk of sabotage to a small fraction of the total risk of the power plant.

D. Safety Analysis

The criterion proposed here for the safety of a nuclear power plant is that the

total estimated radiological risk to the public from accident conditions shall not exceed significantly the risk for normal operation. To ensure that the design provides adequate safety, analyses of the consequences and probabilities of potential failures must be done. The conditions and methods to be used in these analyses are stated in this section.

Requirement D.1 covers probability as well as physical analyses. Probability values used should be based on direct experience or reasonable extrapolations therefrom.

As described in requirement D.2, it will be the responsibility of the designer to develop a list of potential fault sequences for analysis, to be submitted to the AECB at an appropriate time.

Requirement D.3 states that failure sequences should be analyzed in a realistic manner, whenever possible. Consistent with this approach, all analyses should include error estimates in both physical and probability terms. When bounding analyses are neccessary, the probabilistic estimates should recognize that such is the case.

The risk to the public estimated from the analyses of the failure sequences on the above list shall be judged with reference to the accident categories given in Table 4, according to the procedure described in requirement D.4.

These accident categories were established by considering the fundamental risk criterion stated above, the existing single-failure/dual-failure criteria of the Siting Guide (14,15), the recommendations of the IOWG (16) as well as other information (e.g., 21). The definitions of the categories take into account risk aversion for higher-consequence failures.

The accident categories of Table 4 are to be used to judge the acceptability of the predicted results of accident sequences. While requirement D.3 states that the analyses of accident sequences shall be done as realistically as possible, it is recognized that it will not be possible to analyze all potential accident sequences, that complete realism of the analyses cannot always be achieved and that conservative, bounding analyses will be required in many cases. Thus, the probabilities and the consequences associated with the categories should not be interpreted as representations of the actual accident behavior to be expected from a power reactor. They have been established to provide a basis for the acceptance of the design of a nuclear power plant, not to provide a prediction

of future behavior.

The permitted maximum consequences in each category are expressed in terms of effective dose-equivalents, following the latest recommendations of the ICRP (18). This approach eliminates the need for defining limits for thyroid doses.

The categories in Table 4 are based on defined consequence intervals of equal effective dose-equivalent ratios (except for category 1). Each category of dose-equivalent interval has an upper limit value of the permitted sum of the probabilities of mutually-exclusive failure sequences within the category. The acceptability of the predicted results of accident sequences is to be judged as follows:

a) if the sums lie below the limit values in all the categories, the estimated total risk is acceptable

b) if the sum in any category lies above the upper limit value, the estimated risk is generally not acceptable

c) In the case described in item b) above, the AECB may accept the situation, provided that the maximum expected value of risk to an individual member of the public from all the accident sequences described in requirement D.2 is equal to or less than that corresponding to the summation of the limiting risks of all the accident categories of Table 4. (See Table 5). In making this judgment, the AECB should consider the consequence level of the particular consequence interval or intervals involved, uncertainties in physical data, adequacy of analytical models, uncertainties in probabilistic models and data, conservatisms in the analysis, economic and social factors and any other factors which might affect the analysis. The AECB should also ensure that the total calculated risk is as low as practicable and should ensure that the risk-aversion aspect* of the categories is maintained to the extent practicable.

---

*See p. 31

TABLE 5

Calculated Maximum
Values of Risk to Most Highly
Exposed Individual in the Population

ACCIDENT SEQUENCES

Criterion	Risk, Sieverts/Reactor year *
ACNS-4:	2.5×10^{-3}
IOWG Recommendation	1.6×10^{-4}
AECB Siting Guide (Single Failure/Dual Failure)	1.8×10^{-3}**

NORMAL OPERATION

Criterion	Risk, Sieverts/Plant year
ALARA Target	5.0×10^{-5}
Regulatory Limit	5.0×10^{-3}

BACKGROUND RADIATION

Source	Risk, Sieverts/Year
Natural Sources (indoor and outdoor) (Ref. 23)	10^{-3}

*The risk values given are conservative since they assume that all accident sequences in a given category are at the upper consequence limit of the category.

**The calculated maximum risk corresponding to the AECB Siting Guide criteria is more of a nominal value than that corresponding to the present recommendations because of the greater use of deterministic and arbitrary methods in the Siting Guide.

Since the total probability of all events within an accident category must be judged against the acceptance limit, an iterative process by the designers and analysts will be necessary in general.

The limiting probability for Category 1 is set at 3.33×10^{-1} (1 in 3 years) to keep the summation of probabilities in this category equal to the maximum permissible probability for single-failure events in the AECB Siting Guide (14, 15).

The proposed accident categories are shown plotted in the form of a histogram in Figure 2. Figure 2 also compares the single-failure and dual-failure criteria of the Siting Guide to the proposed risk categories. It can be seen from Figure 2 that the limiting probabilities of categories 2 and 5 are somewhat less than the maximum frequencies for single-failures and dual-failures, respectively, as stated in the Siting Guide.

In Figure 2, a line is drawn through the higher ends of the consequence categories for the limiting probabilities. This line can be interpreted as approximating a complementary cumulative distribution function (CCDF) as explained in reference 22. Appropriate integration of this function provides a quantitative measure of the expected risk of a nuclear power plant (22).

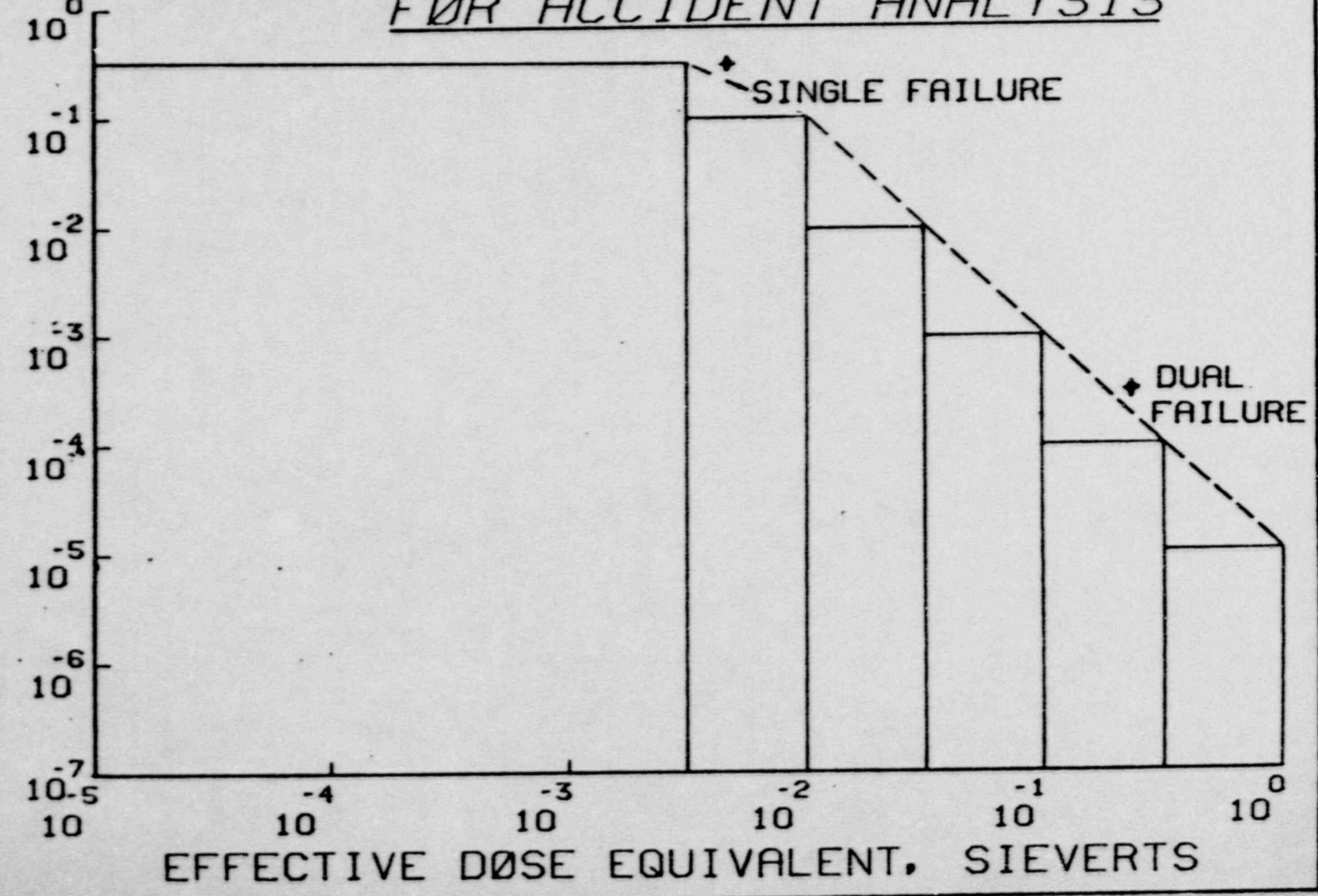
The limit line in Figure 2 has a slope of -1 from category 1 to category 2, i.e., each of these categories represent equal risks. For the remaining categories, the limit line has a slope of -2, thus providing a risk aversion effect as the accident consequences increase.

The maximum value of the overall risk for the six categories is given in Table 5, where it is compared to the expected values of the risk given by the IOWG recommendations and that corresponding to the AECB Siting Guide*, as well as

---

* See footnote in Table 5 concerning maximum risk corresponding to the Siting Guide criteria.

FIGURE 2 PROPOSED RISK CATEGORIES FOR ACCIDENT ANALYSIS



the risks associated with normal operation at the regulatory limit and the ALARA target. It can be seen that the proposed accident sequences risk is of the same magnitude as the risk from normal operation at the regulatory limit. It is emphasized that generally a nuclear power plant will be judged acceptable only if the risk distribution indicated by the categories of Table 4 is satisfied, as stipulated in section D.

Of course, in considering Table 5 it must be recognized that it will not be possible to identify and analyze all possible accident sequences. (Requirement D.2 recognizes this fact by specifying that the designer is to develop a list of failure sequences to be analyzed). Also, failure sequences with probabilities less than 10^{-7} will not be included in the analyses, as specified in requirement D.5. Furthermore, as stated earlier, complete realism of the analyses cannot always be achieved and bounding analyses will be required in many cases. For all these reasons, the value of overall risk from reactor accidents, determined as described, cannot be the real overall risk from accidents. Therefore, ensuring that this calculated risk is less than the maximum risk specified in Table 5 will not necessarily ensure that the real risk of reactor accidents is less than this value. Nevertheless, the ACNS expects that, with a conscientious effort to identify and analyze potential accident sequences, using bounding analyses where necessary, the calculated risk will be of the same order as the real risk. (For the reasons given later, the neglect of accident sequences of probability less than 10^{-7} should not have any significant effect on the calculated or the real risk). ACNS also expects that, as experience with, and knowledge of, reactor operation and risk analysis grows, the differences between the calculated and the real risk will diminish.

To provide further perspective on the calculated maximum value of risk resulting from the these recommendations, it is pointed out that naturally-occuring background radiation in Canada exposes individuals to an average dose equivalent of about 10^{-3} Sieverts per year (23). Since each individual receives this dose, on the average, the associated risk is also 10^{-3} Sieverts per year. This value is also shown for comparison in Table 5. We may conclude that the proposed criteria for the expected risk from accident sequences results in a risk to the most highly-exposed individual in the general public which is of the same order as that resulting from natural background radiation.

The cut-off probability recommended in requirement D.5 is 10^{-7} per reactor year, the same as that recommended by the IOWG. A nuclear power plant design will be judged as acceptable if the probability of a postulated event or sequence of events is 10^{-7} or less per reactor year whatever the potential effective dose equivalent. As discussed below, the ACNS believes that accident sequences with a probability of 10^{-7} or less per reactor year will make no significant contribution to the total expected value of risk to the public. However, reasonable assurance should be given by the designer to the AECB that such is the case.

A justification for the cut-off is that the most comprehensive generalized studies of reactor risks, the Reactor Safety Study (Rasmussen Study) in the USA (24) and the German Risk Study (25) show that overall late-fatality risk curves for light water reactor (LWR) power plants become very steep as the probability of an accident sequence decreases below about 10^{-6} per year for the weighted population densities around nuclear power plants in the USA and the Federal Republic of Germany. This behavior indicates relatively small contributions to overall risk from potential accident sequences of probabilities less than about 10^{-6} per year.* This behavior also implies an upper limit to the magnitude of the consequences of any reactor accident which is not much greater than that associated with an event with a probability of 10^{-6}.

While no such comprehensive study of CANDU reactor risks has been undertaken, various studies of severe accident conditions in CANDU reactors indicate that there will be no fuel melting even for a serious loss-of-coolant accident combined with ineffective emergency coolant injection (e.g., 26). This is not the case for light water reactors. Considering the requirements for two independent safety shut-down systems in CANDU reactors, the probability of melting of the core resulting from reactor transients is also expected to be lower in CANDU reactors than in LWRs. Thus, it would be expected that the total probability of core melting would be less for a CANDU than for an LWR. Since the Reactor Safety Study and the German Risk Study show that there is no significant hazard to the public unless core melting occurs, it is concluded that the overall risk associated with accident conditions in a CANDU will not be

---

* Note that these probabilities are associated with 100 reactors in the US study and 25 reactors in the German study.

greater than that associated with accident conditions in an LWR, particularly considering the lower average population density in Canada than in the USA or West Germany. Therefore, the use of such information from the American and German risk studies to support this safety criterion for CANDU reactors is believed to be justified.

A practical consideration in the stipulation of a cut-off limit is that the analysis of accident sequences of very low probability becomes extremely difficult and the results will be very speculative. Thus, it is doubtful that the analysis of such events would be meaningful; requiring such analysis could divert attention from more-probable events which are the major contributors to the overall risk.

In requirement D.6, the use of realistic meteorological or dispersion conditions in calculating dose-equivalents means that the probabilities of various weather conditions shall be taken into account to establish the most probable dose-equivalent.

E. Construction

Construction, which in this context includes manufacturing of components, represents the execution of the design and therefore must be done in a manner to ensure that the design requirements are met.

Requirements E.1 and E.2 require good manufacturing and construction practice and appropriate quality assurance and quality control methods.

Requirement E.3 is intended to ensure that field construction methods, e.g., the arrangement of pipe runs, do not interfere with the requirement for access for periodic inspection and maintenance.

F. Commissioning

Commissioning includes all those tests, examinations, and other activities conducted prior to commercial operation to ensure that the plant, as constructed, meets all the design requirements.

The safety-related aspects of the commissioning program are covered in requirements F.1 to F.3.

G. Operation

During operation of a nuclear power plant, continued attention is necessary to ensure that the reactor remains within safe limits and that all components, systems, and structures can meet their safety-related requirements.

Requirement G.1 emphasizes the primary responsibility of the licensee for the safe operation of a nuclear power plant.

Requirement G.2 states the need for an independent group in the licensee's organization to audit all safety-related aspects of the operation of a nuclear power plant.

Requirement G.3 covers qualifications and training of atomic radiation workers at a nuclear power plant. The qualifications of these workers will require periodic monitoring, and up-dating as necessary.

Requirement G.4 recognizes that all staff at a nuclear power plant will require periodic training in safety and radiological protection.

The intention of requirement G.5 is to ensure that operating procedures are such as to preclude the use of non-radiation workers as radiation workers unless required by exceptional circumstances.

Requirement G.6 states the need to establish, before a nuclear power plant begins operation, broad administrative controls to ensure appropriate approval of operating actions and of detailed operating procedures.

The operating bounds and procedures specified in requirement G.7 are to be defined by the licensee, since these actions fall within his responsibility for safe operation of the plant, as stated in requirement G.1.

Requirement G.8 specifies the need for periodic inspection and testing of all special safety systems and safety-related components to provide an ongoing assurance of their quality and reliability.

Requirements G.9 and G.10 specify the need to develop plans and guidelines for application in the event of emergency conditions.

H. Effluent and Waste Management

All radioactive wastes from nuclear power plants must be managed to ensure that the consequential effect on people and the environment is within regulatory or prescribed limits and is as low as reasonably achievable. The long-term management of high-level radioactive waste shall employ special facilities. These facilities must be specifically approved for that purpose.

Requirement H.1 governs the control and monitoring of gaseous or liquid releases under normal conditions. It stipulates that the releases must result in doses to the public which meet the requirements of section A.

Requirement H.2 governs arrangements for the disposal of radioactive materials in a manner that renders them irretrievable.

Requirement H.3 establishes criteria for the storage of radioactive waste at a nuclear power plant.

Releases of non-radioactive wastes from nuclear power plants shall be within the limits prescribed by the appropriate authorities.

I. Decommissioning

The eventual need to be able to place and maintain a nuclear power plant in a safe state at the end of its useful life and, eventually, if necessary, to restore the site to unrestricted use should be borne in mind during design, construction and operation.

Requirements I.1 and I.2 are intended to achieve these goals. It is not anticipated that these requirements will present major difficulties considering the world-wide experience already gained from the decommissioning of nuclear power plants.

5.0 GLOSSARY OF TERMS

Absorbed Dose - The quotient obtained by dividing the amount of energy absorbed in the body, or in an organ or tissue of the body, due to ionizing radiation by the respective mass of the body, organ or tissue. It is expressed in Grays where one Gray is equal to one Joule per kilogram.

ALARA - A basic principle of radiation protection that specifies that radioactive discharges from nuclear power plants and radiation exposure to persons be kept as far below regulatory limits as is reasonably achievable taking into account the state of the technology and the economics of improvement related to benefits to public health and safety and other societal and socio-economic considerations and to the utilization of nuclear energy in the public interest.

Anticipated Operational Occurrences - All operations deviating from normal conditions beyond specified operational limits and conditions which may be expected to occur once or several times during the operating life of the plant and which do not cause any significant damage to the special safety systems and to safety-related equipment and systems and do not lead to failure sequences as defined in article D.2.

Atomic Radiation Worker - Any person who in the course of his work, business or occupation is likely to receive a dose of ionizing radiation in excess of any dose specified in Column IV of Schedule II of the regulations (SOR/74-334, Canada Gazette, Part II, Volume 108, No. 12, June 4, 1974, as amended) made pursuant to the Atomic Energy Control Act.

CANDU - A Canadian-developed nuclear power reactor system which uses a pressure tube reactor, heavy water moderator and natural uranium fuel with on-power re-fuelling.

Collective Dose - See Population Dose.

Committed Dose Equivalent - The dose equivalent to a given organ or tissue that will be accumulated over 50 years, representing a working life, from a single intake of radioactive material into the body.

Common Cause Failure - The failure of two or more components to perform their functions as a result of a single specific cause or event.

Common Mode Failure - The failure of two or more components in an identical manner.

Credible Fault - A failure of a component or system that could occur under reasonable physical assumptions, with a probability high enough to require analysis.

Cross-Linked Failure - A failure of one or more components resulting from the failure of another component.

Deterministic - When applied to safety design and analysis, a method that explicitly ignores the probabilities of various event sequences.

Disposal - The placing of nuclear waste in a facility which does not allow for its retrieval and is designed to ensure that any release of radioactivity or radioactive substances from the facility does not present a serious hazard to the public.

Dose Equivalent - The product obtained by multiplying the absorbed dose in the body, an organ or tissue by a quality factor to account for the different potential for injury of different types of radiation, and by a factor representing all the other modifying factors recommended by the ICRP. It is expressed in Sieverts. Dimensionally, the Sievert is equivalent to a joule per kilogram.

Dose Equivalent Commitment - The infinite time integral of the average dose-equivalent rate from a given practice to a given organ or tissue for a specified population.

Effective Dose Equivalent - The sum of the dose equivalents, in Sieverts, for each of the various organs or tissues multiplied by an appropriate weighting factor for each organ or tissue. The weighting factors, as recommended by the ICRP (18), ensure that the detriment is equal whether the whole body is irradiated uniformly or whether there is non-uniform irradiation of the body.

Ergonomics - The discipline dealing with the interaction of human beings with technological systems - "person-machine interaction".

External Event - A natural or man-made event, originating outside a nuclear power plant which may affect the safety of the plant, e.g. an earthquake, flood, storm, aircraft crash.

Failure Points or Conditions of a System - Parameters characterizing a state of a system in which failures to fulfill its function will occur.

Internal Event - An event originating within a nuclear power plant which may affect the safety of the plant, e.g. fire, operator error.

Normal Operation - The operation of a nuclear power plant within specified operational limits and conditions, and under anticipated operational occurrences, including starting up, power operation, shutting down, shut down, maintenance and testing.

Normal Activities Associated with a Nuclear Power Plant - Activities other than normal operation including construction, commissioning, moth-balling, decommissioning and dismantling.

Nuclear Power Plant - A thermal neutron reactor or reactors together with all structures, systems and components necessary for safety and for the production of power, i.e., heat or electricity.

Population Dose - The product of the average dose to an individual in a given population and the number of individuals in the population. It is measured in person-sieverts. It is also called Collective Dose.

Probabilistic - When applied to safety design and analysis, a method that takes into account the probabilities of various event sequences.

Probability - A numerical property attached to an activity or event whereby the likelihood of its future occurrence is expressed or clarified.

Process System - A system required for the normal operation of the reactor, e.g. the primary heat transport system, the regulating system.

Public (member of) - Any person who is not an atomic radiation worker.

Risk - The product of the probability of the occurrence of an event and the magnitude of the consequences resulting from the event.

Risk Aversion - The view that a single large-scale accident with severe consequences is more undesirable than many smaller accidents, each of lesser consequences, even when the total aggregated consequences of the many smaller accidents are equal to or comparable to the total consequences of the single large accident.

Safe Shut-down State - The state in which a nuclear power reactor is maintained in a shut-down condition indefinitely such that it is not possible for start-up to occur in a spontaneous manner.

Serious Process Failure - A failure of a process system which in the event of failure of any one of the special safety systems would result in a significant release of radioactive material from a nuclear power plant.

Target - A condition which, by agreement, is to be achieved in so far as possible in the design or operation of a nuclear power plant. It is to be contrasted with a regulatory limit which must be achieved at all times.

Trip-Point - for an instrument is the level of the quantity measured by the instrument which would cause an automatic shut-down of a nuclear reactor.

Unavailability - The fraction of time that a system or component is unable to function as designed because of failure, recognized or not, and repair.

6.0 REFERENCES

1. Safety Objectives for Nuclear Activities in Canada
   Report of the Advisory Committee on Nuclear Safety
   ACNS-2 — June, 1981
   Amended April, 1982

2. Paskievici, W.
   Risks from Energy Production and Supply
   Risk-Risque. Proceedings of a Symposium on the Assessment and Perception of Risk to Human Health in Canada, — October 1982

   J.T. Rogers and D.V. Bates, editors
   Royal Society of Canada, Science Council of Canada — April 1983

3. Cohen, A.V., and D.K. Pritchard
   Comparative Risk of Electricity
   Production Systems: A Critical Survey of the Literature.
   Research Paper No.11
   UK Health and Safety Executive — December, 1980

4. Niehaus, F., and A. Novegno
   Optimal Allocation of Resources for Safety
   Risk-Risque. Proceedings of a Symposium on the Assessment and Perception of Risk to Human Health in Canada — October, 1982

   J.T. Rogers and D.V. Bates, editors
   Royal Society of Canada, Science Council of Canada — April, 1983

5. Hamilton, L.D.
   Comparative Risks from Different Energy Systems:
   Evolution of the Methods of Studies
   Nuclear Safety, 24,2 — March-April, 1983

6. McConnell, L.G., L.W. Woodhead, G.R. Fanjoy
   CANDU Operating Experience, IAEA-CN-42/68
   Proc. of International Conference on
   Nuclear Power Experience, Vol. 2, p. 103
   International Atomic Energy Agency, Vienna — September, 1982

7. Nuclear Industry Review
   Problems and Prospects 1981-2000
   Energy Mines and Resources, Canada — 1982

8. Siddall, E.
Risk, Fear and Public Safety
AECL-7404 April 1981

9. Siddall, E.
Safety Policy in the Production of Electricity
Proc. Int. Meeting on Thermal
Nuclear Reactor Safety, Chicago September 1982

10. Meinel, M.P., and A.B. Meinel
Energy for the Future: The World View
Ann. Nucl. Energy, Vol. 10, No.3/4, p. 209 1983

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

12. Siddall, E., and W.B. Lewis
Reactor Safety Standards and their Attainment
AECL-498 September 1957

13. Siddall, E.
Statistical Analysis of Reactor Safety Standards
Nucleonics, 17, 2, pp. 64-69 February 1959

14. ---------
Reactor Siting and Design Guide
AECB Document November 1964

15. Hurst, D.G. and F.C. Boyd
Reactor Licensing and Safety Requirements
Paper presented at Canadian Nuclear Association Conference
AECB-1059 June 1972

16. -------
Proposed Safety Requirements for Licensing of CANDU Nuclear Power Plants.
The Report of the Inter-Organizational Working Group.
AECB-1149 November 1978

17. Paskievici, W.
Proposed General Principles and Safety Requirements for CANDU Nuclear Power Plants.
Proceedings of Symposium on CANDU Reactor Safety Design
Canadian Nuclear Association November 1978

18. ----------
Annals of the ICRP. Recommendations of the International Commission on Radiological Protection. ICRP Publication 26, Vol. 1, No. 3
Pergamon Press 1977

19. ----------
Licensing Guide No.39. Requirements for the Safety Analysis for CANDU Nuclear Power Plants. (Draft)
AECB Consultative Document C-6 June 1980

20. Webb, J.R.
Protection from Common Mode Events
Proceedings of Symposium on CANDU Reactor Safety Design
Canadian Nuclear Association November 1978

21. Duncan, D.S.,
Conditions of Design for Thermal Reactors, A Revised Approach
Generic Atomic Company, San Diego, California
GA-A14531 August 1977

22. Cox, D.C., and P. Baybutt
Limit Lines for Risk
Nuclear Technology, Vol. 57, p. 320 June 1982

23. Butler, G.C.
Radioactivity in the Canadian Environment
Associate Committee on Scientific Criteria for Environmental Quality
National Research Council of Canada
NRCC No. 18134 1980

24. --------
Reactor Safety Study
An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants
WASH-1400 August 1975

25. --------
The German Risk Study
Summary
Federal Minister of Research & Technology August 1979

26. Meneley, D.A., and W.T. Hancox
LOCA Consequence Predictions in a CANDU-PHWR
Paper 145
IAEA International Conference on Nuclear Power Experience
Vienna September 1982

INFO-0116

ACNS Advisory Committee on Nuclear Safety

CCSN Comité consultatif de la sûreté nucléaire

CCSN-4

EXIGENCES GÉNÉRALES DE SÛRETÉ RECOMMANDÉES POUR LES CENTRALES NUCLÉAIRES

par le

Comité consultatif de la sûreté nucléaire

juin 1983

An Advisory Committee of the Atomic Energy Control Board of Canada – Secretariat: Ottawa, Canada K1P 5S9

Comité consultatif de la Commission de contrôle de l'énergie atomique du Canada – Secrétariat: Ottawa, Canada K1P 5S9

PRÉFACE

Le présent rapport, soumis à la Commission de contrôle de l'énergie atomique, contient les recommandations du Comité consultatif de la sûreté nucléaire touchant les exigences générales de sûreté relatives aux centrales nucléaires CANDU construites au Canada. Pour élaborer ces exigences, le CCSN a constitué un groupe de travail formé de quelques-uns de ses membres, lors de sa cinquième réunion tenue le 20 janvier 1981. Dans l'élaboration des exigences générales de sûreté, le groupe de travail a passé en revue l'évolution de la réglementation canadienne en matière de sûreté des réacteurs; il a consulté les spécialistes de la CCEA, le Comité consultatif de la radioprotection de la CCEA et des représentants de L'EACL et des services publics; il a étudié les exigences de sûreté s'appliquant aux réacteurs nucléaires dans les autres pays; et, il a examiné les développements récents dans les domaines de l'évaluation, de l'analyse, de la perception et de la gestion des risques.

Le groupe de travail a également bénéficié des points de vue des autres membres du CCSN. Lors de sa réunion du 27 juin 1983, le CCSN a approuvé le rapport à soumettre à la Commission de contrôle de l'énergie atomique.

Le groupe de travail comprenait les membres suivants:

J.T. Rogers, président
N. Lind
O.R. Lundell
W. Paskievici
A. Pearson

Le groupe de travail a reçu l'aide de F.C. Boyd, conseiller scientifique à la CCEA.

RAPPORT CCSN-4 - EXIGENCES GÉNÉRALES DE SÛRETÉ RECOMMANDÉES POUR LES CENTRALES NUCLÉAIRES

RÉSUMÉ

Le présent rapport présente les recommandations du Comité consultatif de la sûreté nucléaire pour un ensemble d'exigences générales de sûreté sur lesquelles la Commission de contrôle de l'énergie atomique pourrait se baser pour la délivrance de permis aux centrales nucléaires. En plus d'un certain nombre d'exigences précises recommandées, le rapport comprend des critères d'acceptabilité touchant la conception des centrales. Ces critères sont basés sur la probabilité calculée et sur les conséquences possibles (expositions prévues du public aux rayonnements) des défectuosités potentielles. Enfin, le rapport présente l'historique des principes et des pratiques de la sûreté des réacteurs nucléaires au Canada.

ABRÉGÉ

INTRODUCTION

Le rapport présente les recommandations du Comité consultatif de la sûreté nucléaire (CCSN) à la Commission de contrôle de l'énergie atomique (CCEA) au sujet des exigences générales de sûreté pour les centrales nucléaires CANDU au Canada.

Ces exigences ont pour but

a) de fournir une base pour assurer que les objectifs de sûreté définis à la référence 1 peuvent être atteints dans les centrales nucléaires au Canada;

b) de fournir une base détaillée et cohérente à la CCEA pour la réglementation des centrales nucléaires au Canada; et

c) de fournir une déclaration unifiée des exigences de sûreté concernant les centrales nucléaires au Canada pour le gouverne de toutes les parties intéressées.

Les exigences proposées contiennent plusieurs principes fondamentaux de sûreté des réacteurs nucléaires qui ont été mis au point depuis plusieurs décennies de conception et de pratique du processus d'autorisation au Canada. Parmi les principes les plus importants figurent:

a) le recours à la séparation, à l'indépendance, à la redondance et à la diversité dans la conception;

b) la reconnaissance du fait que la prévention des défaillances du système opérationnel représente un élément fondamental pour assurer la sûreté du réacteur; et

c) l'utilisation judicieuse d'arguments de probabilité dans lesquels les valeurs de non-disponibilité des systèmes ou de fréquence des défaillances doivent se fonder sur l'expérience directe ou sur des extrapolations raisonnables qui en découlent.

En proposant ces exigences, le Comité reconnaît que la responsabilité première de la sûreté d'une centrale nucléaire incombe au propriétaire. Comme corollaire, le Comité considère que l'un des principaux rôles de la CCEA est d'examiner et de vérifier que les exigences qu'elle a établies sont respectées. Les exigences recommandées traduisent ce point de vue. Elles ne représentent pas un écart important par rapport à la pratique passée, mais plutôt une étape dans la mise au point de cette pratique.

HISTORIQUE

Les premiers critères particuliers pour la sûreté et l'autorisation des réacteurs au Canada ont été énoncés au début des années 1960 par Laurence (voir ref. 2) qui proposa que la probabilité d'un accident "désastreux" devrait être inférieure à 10^{-5} par année-réacteur, d'après les données réelles sur la fiabilité des composants. Pour assurer une fréquence aussi faible, il fallait installer des "dispositifs de protection" et "de confinement" qui soient à la fois séparés des systèmes operationnels et indépendants l'un de l'autre. La séparation devait être suffisamment complète pour que la probabilité de défaillances corrélées ou de mode commun soit très faible.

L'approche ci-dessus, utilisant les catégories de défaillances "simples" d'un système opérationel et de défaillances "doubles" d'un système opérationnel et d'un système de sûreté, a été incorporée dans le Siting Guide ("Guide d'emplacement") adopté par le Comité consultatif de la sûreté des réacteurs de la CCEA, en 1964, et toujours principalement en usage aujourd'hui (voir ref. 3). Il ressort donc que la sûreté et l'autorisation des réacteurs au Canada, depuis le début, se basent fondamentalement sur une méthode déterministe mais aussi sur un concept de risque, c'est-à-dire que la probabilité d'un accident désastreux devrait être assez faible pour que le risque correspondant soit également très faible.

Bien que cette approche ait fourni une base raisonnable pour l'examen systématique des aspects de la sûreté des centrales nucléaires CANDU, sa simplicité a entraîné quelques malentendus et difficultés d'application. Ces problèmes ont grandi à mesure que la taille des réacteurs, la puissance

des éléments combustibles et la complexité des systèmes ne cessaient de croître, à côté des connaissances sur le comportement des systèmes, des données expérimentales et des méthodes d'analyse qui connaissaient la même pente ascendante. Le besoin d'une approche plus détaillée a mené, en 1977, à la création d'un groupe de travail interorganisationnel (GTI), composé de représentants de la CCEA, du Comité consultatif de la sûreté des réacteurs, de L'Énergie atomique du Canada, Limitée et des trois services publics provinciaux qui ont un programme d'énergie nucléaire. Le GTI a proposé des principes généraux et des exigences de sûreté qui conservaient l'approche déterministe traditionnelle des barrières multiples en exigeant certains critères et systèmes spéciaux de sûreté, mais étendaient la base probabiliste de l'approche précédente en définissant six catégories d'événements d'après leur probabilité et en augmentant les valeurs des doses de référence individuelles admissibles à mesure que la probabilité diminue.

La CCEA a incorporé certaines recommandations du GTI dans son document de consultation n° C-6 (voir ref. 4) qui tient compte du concept des diverses catégories d'accidents (5, en fait, au lieu des 6 proposées) pour lesquelles les doses de référence individuelles proposées varient entre 5×10^{-4} et 0,25 Sv. Toutefois, ces catégories n'ont pas été définies sur une base probabiliste, mais plutôt selon une méthode déterministe, en regroupant des accidents hypothétiques à partir d'une liste établie d'avance.

EXIGENCES PROPOSÉES

Les exigences générales de sûreté proposées pour les centrales nucléaires sont regroupées sous les rubriques suivantes:

a) limite de dose de rayonnements en cours normal d'exploitation
b) choix du site
c) conception
d) analyse de sûreté
e) construction
f) mise en service

g) exploitation
h) gestion des déchets et des effluents
i) déclassement.

Les exigences proposées font usage du principe ALARA dans le cas d'exploitation normale (voir ref. 1).

Comme la conception représente un des facteurs importants de la sûreté des centrales nucléaires, la plupart des exigences recommandées s'appliquent à la conception et aux analyses nécessaires pour démontrer la pertinence de la conception proposée.

Bien que les exigences de sûreté proposées incorporent des critères de risque plus détaillés que le Guide d'emplacement, certaines exigences déterministes de conception, comme celles qui touchent les systèmes spéciaux de sûreté, sont retenues pour assurer le maintien du principe des barrières multiples en cas d'accidents.

En plus des objectifs de sûreté déjà mentionnés, le Comité soutient le critère que le risque total dû aux rayonnements estimé pour la population à partir de toutes les conditions d'accidents ne devrait pas dépasser de façon importante le risque en cours normal d'exploitation. Pour assurer la réussite de cet objectif, il faut effectuer des analyses des conséquences des défaillances possibles. Le Comité propose que l'acceptabilité du risque estimé à partir de ces analyses d'accidents soit déterminée par une série de catégories de risque indiquées au tableau 1 et illustrées graphiquement à la figure 1.

Ces catégories d'accidents ont été établies en considérant le critère fondamental de risque susmentionné, les critères existants de défaillance simple ou double du Guide d'emplacement, les recommandations du GTI et d'autres données diverses. La définition de chaque catégorie tient compte de l'atténuation du risque dans le cas des défaillances plus lourdes de conséquences.

Chaque catégorie a un plafond qui représente la somme permise des probabilités de séquences de défaillances mutuellement exclusives à l'intérieur de l'intervalle de l'équivalent de dose effectif. Il faut juger si les résultats prévus des séquences d'accidents sont acceptables ou non d'après les critères suivants:

a) si les sommes se situent en deça des valeurs limites dans toutes les catégories, le risque total estimé est acceptable;

b) si la somme dans une catégorie quelconque se situe au delà de la valeur limite, le risque estimé est inacceptable en général;

c) dans le cas décrit à l'alinéa b) ci-dessus, la CCEA peut juger que la situation est acceptable, pourvu que la valeur maximale prévue du risque à un membre du public, dû à toutes les séquences d'accidents à analyser, soit égale ou inférieure à la valeur correspondant à la somme des risques limites de toutes les catégories d'accidents du tableau 1 (voir tableau 2). En portant ce jugement, la CCEA devrait considérer le niveau de conséquences de l'intervalle ou des intervalles en cause, les incertitudes que comportent les données physiques, la pertinence des modèles analytiques, les incertitudes dans les données et les modèles probabilistes, la prudence des analyses, les facteurs économiques et sociaux et tout autre facteur qui pourrait modifier l'analyse.

Les catégories de risque proposées sont illustrées sous la forme d'un histogramme à la figure 1 où elles sont comparées au critères du Guide d'emplacement.

La valeur maximale du risque global pour les six catégories figure au tableau 2 où elle est comparée aux valeurs de risque selon les recommandations du GTI et à celles qui correspondent au Guide d'emplacement de la CCEA, de même qu'au risque en cours normal d'exploitation à la limite réglementaire et selon le principe ALARA. Il est donc évident que le risque proposé dans le cas des séquences d'accidents est de la même ampleur que le risque en cours normal d'exploitation à la limite réglementaire.

Si la probabilité d'un événement ou d'une série d'événements hypothétiques est de l'ordre de 10^{-7} ou moins par année-réacteur, le Comité recommande de juger cette probabilité comme acceptable, quel que soit l'équivalent de dose possible. Le rapport donne les arguments en faveur de la limite fixée à 10^{-7} par année.

CONCLUSION

Le CCSN est d'avis que les recommandations du présent rapport continueront d'assurer la sécurité adéquate du public et des travailleurs par rapport à l'exploitation des centrales nucléaires au Canada, tout en permettant de profiter des avantages économiques et sociaux de l'énergie nucléaire.

TABLEAU 1

Catégories de risque proposées pour l'analyse des accidents

Catégorie	Intervalle de l'équivalent de dose effectif individuel (en sieverts)	Somme des probabilités de défaillances à l'intérieur de l'intervalle correspondant de l'équivalent de dose effectif (par réacteur par année)
1	0 à $10^{-2,5}$	$3,33 \times 10^{-1}$
2	$10^{-2,5}$ à 10^{-2}	10^{-3}
3	10^{-2} à $10^{-1,5}$	10^{-2}
4	$10^{-1,5}$ à 10^{-1}	10^{-3}
5	10^{-1} à $10^{-0,5}$	10^{-4}
6	$10^{-0,5}$ à 1	10^{-5}

TABLEAU 2

Valeurs maximales calculées du risque au membre du public le plus fortement exposé au sein de la population

SÉQUENCES D'ACCIDENTS Critère	Risque* (sieverts par année-réacteur)
CCSN-4	$2,5 \times 10^{-3}$
Recommandation du GTI	$1,6 \times 10^{-4}$
Guide d'emplacement de la CCEA (défaillance simple et double)	$1,8 \times 10^{-3}$**

EXPLOITATION NORMALE Critère	Risque (sieverts par année-réacteur)
Principe ALARA	$5,5 \times 10^{-5}$
Limite réglementaire	$5,0 \times 10^{-3}$

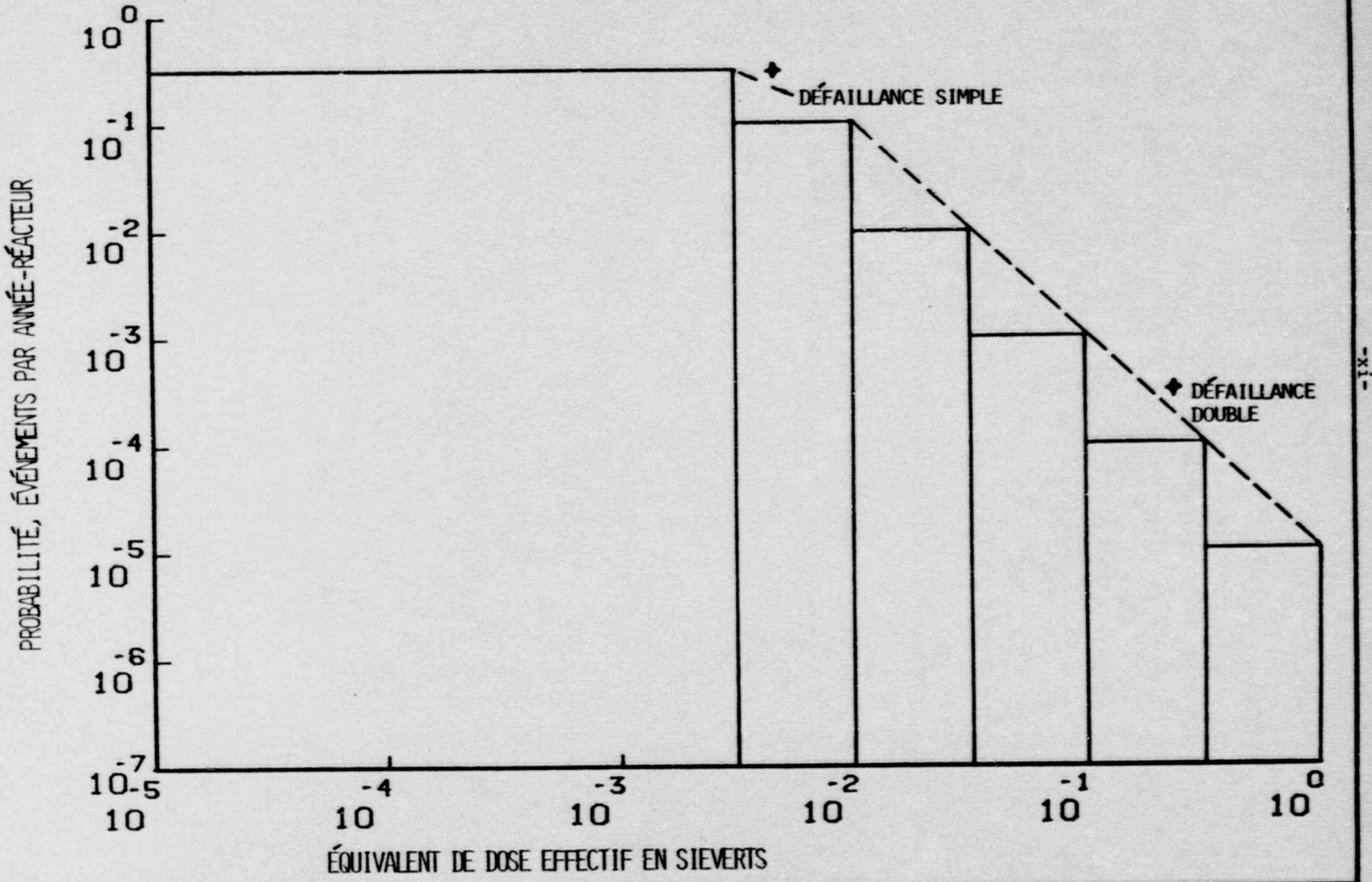
FOND DE RAYONNEMENTS Source	Risque (sieverts par année)
Sources naturelles (à l'intérieur et à l'extérieur) (voir ref. 4)	10^{-3}

---

* Les valeurs de risque sont prudentes étant donné qu'elles supposent que toutes les séquences d'accidents d'une catégorie donnée se situent à la limite supérieure de conséquences de la catégorie en question.

** Le risque maximal calculé correspondant aux critères du Guide d'emplacement de la CCEA représente plutôt une valeur nominale qu'une valeur compatible avec les recommandations actuelles, vu l'emploi plus répandu de méthodes déterministes au arbitraires dans le Guide d'emplacement.

FIGURE 1 CATÉGORIES DE RISQUE PROPOSÉES POUR L'ANALYSE DES ACCIDENTS



Bibliographie

1. CCEA, Comité consultatif de la sûreté nucléaire, "Projet de déclaration de principe sur les objectifs de sûteté relatifs aux activités nucléaires au Canada", document nº CCSN-2, juin 1981, version modifiée d'avril 1982.

2. G.C. Laurence, "Reactor Siting in Canada", L'Énergie atomique du Canada, Limitée, document nº AECL-1375, octobre 1961.

3. CCEA, "Reactor Siting and Design Guide", novembre 1964.

4. CCEA, "Analyse de sûreté des centrales nucléaires CANDU", document de consultation nº C-6 (ancien guide de réglementation nº 39), juin 1980.

INFO-0116

ACNS Advisory Committee on Nuclear Safety

CCSN Comité consultatif de la sûreté nucléaire

CCSN-4

EXIGENCES GÉNÉRALES DE SÛRETÉ RECOMMANDÉES POUR LES CENTRALES NUCLÉAIRES

par le

Comité consultatif de la sûreté nucléaire

juin 1983

An Advisory Committee of the Atomic Energy Control Board of Canada — Secretariat: Ottawa, Canada K1P 5S9

Comité consultatif de la Commission de contrôle de l'énergie atomique du Canada — Secrétariat: Ottawa, Canada K1P 5S9

Table des matières

1.0 INTRODUCTION

L'une des premières tâches confiées au Comité consultatif de la sûreté nucléaire (CCSN), après sa formation en 1980, a été de passer en revue et de commenter les divers guides de délivrance de permis élaborés par les spécialistes de la CCEA. À la suite de son étude et de ses recommandations, le CCSN a été chargé de préparer des documents définissant les objectifs de sûreté applicables à toutes les activités nucléaires au Canada, ainsi que des exigences générales de sûreté pour des activités nucléaires précises. Les objectifs de sûreté ont été définis dans le document de la référence 1.

La Commission de contrôle de l'énergie atomique a approuvé ces objectifs de sûreté et ils font dorénavant partie d'une déclaration de principe de la Commission.

Dans le présent rapport, le CCSN décrit les exigences générales de sûreté qui devraient s'appliquer aux centrales nucléaires* construites au Canada. Lesdites exigences ont pour objectif de:

a) constituer une base pour assurer que les objectifs de sûreté définis dans le document de la référence 1 peuvent être atteints dans les centrales nucléaires au Canada;

b) constituer une base générale et constante pour les règlements de la CCEA en matière de délivrance de permis aux centrales nucléaires du Canada; et

c) fournir une description unifiée des exigences de sûreté applicables au centrales nucléaires du Canada pour l'information de toutes les parties intéressées.

---

* Toute référence aux centrales nucléaires dans le présent rapport doit être comprise comme s'appliquant aux centrales CANDU, à moins d'indication contraire.

Comme on le verra ci-dessous, dans l'élaboration de sa déclaration d'exigences de sûreté, le CCSN a jugé que les centrales nucléaires du Canada qui sont titulaires d'un permis en vertu des critères existants, sont suffisamment sûres, mais que l'application de ces critères a donné lieu à quelques problèmes. Par conséquent, le CCSN s'est donné comme but important, en élaborant les exigences de sûreté, de résoudre ces problèmes et de faciliter le processus de réglementation tout en assurant que les centrales nucléaires continuent de fonctionner de façon sûre.

Les exigences proposées dans le présent rapport renferment de nombreux principes fondamentaux de sûreté des réacteurs ayant été mis au point durant plusieurs décennies d'activités dans le domaine de la conception des réacteurs et de la délivrance de permis. Les principes les plus importants sont:

a) le recours à la séparation, à l'indépendance, à la redondance et à la diversité, à l'étape de la conception;

b) la reconnaissance de la prévention des défaillances du système opérationnel comme élément fondamental servant à assurer la sûreté d'un réacteur; et

c) l'emploi judicieux des arguments de probabilité dans lesquels les valeurs de l'indisponibilité des systèmes ou de la fréquence des défaillances doivent être basées sur l'expérience acquise directement ou sur une extrapolation raisonnable de cette expérience.

Si l'on appliquait avec soin les exigences proposées, les centrales nucléaires en cours normal d'exploitation n'exposeraient les populations environnantes qu'à une petite fraction des limites d'exposition aux rayonnements fixées par des organismes internationaux et adoptées par la CCEA. De plus, le risque encouru par la population à proximité d'une centrale nucléaire, à cause d'accidents provoquées par la défaillance d'un composant ou par une erreur humaine, serait très faible et comparable à celui encouru lorsque le réacteur fonctionne normalement.

Dans l'élaboration de la présente déclaration des exigences générales de sûreté, le CCSN a reconnu que le risque pour la santé encouru par les opérateurs et par le public à cause du cycle complet du combustible associé aux centrales nucléaires actuellement en service au Canada, est comparable, sinon plus faible, que les risques provenant des autres méthodes employées pour produire de l'électricité (voir réf. 2-5). En outre, le CCSN a reconnu les grands avantages économiques et sociaux, directs et indirects, résultant de l'exploitation des centrales nucléaires (voir réf. 6-10). Compte tenu de ces facteurs parmi d'autres, le CCSN a jugé qu'il n'était pas nécessaire de réduire le risque maximal aux opérateurs et au public à cause de l'exploitation des centrales nucléaires, calculé selon le Règlement et les méthodes actuelles de délivrance de permis au Canada. Le CCSN croit que les recommandations contenues dans le présent rapport protégeront le public et les travailleurs de façon adéquate, tout en permettant de profiter des avantages économiques et sociaux de l'énergie nucléaire.

Au cours de ses travaux, le CCSN a reconnu que la première responsabilité en ce qui concerne la sûreté de la conception, de la construction et de l'exploitation d'une centrale nucléaire revient au propriétaire de la centrale. En plus de s'assurer que les limites réglementaires de l'exposition à la radioactivité sont respectées, le propriétaire de la centrale doit veiller à ce que les doses* de rayonnements reçues par le public ou par les travailleurs, dans des conditions normales d'exploitation, soient au niveau le plus bas qu'il soit raisonnablement possible d'atteindre en deça desdites limites, compte tenu des facteurs économiques et sociaux**.

---

* Dans le présent document, le mot "dose" signifie "équivalent de dose" ou "équivalent de dose effectif", selon le contexte. Voir le glossaire à la fin du présent document.

** On appelle généralement principe ALARA (as low as reasonably achievable) cette approche de la radioprotection.

Comme corollaire de la responsabilité assumée par le propriétaire, le CCSN considère que la CCEA a un grand role d'examen et de vérification à jouer pour s'assurer que les exigences qu'elle a établies sont respectées à toutes les étapes des activités reliées aux centrales nucléaires.

Le CCSN suppose que des exigences et des lignes directrices précises de sûreté s'appliquant à la conception, à l'analyse et au fonctionnement des divers systèmes, seront émises par la CCEA pour compléter et clarifier au besoin les exigences générales proposées dans le présent document.

On propose d'appliquer les exigences recommandées dans le présent document à tous les réacteurs de puissance du Canada, dont la construction n'a pas encore été autorisée.

Les exigences proposées dans les pages qui suivent ne s'écartent pas outre mesure de la pratique antérieure, elles constituent plutôt une étape dans la mise au point de ladite pratique, comme cela est décrit à la section 2 du présent rapport. En recommandant ces exigences de sûreté, le CCSN n'insinue pas que la sûreté des centrales nucléaires actuellement en service au Canada est inadéquate ou que les risques encourus par le public et les travailleurs par suite de l'exploitation de ces centrales sont inacceptables. Les recommandations du CCSN ont été élaborées à la lumière de connaissances et d'expériences grandissantes pour indiquer à tous les milieux concernés que les centrales nucléaires construites au Canada ont et continueront d'avoir une sûreté acceptable.

2.0 HISTORIQUE ET ANTÉCÉDENTS DES PRINCIPES ET DES MÉTHODES DE DÉLIVRANCE DE PERMIS POUR LES RÉACTEURS AU CANADA

Les permiers critères de sûreté et de délivrance de permis pour les réacteurs au Canada ont été formulés à la fin des années 1950 et au début des années 1960 par Laurence (voir réf. 11). À la même époque, Siddal et Lewis (voir réf. 12 et 13) ont également fourni une contribution importante à l'élaboration des concepts de sûreté des réacteurs. Laurence énonça que la probabilité d'un accident "désastreux" devrait être inférieure à 10^{-5} par année-réacteur. En outre, cette probabilité allait être basée sur l'expérience réelle de la fiabilité des composants. Pour parvenir à une probabilité de désastre à ce point faible, il fallait recourir à des "dispositifs de protection" et à des "mécanismes de confinement" qui étaient indépendants les uns des autres et séparés des systèmes opérationnels. La séparation devait être suffisamment complète pour que la probabilité des défaillances corrélées ou de mode commun soit très faible.

Cette approche a été incluse dans le premier Siting Guide (Guide d'emplacement) de la CCEA en 1964 (voir réf. 14). Ainsi, depuis le début, l'approche canadienne en matière de sûreté et de délivrance de permis pour les réacteurs, bien qu'il se soit agi fondamentalement d'une méthode déterministe, comportait également un concept de risque, c'est-à-dire que la probabilité d'un accident "désastreux" devait être assez réduite pour que le risque correspondant soit très faible.

Le développement de l'approche en question qui, essentiellement est encore employé aujourdhui (voir réf. 15), est résumé au Tableau 1. Il faut que toute défaillance grave dans les systèmes opérationnels (défaillance simple) ait une probabilité totale ne dépassant pas un cas tous les trois ans et la défaillance ne doit pas exposer le public se trouvant au périmètre du site de la centrale, à une dose totale au corps entier supérieure à 5×10^{-3} sievert, tandis que toute défaillance des systèmes opérationnels combinée à la défaillance de l'un des systèmes* spéciaux de

TABLEAU 1

Guide d'emplacement de la CCEA

Limites de dose de référence

Exploitation normale et conditions d'accident

Situation	Probabilité maximale	Limites de dose individuelle maximales	Limites de dose totale maximales pour la population
Exploitation normale	--	5×10^{-3} sievert/année au corps entier	100 personne-sievert/année au corps entier
		3×10^{-2} sievert/année à la thyroïde	100 thyroïde-sievert/année
Défaillance simple (Système opérationnel)	1 tous les 3 ans	5×10^{-3} sievert au corps entier	100 personne-sievert au corps entier
		3×10^{-2} sievert à la thyroïde	100 thyroïde-sievert
Défaillance double (Système opérationnel et système de sûreté)	1 tous les 3×10^{3} ans	0,25 sievert au corps entier	10^{4} personne-sievert au corps entier
		2,5 sieverts à la thyroïde	10^{4} thyroïde-sievert

(Basé sur la réf. 15)

sûreté (défaillance double) doit avoir une probabilité totale ne dépassant pas $3,3 \times 10^{-4}$ par année et elle ne doit pas exposer le public à une dose au corps entier supérieure à 0, 25 sievert. La défaillance d'un système opérationnel accompagnée de la panne simultanée de deux systèmes spéciaux de sûreté (défaillance triple) n'est pas retenue à cause de la très faible probabilité d'une telle séquence d'incidents ($< 3,3 \times 10^{-7}$ par année-réacteur), étant donné l'indépendance des systèmes spéciaux de sûreté**.

En plus de ces limites de dose individuelle des limites de dose collective correspondantes ont été établies pour l'exploitation normale et pour les deux cas de la défaillance. Les limites de dose individuelle et collective ont été choicies sur la base d'un risque comparé. Le risque de leucémie, considéré comme le plus grand danger radiologique, devrait être faible par rapport à son taux normal d'apparition.

L'approche en question a servi de base raisonnable pour l'étude systématique des différents aspects de la sûreté dans une centrale nucléaire CANDU. Cependant, ces exigences simples ont donné lieu à quelques difficultés

---

* Les systèmes de sûreté comprennent les dispositifs de protection et de confinement, à savoir:

a) deux systèmes d'arrêt d'urgence indépendants et de conception différente;
b) un système de refroidissement d'urgence du coeur; et
c) un système de confinement.

** Le fait de ne pas arrêter le réacteur après la défaillance d'un système opérationnel n'est pas pris en considération dans cette analyse. Étant donné que deux systèmes d'arrêt d'urgence différents et indépendants sont requis, l'indisponibility simultanée et aléatoire de ces deux systèmes spéciaux de sûreté, après la défaillance d'un système opérationnel, constituerait une défaillance triple ayant la très faible probabilité susmentionnée.

d'interprétation et d'application. Le développement de la taille des réacteurs, de la puissance des éléments combustibles et de la complexité des systèmes, de même que l'enrichissement simultané des connaissances relatives au fonctionnement des systèmes, des données expérimentales et des méthodes analytiques, ont donné plus d'ampleur à ces difficultés qui se sont particulièrement manifestées lors de la délivrance de permis pour les réacteurs de la centrale Bruce A en 1976. L'aperçu qui suit résume ces difficultés:

(i) L'approche en question ne permet pas de faire une distinction entre des défaillances simples ayant diverses intervalles d'apparition et des conséquences différentes.

(ii) Elle ne permet pas de faire une distinction entre les défaillances doubles ayant diverses intervalles d'apparition et des conséquences différentes.

(iii) Elle traite de façon trop élémentaire la défaillance des systèmes de sûreté.

(iv) Elle ne s'occupe pas explicitement des événements dont la probabilité est si faible que leurs conséquences peuvent être passées sous silence.

(v) Elle ne s'occupe pas explicitement des événements extérieurs.

(vi) Bien qu'elle soit tout à fait appropriée pour l'arrêt d'urgence du réacteur en cas de défaillance d'un système opérationnel, elle ne convient guère pour les fonctions de sûreté plus complexes comme le refroidissement d'urgence et le confinement.

La nécessité d'une approche plus complète a suscité la formation en 1977 d'un groupe de travail interorganisationnel (GTI) formé de représentants de

la [illegible], du Comité consultatif de la sûreté des réacteurs*, de L'EACL et des services publics. L'objectif du GTI était de passer en revue les principes et les critères de sûreté applicables aux réacteurs et de préparer un ensemble d'exigences mises à jour, complétées, au besoin, par des lignes directrices générales d'application. On s'attendait que ces exigences mises à jour puissent surmonter les difficultés devenues évidentes. Les efforts du GTI ont abouti à la publication d'un rapport qui recommandait des exigences de sûreté pour la délivrance de permis aux centrales nucléaires CANDU et qui expliquait les principes de base des exigences (voir réf. 16, 17). Les principes généraux et les exigences de sûreté proposés par le GTI conservaient l'approche traditionnelle déterministe des barrières multiples en exigeant certains critères et systèmes spéciaux de sûreté, mais ils élargissaient la base probabiliste de l'approche précédente en définissant six catégories d'événements selon leur probabilité et en augmentant les valeurs des doses de référence individuelles permises lorsque la probabilité décroît (voir Tableau 2).

Les autres éléments de l'approche du GTI étaient les suivants:

a) un risque constant égal à celui d'une exploitation normale pour les trois premières catégories d'événements et un risque réduit pour les trois dernières catégories afin d'avoir une approche basée sur l'atténuation du risque dans le cas des accidents hypothétiques à grandes conséquences;

b) une limite d'analyse explicite relative aux événements avec des probabilités inférieures à 10^{-7} par année;

c) un cadre permettant d'englober les événements simples assez rares et les défaillances multiples simultanées, qu'il s'agisse de systèmes opérationnels ou de systèmes de sûreté;

---

* Le Comité consultatif de la sûreté des réacteurs était l'un des comités consultatifs spécialisés que la CCEA a dissous en 1978.

d) des méthodes pour traiter les événements extérieurs comme les tremblements de terres, les impacts d'aéronefs et le sabotage.

Les propositions du GTI n'ont pas toutes été adoptées par la CCEA. Le CCSN estime que deux raisons principales expliquent cette décision. Premièrement, l'augmentation de la dose maximale de référence passée de 0,25 à 1,0 sievert, combinée à une tolérance proposée au facteur de 10 pour les doses de référence prévues qui seraient permises dans les derniers stades de la conception, n'étaient pas acceptables. Deuxièment, la CCEA n'était pas suffisamment assurée, à ce moment-là, que les instruments d'analyse et les données statistiques fourniraient des calculs estimatifs de probabilité raisonnablement précis. De plus, le rapport entre la dose à la thyroïde et la dose au corps entier n'était pas en accord avec les calculs estimatifs les plus récents (voir réf. 18).

TABLEAU 2

Valeurs de référence proposées par le GTI (voir réf. 16)

Intervalle de dose de référence (Dose - en sieverts)		Valeur de référence de la somme des taux prévus de défaillances dans l'intervalle de référence correspondant (par réacteur par année)
Corps entier	Thyroïde	
0 à 5×10^{-4}	0 à 5×10^{-3}	10^{-1}
5×10^{-4} à 5×10^{-3}	5×10^{-3} à 5×10^{-2}	10^{-2}
5×10^{-3} à 5×10^{-2}	5×10^{-2} à 0,5	10^{-3}
5×10^{-2} à 0,1	0,5 à 1,0	10^{-4}
0,1 à 0,3	1,0 à 3,0	10^{-5}
0,3 à 1,0	3,0 à 10,0	10^{-6}

Certaines des recommandations du GTI ont été incorporées dans le document de consultation C-6 (voir réf. 19) de la CCEA qui a conservé le concept de plusieurs catégories d'accidents (5 au lieu de 6) pour lesquelles les doses individuelles de référence allaient de 5×10^{-4} à 0,25 sievert. Cependant, ces catégories n'étaient pas définies sur une base probabiliste mais plutôt déterministe en regroupant des accidents hypothétiques à partir d'une liste établie d'avance. Néanmoins, le regroupement de ces accidents reflétait le jugement des spécialistes de la CCEA sur la probabilité de tels accidents et représentait implicitement les valeurs de probabilité des cinq premières catégories du GTI (voir Tableau 3). Le document de consultation C-6 est employé à titre d'essai dans le processus de réglementation de la centrale nucléaire de Darlington.

TABLEAU 3

Valeurs de référence proposées dans le document de consultation C-6 de la CCEA (voir réf. 19)

Catégories d'événements hypothétiques	Dose limites de référence en sieverts	
	Corps entier	Thyroïde
1	5×10^{-4}	5×10^{-3}
2	5×10^{-3}	5×10^{-2}
3	3×10^{-2}	0,3
4	0,1	1,0
5	0,25	2,5

3.0 EXIGENCES PROPOSÉES

Les exigences générales de sûreté proposées pour les centrales nucléaires sont exposées dans la présente section du rapport, sous les rubriques suivantes:

A. Limites de dose de rayonnements en cour normal d'exploitation
B. Choix du site
C. Conception
D. Analyse de sûreté
E. Construction
F. Mise en service
G. Exploitation
H. Gestion des déchets et des effluents
I. Déclassement

Les exigences générales de sûreté que nous proposons devraient être lues et interprétées dans la perspective du "Projet de déclaration de principe sur les objectifs de sûreté relatifs aux activités nucléaires au Canada" (voir réf. 1) et à la lumière des commentaires sur les exigences proposées qui figurent à la section 4 du présent rapport.

A. Limites de dose de rayonnements en cours normal d'exploitation

A.1 Le choix du site, la conception, la construction, la mise en service, l'exploitation et le déclassement d'une centrale nucléaire doivent assurer que l'équivalent de dose effectif et l'équivalent de dose effectif engagé aux travailleurs sous rayonnements et au public, dus à l'exploitation et aux autres activités normales de la centrale, ne dépasseront pas les niveaux indiqués à l'Annexe II du Règlement (DORS/74-334, Gazette du Canada, Partie II, volume 108, n°12, 4 juin 1974, dans sa version modifiée) établi conformément à la Loi sur le contrôle de l'énergie atomique.

A.2 Le choix du site, la conception, la construction, la mise en service, l'exploitation et le déclassement d'une centrale nucléaire doivent, dans la mesure du possible, assurer que l'équivalent de dose effectif et l'équivalent de dose effectif engagé au public, dû à l'exploitation et aux autres activités normales de la centrale, ne dépasseront pas 1% de la limite réglementaire indiquée en A.1.

A.3 Le choix du site, la conception, la construction, la mise en service, l'exploitation et le déclassement d'une centrale nucléaire doivent assurer que l'équivalent de dose effectif et l'équivalent de dose effectif engagé aux travailleurs sous rayonnements à la centrale, seront au niveau le plus bas qu'il soit raisonnablement possible d'atteindre en deça de la limite réglementaire indiquée en A.1.

B. Choix du site

B.1 Dans le choix du site d'une centrale nucléaire, il faut tenir compte des exigences radiologiques indiquées à la section A, c'est-à-dire que le site ne doit présenter aucune caractéristique qui pourrait donner lieu à des exigences ou à des limitations indues dans la conception ou dans l'exploitation de la centrale.

B.2 Si l'on considère divers sites possibles pour une centrale nucléaire, il faudrait estimer les doses collectives à la population, d'une part, en cours normal d'exploitation et, d'autre part, en cas d'accidents, en ayant recours à des méthodes acceptées. Les valeurs estimées devraient être considérées comme un facteur important dans le choix d'un site.

B.3 Sur le site choisi d'une centrale nucléaire, la fréquence et la sévérité des événements extérieurs naturels (à l'exception des tremblements de terre) ou causés par l'homme devraient être suffisamment faibles pour que le risque estimé qu'encourrait le public par suite d'une défaillance de la centrale provoquée par ces événements, ne constitue qu'une petite fraction du risque global au public dû à la centrale.

B.4 En ce qui concerne les tremblements de terre, sur le site choisi d'une centrale nucléaire ou à proximité de ce site, dont les conséquences hypothétiques seraient plus graves que les effets enregistrés par le passé et pour lesquels il n'existe pas de modèle théorique valable qui permette de mettre en corrélation la fréquence et les conséquences de tels séismes, le risque estimé qu'encourrait le public par suite d'une défaillance de la centrale due au tremblement de terre devrait être faible comparé au risque que le public encourrait à cause du tremblement de terre lui-même.

B.5 Les caractéristiques du site doivent permettre de prendre facilement des mesures d'urgence en cas d'accidents pouvant avoir des conséquences dangereuses au-delà du périmètre de la centrale.

C. Conception

C.1 La conception des centrales nucléaires doit être conforme aux bons principes et aux bonnes techniques de génie. Elle doit suivre les normes et les codes appropriés reconnus et recourir aux méthodes pertinentes pour le contrôle et l'assurance de la qualité.

C.2 Au cours de la conception d'une centrale nucléaire, il faut prendre toutes les mesures nécessaires pour éviter que des accidents se produisent ou pour réduire leur probabilité.

C.3 Au cours de la conception d'une centrale nucléaire, on doit recourir à tous les moyens raisonnables pour assurer que les produits de fission restent à l'intérieur des éléments combustibles dans des conditions d'exploitation prévisibles et on doit établir des barrières appropriées pour les empêcher de s'échapper.

C.4 Au cours de la conception d'une centrale nucléaire, on doit prévoir certaines fonctions de sûreté dans le but de supprimer ou de minimiser les conséquences des défaillances dans les systèmes opérationnels. Les fonctions de sûreté sont:

a) l'arrêt d'urgence rapide du réacteur et le maintien de l'arrêt en cas d'accident réel ou prévu;

b) le refroidissement adéquat du combustible en cas d'accident; et

c) le confinement adéquat des matières radioactives en cas d'accident.

C.5 Les centrales nucléaires doivent avoir des systèmes spéciaux de sûreté ayant pour but de remplir les fonctions susmentionnées. Les systèmes spéciaux de sûreté doivent comprendre au moins:

a) deux systèmes différents pour arrêter rapidement la réaction nucléaire, chacun d'eux étant capable, seul, d'arrêter le réacteur, quel que soit son niveau de fonctionnement. Chaque système doit être en mesure de maintenir le réacteur à l'arrêt en toute sécurité de façon indéfinie ou jusqu'à ce qu'un autre système pouvant le maintenir dans cet état puisse être employé;

b) un système d'injection et, au besoin, de réinjection de fluide de refroidissement pour remplacer le caloporteur primaire normal au cas où l'enveloppe de pression du circuit primaire de caloportage serait rompue; et

c) un système pouvant retenir toute substance radioactive provenant du circuit primaire de caloportage au cas où l'enveloppe de pression du système normalement utilisée serait rompue.

C.6 Chaque système spécial de sûreté doit être conçu avec un taux d'indisponibilité égal ou inférieur à 10^{-3}.

C.7 Chaque système spécial de sûreté doit:

a) être conçu de façon telle que son fonctionnement permette de remplir les fonctions de sûreté stipulées à l'exigence C.4;

b) être suffisamment séparé, physiquement et fonctionnellement, des autres systèmes spéciaux de sûreté et des systèmes opérationnels et suffisamment différent d'eux pour que l'on soit sûr que les défaillances plausibles corrélées et les défaillances de cause commune ou de mode commun n'empêcheront pas de se conformer à l'exigence C.6;

c) avoir des systèmes auxiliaires (électricité, air, eau, etc.) fiables et indépendants pour répondre aux exigences C.6, C.7a) et C.7b);

d) pouvoir être soumis à des essais assez fréquents pour que l'on soit raisonnablement sûr que l'exigence en matière d'indisponibilité stipulée en C.6 est respectée; et

e) avoir une redondance suffisante pour que, en général, aucune défaillance plausible d'un seul composant ne l'empêche de bien fonctionner.

C.8 Si un système spécial de sûreté est subdivisé ou relié à des sous-systèmes et si ces divisions ou sous-systèmes sont considérés comme indépendants à des fins d'analyse de sûreté, la conception de chaque sous-système doit répondre aux exigences C.7.

C.9 Chaque système spécial de sûreté et ses systèmes auxiliaires doivent être conçus de façon à pouvoir remplir leurs fonctions propres de façon sûre dans des conditions provoquées par les défaillances dans les systèmes opérationnels ou dans les autres systèmes spéciaux de sûreté au cours desquelles ils doivent intervenir.

C.10 Les systèmes spéciaux de sûreté doivent être conçus pour se déclencher automatiquement sans l'intervention immédiate d'un opérateur, mais il doit être possible qu'un opérateur les déclenche ou qu'il intervienne, au besoin, pour assurer ou renforcer la sûreté.

C.11 La conception doit prévoir des intervalles de déclenchement, c'est-à-dire que l'intervalle entre le déclenchement du système spécial de sûreté et les points de défaillance d'un système ou d'un composant doit dépendre de données expérimentales directement applicables ou d'une extrapolation prudente des données disponibles.

C.12 La conception doit comprendre un moyen permettant le refroidissement du combustible nucléaire au cas où le puits primaire d'évacuation de la chaleur ne serait pas disponible tandis que l'enveloppe de pression normalement utilisée du circuit primaire de caloportage demeure toujours intacte.

C.13 La centrale doit être conçue de telle façon qu'elle puisse continuer de fonctionner en toute sûreté ou être arrêtée et maintenue dans un état d'arrêt sûr, au cours et à la suite de tout événement interne ou externe plausible et prévisible sur les lieux. Une mesure à prendre est d'avoir deux postes physiquement séparés à partir desquels le réacteur peut être arrêté, les services essentiels à la sûreté maintenus et l'état général de la sûreté de la centrale contrôlé.

C.14 Des dispositions appropriées doivent être prises en vue de la protection du personnel des centrales en cas de toute défaillance plausible. L'accès du personnel aux zones essentielles ne doit pas être rendu impossible à la suite des conditions résultant d'une défaillance.

C.15 La conception doit présenter une redondance et une diversité suffisantes pour que les limites de dose de rayonnements indiquées à la section A ne soient pas dépassées et pour que les objectifs de sûreté décrits à la section D puissent être atteints en toute confiance.

C.16 La conception devrait rendre la centrale capable de supporter les défaillances. En fait, la résistance de la centrale aux défaillances possibles devrait se présenter dans l'ordre suivant: (i) aucun effet important susceptible de nuire à la sûreté; (ii) un changement vers un état plus sûr; (iii) l'état sûr maintenu ou rétabli par des systèmes constamment disponibles et en marche; (iv) condition sûre rétablie par l'intervention d'un système spécial de sûreté.

C.17 Il doit y avoir des instruments de mesure suffisants et appropriés, assez redondants et diversifiés pour fournir l'information fiable requise pour le contrôle sûr de la centrale nucléaire en tout temps, y compris les périodes faisant suite aux défaillances ou à des événements internes ou externes.

C.18 La centrale doit être conçue de façon à faciliter les inspections périodiques et la maintenance de l'équipement et des systèmes opérationnels.

C.19 La conception de la centrale, y compris la salle des commandes, doit tenir compte des principes d'ergonomie et des données connexes.

C.20 Au moment de la conception, il faut prévoir des mesures appropriées pour empêcher toute interférence de personnes non autorisées ou l'accès de telles personnes aux structures, aux systèmes et aux composants reliés à la sûreté.

D. Analyse de la sûreté

D.1 Les méthodes, les modèles et les données employés dans les analyses de sûreté doivent être basés sur des connaissances théoriques, expérimentales, ou opérationnelles pertinentes et valables.

D.2 Le concepteur doit établir une liste des séquences de défaillances potentielles, au moyen d'une méthode systématique d'identification de ces séquences, qui seront analysées pour démontrer que la conception est conforme à l'exigence D.4.

D.3 Dans la mesure du possible, les séquences de défaillances potentielles doivent être analysées de façon réaliste. S'il est impossible de faire une analyse réaliste, des séries de séquences ayant des caractéristiques semblables devraient être identifiées et un cas limite devrait être analysé.

D.4 Le risque estimé à partir de l'analyse des séquences de défaillances définies selon l'exigence D.2, doit être jugé en fonction du Tableau 4. (La Figure 1 montre le Tableau 4 sous forme d'histogramme.) Tel

qu'indiqué au Tableau 4, il faut faire la somme des probabilités de séquences de défaillances pouvant avoir des conséquences dans chaque intervalle d'équivalent de dose.

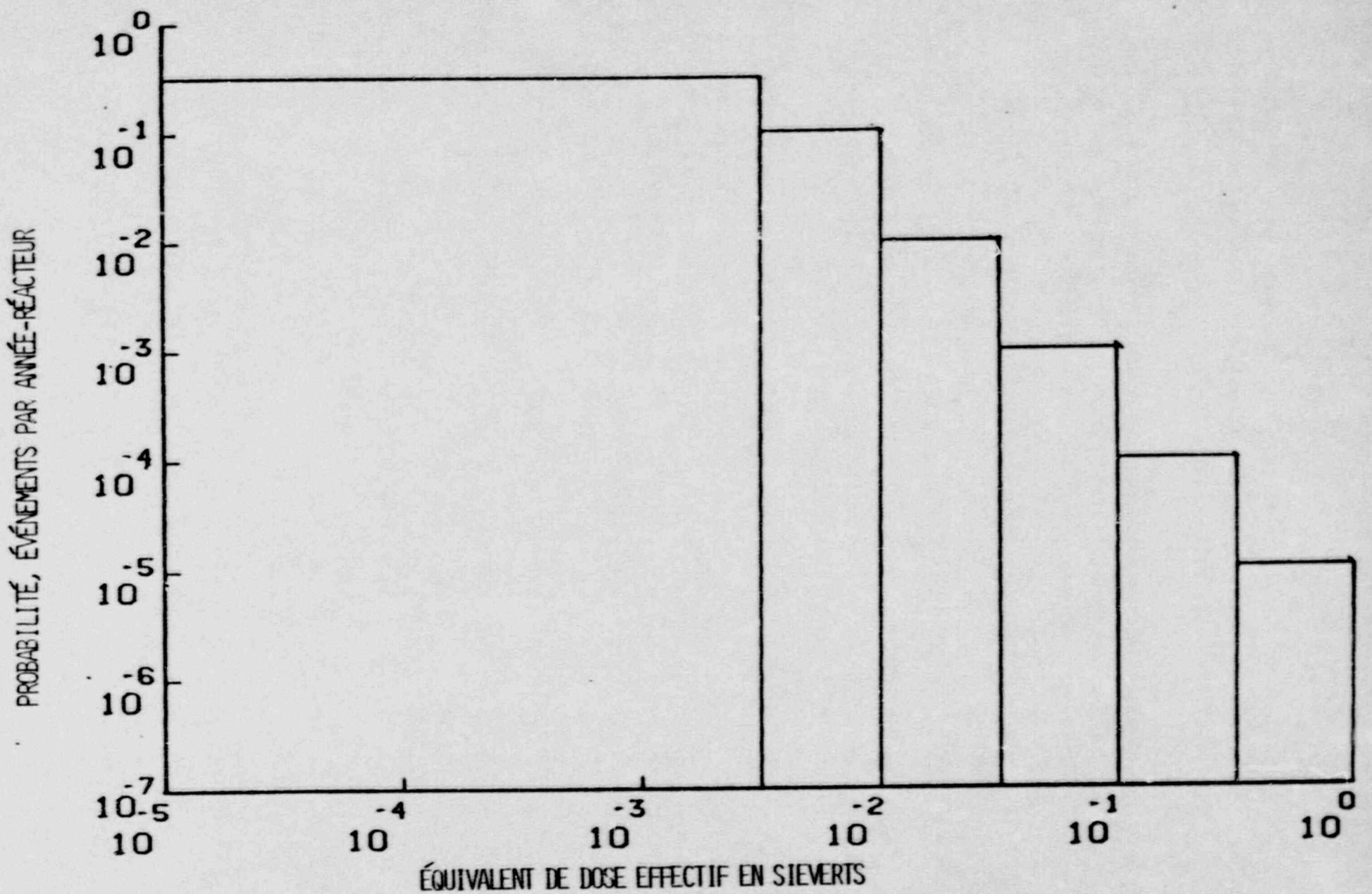
a) Si les sommes se trouvent en deça des limites dans tous les intervalles d'équivalent de dose, dans la troisième colonne du Tableau 4, le risque estimé est acceptable.

TABLEAU 4

Catégories de risque proposées pour l'analyse des accidents

Catégorie	Intervalle de l'équivalent de dose effectif individuel (en sieverts)	Somme des probabilités de défaillances à l'intérieur de l'intervalle correspondant d'équivalent de dose effectif (par réacteur par année)
1	0 à $10^{-2,5}$	$3,33 \times 10^{-1}$
2	$10^{-2,5}$ à 10^{-2}	10^{-1}
3	10^{-2} à $10^{-1,5}$	10^{-2}
4	$10^{-1,5}$ à 10^{-1}	10^{-3}
5	10^{-1} à $10^{-0,5}$	10^{-4}
6	$10^{-0,5}$ à 1	10^{-5}

FIGURE 1 CATÉGORIES DE RISQUE PROPOSÉES POUR L'ANALYSE DES ACCIDENTS



b) Si la somme de n'importe quel intervalle d'équivalent de dose se trouve au-delà de la limite, dans la troisième colonne du Tableau 4, le risque estimé n'est généralement pas acceptable.

c) Dans le cas décrit en D.4b), la CCEA peut accepter la situation, à condition que le total du risque encouru par un membre du public dû à toutes les séquences d'accidents décrites dans l'exigence D.2 soit égal ou inférieur au risque correspondant à la somme des limites de risque de toutes les catégories d'accidents présentées au Tableau 4. Pour porter ce jugement la CCEA devra considérer les intervalles (de dose) de conséquences, les incertitudes dans l'évaluation des conséquences et des probabilités, le degré de prudence et d'autres facteurs, et s'assurer que le total du risque calculé soit aussi minime que possible.

D.5 Les conséquences de n'importe quel événement unique ou de n'importe quelle séquence d'événements figurant dans la liste établie à l'exigence D.2, dont le calcul estimatif de la probabilité est inférieur à 10^{-7} par réacteur et par année, n'ont pas besoin d'être incluses dans cette analyse.

D.6 Pour calculer les équivalents de dose afin de répondre à l'exigence D.4, il faut avoir recours à des conditions météorologiques ou à des conditions de dispersion réalistes et à des relations acceptées entre l'exposition ou l'incorporation et l'équivalent de dose effectif.

E. Construction

E.1 Pour la construction de la centrale, y compris la fabrication de tous les composants relatifs à la sûreté, on doit employer des procédés reconnus ou approuvés et se conformer aux normes et aux codes appropriés.

E.2 La construction de la centrale et la fabrication des composants doivent être conformes aux principes et aux normes reconnus de contrôle et d'assurance-qualité.

E.3 Les particularités conceptuelles permettant les inspections périodiques et la maintenance ne doivent pas être compromises par les méthodes de construction employées.

F. Mise en service

F.1 Un programme détaillé, complet et documenté doit être préparé et mis en oeuvre pour démontrer que l'ensemble des structures, des systèmes et des composants relatifs à la sûreté répondent ou peuvent répondre aux exigences nominales.

F.2 Avant la première divergence d'un réacteur nucléaire, il faut faire la preuve que les systèmes de sûreté sont en état de fonctionner et qu'ils peuvent répondre aux exigences nominales.

F.3 L'état ou le fonctionnement réel de l'ensemble des structures, des systèmes et des composants relatifs à la sûreté, tel qu'établi dans le programme de mise en service, doit être documenté de façon appropriée afin de servir de base aux essais et aux inspections ultérieurs menés au cours de l'existence de la centrale.

G. Exploitation

G.1 La responsabilité primordiale du maintien de la sûreté pendant l'exploitation d'une centrale nucléaire revient au titulaire de permis et aux membres de son personnel, selon le cas.

G.2 L'organisation du titulaire de permis doit comprendre un groupe chargé de vérifier tous les aspects de l'exploitation de la centrale relatifs à la sûreté. Le groupe en question ne devra pas faire partie du personnel d'exploitation et relèvera de la haute direction.

G.3 Les membres du personnel d'exploitation et de maintenance doivent avoir une formation et une compétence appropriées à leurs fonctions et il faut un programme permanent de contrôle et de mise à jour, au besoin, de leur compétence et de leur formation.

G.4 Nonobstant l'exigence G.3, tout le personnel d'une centrale nucléaire doit recevoir une formation périodique en matière de sûreté et de radioprotection.

G.5 L'effectif régulier du personnel d'exploitation doit être suffisant pour faire fonctionner adéquatement la centrale en tout temps et pour éliminer le besoin d'employer du personnel temporaire additionnel pour que les limites de dose individuelles soient respectées, sauf dans des circonstances exceptionnelles.

G.6 L'exploitation de la centrale doit être régie par des marches à suivre générales écrites à l'avance.

G.7 Des limites opérationnelles acceptables doivent être définies pour tous les paramètres importants relatifs à la sûreté; des méthodes claires doivent être établies au cas où de tels paramètres dépasseraient les limites fixées.

G.8 Tous les systèmes spéciaux de sûreté et tous les composants relatifs à la sûreté doivent être inspectés et soumis à des essais périodiques, selon un programme précis, pour vérifier s'ils répondent toujours à l'exigence C.6.

G.9 Des plans doivent être disponibles pour les cas d'urgence ayant des effets à l'intérieur ou à l'extérieur de la centrale; ces plans doivent être soumis à des essais périodiques selon des méthodes réalistes.

G.10 Le titulaire de permis doit élaborer des lignes directrices au sujet des expositions maximales aux rayonnements que les travailleurs pourront subir dans des situations d'urgence et les soumettre à la CCEA pour approbation.

H. Gestion des déchets et des effluents

H.1 Les effluents liquides ou gazeux contenant des matières radioactives ne doivent être évacués que dans des conditions approuvées et l'évacuation doit être contrôlée pour vérifier la conformité aux exigences de la section A.

H.2 Aucune matière radioactive ne doit être évacuée sur le site de la centrale, sauf si l'évacuation est conforme à l'exigence H.1 ou approuvée spécialement par la CCEA.

H.3 Toutes les dispositions prises pour entreposer des déchets radioactifs dans une centrale nucléaire doivent prévoir des mesures appropriées concernant le blindage, l'évacuation de la chaleur, la sécurité physique et la récupération.

I. Déclassement

I.1 La conception, la construction et l'exploitation d'une centrale nucléaire doivent pouvoir faciliter son déclassement et son démantèlement après son exploitation, afin de minimiser la surveillance nécessaire et le temps qui s'écoulera avant que le site retourne à un état radiologique sûr.

I.2 Des plans doivent être dressés, dans les grandes lignes, pour remettre le site dans un état radiologique sûr, après l'exploitation d'une centrale nucléaire. Ces plans sommaires doivent être préparés au stade de la conception et mis à jour par la suite, au besoin.

4.0 COMMENTAIRES SUR LES EXIGENCES PROPOSÉES

La présente section du rapport donne la raison d'être ou l'explication des exigences proposées, sous les mêmes rubriques que celles de la section 3.

A. Limites de dose de rayonnements en cours d'exploitation normale

L'exigence A.1 stipule que les limites réglementaires s'appliquant aux équivalents de dose effectifs et aux équivalents de dose effectifs engagés reçus par un travailleur sous rayonnements dans une centrale nucléaire ou par un membre du public touché par les opérations en cours à la centrale doivent être respectées.

L'exigence A.2 précise, sur la base de l'expérience, jusqu'où les doses reçues par un membre du public peuvent être limitées en appliquant le principe ALARA aux centrales nucléaires CANDU. En vertu de ce principe, l'établissement d'une limite cible ne signifie pas qu'on ne devrait pas recourir à d'autres méthodes permettant de réduire davantage l'exposition aux rayonnements, lorsque lesdites méthodes sont aisément disponibles à un coût raisonnable. Inversement, si le principe ALARA est appliqué consciencieusement dans la conception et dans l'exploitation de la centrale, des limites plus élevées que la cible susmentionnée pourraient être acceptables.

L'exigence A.3 stipule la nécessité d'appliquer le principe ALARA aux doses de rayonnements reçues par les travailleurs sous rayonnements dans une centrale nucléaire. Tel qu'indiqué à la section 1 du présent rapport, il revient au propriétaire de la centrale d'établir et de mettre en vigueur le principe ALARA pour limiter les doses reçues par ses travailleurs.

Dans l'application des exigences A.1, A.2 et A.3, des méthodes acceptées (voir réf. 18) devraient être employées pour calculer les équivalents de dose effectifs et les équivalents de dose effectifs engagés reçus par les travailleurs sous rayonnements et par le public.

Les limites de dose collective (dose à la population) ne sont pas précisées dans les exigences proposées, car on admet généralement que la mise en vigueur des limites de dose individuelle permettra d'assurer que les doses à

la population sont acceptables. Par ailleurs, la difficulté que présente le calcul des doses totales à la population effectué de façon fiable pendant l'exploitation normale empêche toute précision significative des limites propres à ces doses. Cependant, l'exigence B.2 précise que les doses à la population ou les doses collectives estimées doivent être considérées sur une base relative lors du choix du site.

Les lignes directrices touchant les doses radiologiques en cas d'accidents se trouvent à la section D.

B. Choix du site

Bien que l'emplacement d'une centrale nucléaire peut ne pas influer directement sur sa sûreté, les caractéristiques d'un site peuvent influencer la conception des installations, avoir des répercussions sur les conséquences d'un accident et empêcher de prendre certaines mesures d'atténuation.

Les exigences proposées à la section B ont pour but d'assurer que le site choisi convient pour une centrale nucléaire et que le site lui-même n'impose pas d'exigences conceptuelles excessives. Tel qu'indiqué ci-dessus, l'exigence B.2 stipule que les doses à la population doivent être considérées comme l'un des facteurs de choix d'un site. Tous les autres facteurs étant égaux, c'est le site offrant la plus faible dose collective engagée qui doit être favorisé.

Les exigences B.3 et B.4 ont pour but d'assurer que les événements extérieurs prévus d'origine humaine ou naturelle, y compris les tremblements de terre, ne rendront pas impossibles ou indûment difficiles la conception et l'exploitation sûres de la centrale sur le site choisi. On ne prévoit pas qu'il sera nécessaire de faire l'analyse exhaustive des effets d'un tremblement de terre dans toute la région où se trouve la centrale nucléaire, mais des efforts raisonnables doivent être faits pour s'assurer que le site ne rendra pas indûment difficile l'application des exigences B.3 et B.4.

On ne devrait pas interpréter le principe énoncé dans l'exigence B.4 comme signifiant que les centrales devraient être situées dans des régions très peuplées plutôt que loin des agglomérations.

On suppose que de nombreuses exigences non apparentées directement à la sûreté, tels les effets environnementaux et socio-économiques, seront prises en considération pour choisir le site d'une centrale nucléaire.

De toute évidence, lors de la conception d'une centrale nucléaire il faut prendre en considération les effets des événements extérieurs humains et naturels sur le site choisi. L'exigence C.13 rend compte de cette nécessité.

C. Conception

La sûreté d'une centrale nucléaire dépend de certains facteurs dont un des plus importants est la conception. Les exigences proposées pour la conception dans la section C reflètent les concepts de sûreté qui ont évolué au Canada et ailleurs, et elles représentent une pratique prudente bien établie, comme le stipule l'exigence C.1.

L'exigence C.2 reconnaît que la meilleure façon d'assurer la protection du public et des travailleurs est de s'assurer que des accidents ne se produiront pas ou que leur probabilité soit aussi faible qu'il soit raisonnablement possible de le faire.

L'exigence C.3 reconnaît qu'il n'y aura pas de danger grave pour les travailleurs ou pour le public si les produits de fission sont retenus à l'intérieur des éléments combustibles, et fait appel au principe des barrières multiples qui empêchent la libération des produits de fission.

L'exigence C.4 reconnaît qu'il est essentiel que certaines fonctions de sûreté soient fournies dans une centrale nucléaire pour faire face aux défaillances des systèmes opérationnels de la centrale.

Bien que les exigences de sûreté proposées comportent, à la section D, des critères de risque plus complets que ceux du Guide d'emplacement (voir réf. 14, 15), certaines exigences conceptuelles déterministes sont retenues

pour assurer la mise en oeuvre du principe des barrières multiples contre les accidents potentiels. Les plus importantes parmi ces exigences sont celles destinées aux systèmes spéciaux de sûreté que l'on trouve dans l'exigence C.5 et dont le but est d'assurer que les fonctions de sûreté peuvent être assumées avec efficacité et fiabilité. L'exigence C.5 précise qu'il est nécessaire d'avoir deux systèmes d'arrêt d'urgence indépendants, un système d'injection et de réinjection de fluide de refroidissement d'urgence et un système de confinement. La référence à la réinjection de fluide de refroidissement prévoit que le fluide de refroidissement d'urgence déchargé dans les puisards du bâtiment peut être renvoyé dans le circuit primaire de caloportage lors de la phase de "recirculation" du refroidissement d'urgence.

L'exigence C.6 conserve le critère actuel d'indisponibilité pour les systèmes spéciaux de sûreté. On reconnaît que ce critère d'indisponibilité est une cible opérationnelle. Pour les besoins de rapport, les systèmes spéciaux de sûreté sont généralement considérés comme indisponibles lorsqu'ils ne sont pas efficaces à 100%, bien qu'ils puissent être en mesure d'assumer leur fonction de système de sûreté de façon adéquate. De telles considérations devraient intervenir lorsqu'on détermine si un système spécial de sûreté répond à la cible d'indisponibilité et dans l'analyse de sûreté décrite à la section D. La cible d'indisponibilité doit pouvoir être démontrée telle qu'indiquée à l'exigence C.7d).

L'exigence C.7a) doit être interprétée comme signifiant que la conception de chaque système spécial de sûreté doit assurer que le système peut répondre aux exigences de fonctionnement et pourra fonctionner avec fiabilité lorsqu'il sera en service.

Il est important de faire une distinction entre une fonction de sûreté comme celle décrite à l'exigence C.4 et un système spécial de sûreté comme celui décrit à l'exigence C.5. Il est entendu que les systèmes spéciaux de sûreté nécessiteront des systèmes de soutien et que les fonctions de sûreté nécessiteront dans certains cas l'emploi de composants du système opérationnel comme les collecteurs, les conduites d'alimentation et les pompes de circulation du fluide de refroidissement, dans l'ensemble du procédé de refroidissement d'urgence. Les critères conceptuels s'appliquant à ces cas sont précisés aux exigences C.6 et C.7a), b) et c).

Les exigences générales s'appliquant à la conception des systèmes spéciaux de sûreté, telles qu'indiquées aux exigences C.7a) à C.7e) sont compatibles avec la pratique actuelle.

L'exigence C.8 reconnaît qu'un système spécial de sûreté peut être composé de sous-systèmes séparés comme diverses parties du système de confinement, entre autres, les registres de ventilation, le mécanisme d'aspersion, etc. Lorsqu'un tel sous-système séparé est considéré comme indépendant en ce qui concerne l'analyse de sûreté, la conception de ce sous-système doit répondre aux critères des systèmes spéciaux de sûreté stipulés dans l'exigence C.7. On reconnaît, naturellement, que certains sous-systèmes font partie intégrante du système spécial de sûreté en question et qu'ils ne peuvent pas vraiment en être "physiquement séparés" tel que stipulé à l'exigence C.7b). Cependant, le but de l'exigence C.7b), dans ce cas, est d'assurer que le critère d'indisponibilité de l'exigence C.6 puisse être satisfait.

Le but de l'exigence C.9 est d'assurer qu'un système spécial de sûreté peut remplir sa fonction dans des conditions pouvant résulter de défaillances dans les systèmes opérationnels ou dans d'autres systèmes spéciaux de sûreté pour lesquelles le système spécial de sûreté est conçu.

L'exigence C.10 précise que le fonctionnement d'un système spécial de sûreté doit être automatiquement déclenché en réponse à des signaux appropriés comme le veut l'exigence C.17. Cependant, l'exigence C.10 n'écarte pas l'intervention de l'opérateur dans des conditions appropriées, tel que le déclenchement manuel ou la mise en marche de la phase de recirculation du refroidissement d'urgence du coeur.

L'exigence C.11 stipule qu'il est nécessaire d'établir des points de déclenchement appropriés pour diverses mesures du réacteur qui jouent un rôle en matière de sûreté. Les points de déclenchement doivent être établis de façon à réduire la probabilité d'endommagement de tout système ou composant, qui pourrait provoquer des rejets de radioactivité.

L'exigence C.12 stipule qu'un système de refroidissement auxiliaire ou de secours est nécessaire comme puits d'évacuation de la chaleur au cas où les générateurs de vapeur qui constituent les puits d'évacuation de la chaleur normaux du circuit primaire de caloportage ne seraient pas disponibles.

L'exigence C.13 a pour but d'assurer la sûreté de la centrale nucléaire lors d'événements internes ou externes prévisibles comme les tremblements de terre, les incendies, etc. Elle met en application, du fait qu'elle exige deux postes de contrôle séparés, le "concept des deux groupes" maintenant employé dans la conception des centrales nucléaires CANDU (voir réf. 20).

L'exigence C.14 souligne la nécessité d'assurer la protection du personnel d'une centrale nucléaire et d'assurer que les travailleurs peuvent avoir accès à toutes les zones essentielles afin d'assurer la sûreté de la centrale après la défaillance d'un composant ou d'un système.

Les exigences C.15 à C.19 présentent de bonnes pratiques de génie et sont compatibles avec la façon dont on aborde actuellement la conception des réacteurs au Canada.

L'exigence C.20 stipule qu'il faut prendre en considération, au stade de la conception, la nécessité de rendre le sabotage d'une centrale nucléaire aussi difficile qu'il soit raisonnablement possible de le faire. Toute tentative de sabotage nécessiterait en général un connaissance détaillée de la conception et du plan de la centrale, ce qu'une personne du dehors aurait beaucoup de mal à obtenir. En assignant un personnel adéquat dans la centrale, on devrait pouvoir réduire la probabilité de réussite de toute tentative de sabotage. Le CCSN croit que les exigences relatives à la sûreté des centrales nucléaires, exposées dans le présent rapport, peuvent, de concert avec certaines mesures de sécurité raisonnables, limiter le risque de sabotage à une petite fraction du risque total que la centrale représente.

D. Analyse de sûreté

Le critère proposé ici pour la sûreté d'une centrale nucléaire est que le risque radiologique total estimé auquel le public est exposé en conditions d'accident, ne doit pas dépasser de beaucoup le risque encouru au cours de l'exploitation normale de la centrale. Pour assurer que la conception fournit une sûreté adéquate, il faut effectuer des analyses de conséquences et de probabilités des défaillances potentielles. Les conditions et les méthodes à employer pour ces analyses sont indiquées dans cette section.

L'exigence D.1 couvre les analyses de probabilité ainsi que les analyses physiques. Les valeurs de probabilité employées devraient être fondées sur une expérience directe ou sur des extrapolations raisonnables.

Tel qu'indiqué dans l'exigence D.2, le concepteur aura la responsabilité d'élaborer une liste de séquences de défaillances potentielles à analyser qu'il devra soumettre à la CCEA en temps voulu.

L'exigence D.3 précise que les séquences de défaillances devraient être analysées de façon réaliste autant que possible. Conformément à cette approche, toutes les analyses devraient comprendre des estimations d'erreurs physiques et d'erreurs de probabilité. Lorsque des analyses de cas extrêmes sont nécessaires, les estimations probabilistes devraient le reconnaître.

Le risque encouru par le public, que l'on évalue à partir de l'analyse des séquences de défaillances indiquées dans la liste susmentionnée, doit être jugé par rapport aux catégories d'accidents données au Tableau 4, selon la méthode décrite à l'exigence D.4.

Les catégories d'accidents en question ont été déterminées en considérant le critère fondamental de risque énoncé ci-dessus, les critères existants de défaillance simple ou double du Guide d'emplacement (voir réf. 14 et 15), les recommandations du GTI (voir réf. 16) et d'autres données pertinentes (voir réf. 21). La définition des catégories prend en considération l'atténuation du risque pour les défaillances ayant des conséquences graves.

Les catégories d'accidents du Tableau 4 doivent être employées pour juger l'acceptabilité des résultats prévus pour les séquences d'accidents. Bien que l'exigence D.3 précise que l'analyse des séquences d'accidents doit être effectuée d'une façon aussi réaliste que possible, il est admis qu'il ne sera pas possible d'analyser toutes les séquences d'accidents potentiels, que les analyses ne peuvent toujours être complètement réalistes et que des analyses prudentes de cas extrêmes seront nécessaires dans de nombreux cas. Par conséquent, les probabilités et les conséquences associées aux catégories ne devraient pas être interprétées comme des représentations du comportement réel prévu du réacteur de puissance en cas d'accident. Elles ont été élaborées pour fournir une base d'acceptation de la conception d'une centrale nucléaire et non pour servir de prévision du comportement futur de la centrale en question.

Les conséquences maximales admises dans chaque catégorie sont exprimées en termes d'équivalents de dose effectifs, d'après les plus récentes recommandations de la Commission internationale de protection radiologique (voir réf. 18) qui élimine le besoin de définir des limites de dose à la thyroïde.

Les catégories indiquées au Tableau 4 sont basées sur des intervalles de conséquences définis présentant des rapports égaux d'équivalents de dose effectifs (sauf pour la catégorie 1). Chaque catégorie d'intervalles d'équivalents de dose pose une valeur limite supérieure pour la somme permise des probabilités de séquences de défaillances mutuellement exclusives à l'intérieur de la catégorie. L'acceptabilité des résultats prévus des séquences d'accidents doit être jugée comme suit:

a) si les sommes se trouvent en deçà des valeurs limites dans toutes les catégories, le risque total calculé est acceptable;

b) si la somme dans n'importe quelle catégorie se trouve au-delà de la valeur limite supérieure, le risque calculé est généralement inacceptable; et

c) dans le cas décrit en b) ci-dessus, la CCEA peut accepter la situation, à condition que la valeur maximale prévue du risque à un membre du public en particulier, dû à toutes les séquences d'accidents décrites conformément à l'exigence D.2 soit égale ou inférieure à celle correspondant à la somme des risques limites de toutes les catégories d'accidents du Tableau 4. (Voir Tableau 5). En portant ce jugement, la CCEA devrait considérer le niveau de conséquences de l'intervalle ou des intervalles en cause, les incertitudes que comportent les données physiques, la pertinence des modèles analytiques, les incertitudes que comportent les données et les modèles probabilistes, l'approche prudente des analyses, les facteurs économiques et sociaux et tout autre facteur pouvant influencer l'analyse. La CCEA devrait également s'assurer que le risque total calculé est aussi faible que possible et veiller à ce que l'aspect de l'"atténuation du risque"* dans les catégories soit maintenu dans la mesure du possible.

---

*Voir p.48.

TABLEAU 5

Valeurs maximales calculées
du risque au membre du public
le plus fortement exposé

SÉQUENCES D'ACCIDENTS

Critère	Risque* (sieverts par année-réacteur)
CCSN-4	$2,5 \times 10^{-3}$
Recommandation du GTI	$1,6 \times 10^{-4}$
Guide d'emplacement de la CCEA (Défaillance simple et double)	$1,8 \times 10^{-3}$**

EXPLOITATION NORMALE

Critère	Risque (sieverts par année-centrale)
Principe ALARA	$5,0 \times 10^{-5}$
Limite réglementaire	$5,0 \times 10^{-3}$

FOND DE RAYONNEMENTS

Source	Risque (sieverts par année)
Sources naturelles (à l'intérieur et à l'extérieur) (Voir réf. 23)	10^{-3}

---

* Les valeurs de risque sont prudentes, étant donné qu'elles supposent que toutes les séquences d'accidents d'une catégorie donnée se situent à la limite supérieure de conséquences de la catégorie en question.

**Le risque maximal calculé correspondant aux critères du Guide d'emplacement de la CCEA représente plutôt une valeur nominale qu'une valeur compatible avec les recommandations actuelles, vu l'emploi plus répandu de méthodes déterministes ou arbitraires dans le Guide d'emplacement.

Étant donné que la probabilité totale de tous les événements dans une catégorie d'accidents doit être jugée à la lumière de la limite d'acceptation, il faudra, en général, que les concepteurs et les analystes aient recours à un procédé itératif.

La probabilité limite pour la catégorie 1 est fixée à $3,33 \times 10^{-1}$ (1 en 3 ans) pour garder la somme des probabilités de cette catégorie égale à la probabilité maximale admissible s'appliquant aux événements à défaillance simple dans le Guide d'emplacement de la CCEA (voir réf. 14, 15).

Les catégories d'accidents proposées sont présentées sous la forme d'un histogramme à la Figure 2. Par ailleurs, la Figure 2 compare les critères de la défaillance simple et de la défaillance double se trouvant dans le Guide d'emplacement avec les catégories de risque proposées. On peut voir à la Figure 2 que les probabilités limites des catégories 2 et 5 sont légèrement inférieures aux fréquences maximales des défaillances simples et des défaillances doubles, respectivement, stipulées dans le Guide d'emplacement.

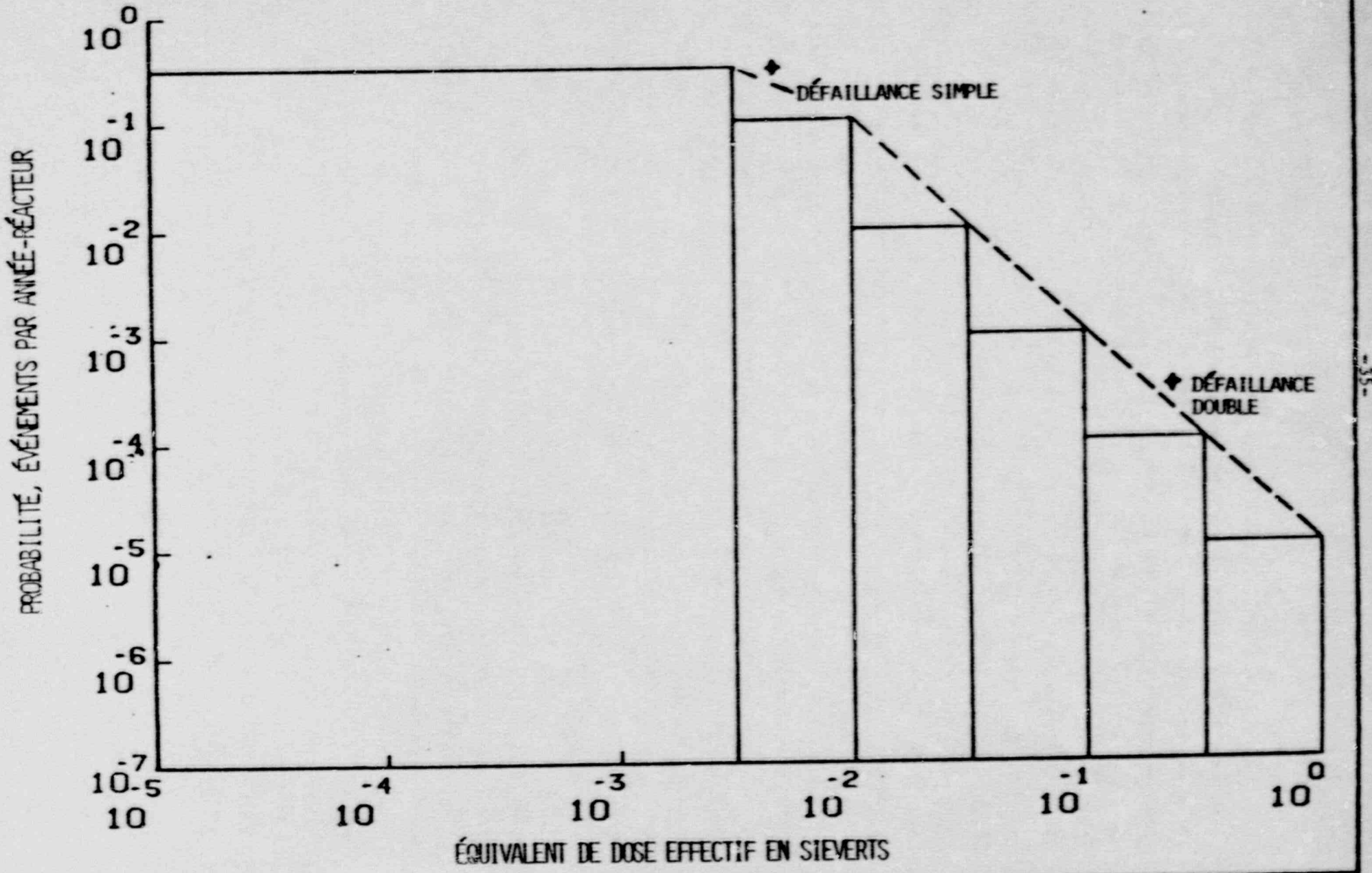
Dans la Figure 2, une ligne relie les limites supérieures des catégories de conséquences pour les probabilités limites. Cette ligne peut être interprétée comme représentant une approximation de la fonction cumulative complémentaire, comme cela est expliqué à la référence 22.

L'intégration appropriée de cette fonction fournit une mesure quantitative du risque prévu qu'une centrale nucléaire comporte (voir réf. 22).

La ligne limite de la Figure 2 présente une inclinaison de -1 depuis la catégorie 1 jusqu'à la catégorie 2, c'est-à-dire que ces deux catégories présentent des risques égaux. Pour les autres catégories, la ligne limite a une inclinaison de -2, ce qui entraîne un effet d'atténuation du risque proportionnel à l'augmentation des conséquences des accidents.

Le Tableau 5 donne la valeur maximale du risque total pour les six catégories et la compare aux valeurs prévues du risque données dans les recommandations du GTI et à celles qui correspondent au Guide d'emplacement

FIGURE 2 CATÉGORIES DE RISQUE PROPOSÉES POUR L'ANALYSE DES ACCIDENTS



de la CCEA*; le Tableau 5 donne aussi les risques associés à l'exploitation normale conforme à la limite réglementaire et au principe ALARA. On peut voir que le risque proposé dans le cas des séquences d'accidents est de la même ampleur que le risque encouru lors de l'exploitation normale conforme à la limite réglementaire. Il y a lieu de souligner que, généralement, une centrale nucléaire ne sera jugée acceptable que si la distribution des risques indiquée par les catégories du Tableau 4 est respectée, comme le stipule la section D.

Naturellement, compte tenu du Tableau 5, il faut reconnaître qu'il ne sera pas possible d'identifier et d'analyser toutes les séquences d'accidents possibles. (L'exigence D.2 reconnaît ce fait en précisant que le concepteur doit établir une liste de séquences de défaillances à analyser.) Par ailleurs, les séquences de défaillances ayant une probabilité inférieure à 10^{-7} ne seront pas incluses dans les analyses, tel que le stipule l'exigence D.5. De plus, tel qu'indiqué précédemment, il n'est pas toujours possible d'effectuer des analyses complètement réalistes et, dans de nombreux cas, il faudra recourir à des analyses de cas extrêmes. Pour toutes ces raisons, la valeur du risque total dΩ à des accidents de réacteur, tels que déterminés, ne peut pas représenter le véritable risque global dΩ aux accidents. Par conséquent, le fait de s'assurer que le risque calculé en question est inférieur au risque maximal stipulé au Tableau 5 n'assurera pas nécessairement que le risque réel dΩ aux accidents de réacteur est inférieur à la valeur susmentionnée. Néanmoins, le CCSN s'attend que le risque calculé soit du même ordre que le risque réel, à condition que des efforts consciencieux soient faits pour identifier et analyser des séquences d'accidents possibles et que, au besoin, on ait recours à des analyses de cas extrêmes. (Étant donné les raisons présentées ci-dessous, le fait de ne pas considérer les séquences d'accidents dont la probabilité est inférieur à 10^{-7} ne devrait avoir aucun effet important sur le risque calculé ou réel.) Le CCSN s'attend également que les différences existant entre le risque réel et le risque calculé diminueront à mesure qu'augmenteront les connaissances et l'expérience relatives à l'exploitation des réacteurs et à l'analyse des risques.

---

* Voir note au bas du Tableau 5, au sujet du risque maximal correspondant aux critères du Guide d'emplacement.

Pour donner une autre perspective à la valeur maximale calculée du risque résultant des présentes recommandations, il est à noter que le fond naturel de rayonnements au Canada expose les individus à un équivalent de dose moyen d'environ 10^{-3} sievert par année (voir réf. 23). Étant donné que, en moyenne, chaque individu reçoit cette dose, le risque associé est également de 10^{-3} sievert par année. En outre, cette valeur figure à titre de comparaison au Tableau 5. Il est possible de conclure que les critères proposés pour le risque prévu dû aux séquences d'accidents entraînent un risque au membre du public le plus fortement exposé, qui soit du même ordre que celui résultant du fond naturel de rayonnements.

La probabilité limite recommandée dans l'exigence D.5 est de 10^{-7} par année-réacteur, soit la même valeur que le GTI recommande. La conception d'une centrale nucléaire sera jugée acceptable si la probabilité d'un événement donné ou d'une séquence d'événements est égale ou inférieure à 10^{-7} par année-réacteur, quel que soit l'équivalent de dose effectif potentiel. Tel que mentionné ci-dessous, le CCSN croit que les séquences d'accidents ayant une probabilité équivalente ou inférieure à 10^{-7} par année-réacteur ne modifieront guère la valeur du risque total prévu encouru par le public. Cependant, le concepteur devrait fournir une assurance raisonnable à la CCEA qu'il en est ainsi.

La limite d'analyse en question peut être justifiée, entre autre, par le fait que les études générales les plus complètes concernant les risques que les réacteurs présentent, à savoir l'étude Rasmussen portant sur la sûreté des réacteurs aux États-Unis (voir réf. 24) et l'étude allemande concernant les risques (voir réf. 25) montrent que les courbes de risque de mortalité tardive pour les réacteurs à eau ordinaire deviennent très abruptes lorsque la probabilité d'une séquence d'accidents décroît en deça d'environ 10^{-6} par année pour les densités de population pondérées que l'on trouve aux environs des centrales nucléaires aux États-Unis et en République fédérale d'Allemagne. Ce comportement indique que des séquences d'accidents potentiels dont les probabilités sont inférieures à environ 10^{-6} par année modifient relativement peu le risque global.* Par ailleurs, ce

---

* Il est à noter que ces probabilités sont basées sur 100 réacteurs dans l'étude américaine et 25 réacteurs dans l'étude allemande.

comportement propose une limite supérieure à l'ampleur des conséquences de tout accident de réacteur qui n'est guère plus grande que celle associée à un événement ayant une probabilité de 10^{-6}.

Bien qu'aucune étude complète de ce genre n'ait été effectuée sur les risques des réacteurs CANDU, diverses études sur les conditions d'accident graves dans les réacteurs CANDU démontrent qu'il n'y aura pas de fusion du combustible, même dans le cas d'un accident grave dû à une perte de caloporteur combinée à une injection défectueuse de fluide de refroidissement d'urgence (voir réf. 26). Ce n'est pas le cas des réacteurs à eau ordinaire. Compte tenu de l'exigence selon laquelle les réacteurs CANDU doivent être munis de deux systèmes d'arrêt d'urgence indépendants, on croit en outre que la probabilité de la fusion du coeur qui résulterait de transitoires du réacteur sera moindre dans les réacteurs CANDU que dans les réacteurs à eau ordinaire. Par conséquent, on peut s'attendre que la probabilité totale de la fusion du coeur est moindre pour un réacteur CANDU que pour un réacteur à eau ordinaire. Étant donné que l'étude Rasmussen et l'étude allemande montrent qu'il n'y a pas de danger important pour le public à moins que la fusion du coeur ne se produise, il y a lieu de conclure que le risque global associé aux conditions accidentelles d'un réacteur CANDU ne sera pas plus grand que le risque associé aux conditions accidentelles d'un réacteur à eau ordinaire, particulièrement si l'on considère que la densité moyenne de la population au Canada est plus faible que celles des États-Unis ou de l'Allemagne de l'Ouest. Par conséquent, l'emploi des données provenant des études de risque faites par les États-Unis et la RFA pour appuyer le présent critère de sûreté destiné aux réacteurs CANDU, paraît pleinement justifié.

Une considération pratique pour l'établissement d'une limite d'analyse est que l'analyse des séquences d'accidents ayant une très faible probabilité devient très difficile et que les résultats seront très spéculatifs. Par conséquent, il est douteux que l'analyse de tels événements soit significative. En exigeant des analyses de ce genre, on pourrait détourner l'attention d'événements plus probables qui représentent en fait la principale contribution au risque global.

Dans l'exigence D.6, le recours à des conditions météorologiques ou à des conditions de dispersion réalistes dans le calcul des équivalents de dose, signifie que les probabilités de diverses conditions météorologiques doivent être prises en considération pour établir l'équivalent de dose le plus probable.

E. Construction

La construction qui, dans le présent contexte, comprend la fabrication des composants, représente l'exécution de la conception et, par conséquent, elle doit se faire de façon à ce que les exigences nominales soient respectées.

Les exigences E.1 et E.2 stipulent de bonnes méthodes de construction et de fabrication, ainsi que des techniques appropriées de contrôle et d'assurance-qualité.

L'exigence E.3 a pour but d'assurer que les méthodes de construction sur le chantier, par exemple en ce qui concerne la disposition des canalisations, ne compromettront pas le respect de l'exigence selon laquelle on ne doit pas nuire à la maintenance et aux inspections.

F. Mise en service

La mise en service comprend tous les essais, les examens et autres activités effectués avant l'exploitation commerciale pour s'assurer que la centrale, telle qu'elle est construite, répond à toutes les exigences nominales.

Les exigences F.1, F.2 et F.3 tiennent compte des aspects relatifs à la sûreté du programme de mise en service.

G. Exploitation

Au cours de l'exploitation d'une centrale nucléaire, on doit porter une attention continue aux opérations pour s'assurer que le réacteur fonctionne à l'intérieur de limites sûres et que tous les composants, systèmes et structures peuvent répondre aux exigences de sûreté qui leur sont propres.

L'exigence G.1 stipule que le titulaire de permis est le premier responsable de l'exploitation sûre de la centrale nucléaire.

L'exigence G.2 précise qu'il est nécessaire qu'un groupe indépendant, faisant partie de l'organisation du titulaire de permis, vérifie tous les aspects de la sûreté relatifs à l'exploitation de la centrale nucléaire.

L'exigence G.3 couvre la compétence et la formation des travailleurs sous rayonnements oeuvrant dans une centrale nucléaire. La compétence desdits travailleurs doit faire l'objet de contrôles périodiques et des périodes de recyclage doivent être préconisées au besoin.

L'exigence G.4 précise que tout le personnel d'une centrale nucléaire devra recevoir périodiquement une formation en radioprotection et en protection de la sûreté.

L'objectif de l'exigence G.5 est d'assurer que les méthodes d'exploitation sont telles qu'on n'emploiera pas comme travailleurs sous rayonnements des travailleurs qui n'en ont pas le statut, à moins de circonstances exceptionnelles.

L'exigence G.6 fait état du besoin d'élaborer, avant qu'une centrale nucléaire entre en service, de vastes contrôles administratifs pour assurer l'approbation appropriée des opérations et des méthodes détaillées d'exploitation.

Les méthodes et les limites d'exploitation visées à l'exigence G.7 doivent être définies par le titulaire de permis étant donné qu'elles relèvent de la responsabilité dudit titulaire qui doit veiller à l'exploitation sûre de la centrale, tel qu'indiqué à l'exigence G.1.

L'exigence G.8 précise qu'il est nécessaire de procéder à des inspections et à des essais périodiques de tous les systèmes spéciaux de sûreté et des composants apparentés à la sûreté pour fournir une assurance continue de leur qualité et de leur fiabilité.

Les exigences G.9 et G.10 stipulent la nécessité d'élaborer des plans et des lignes directrices à appliquer en cas d'urgence.

H. Gestion des déchets et des effluents

Tous les déchets radioactifs en provenance des centrales nucléaires doivent être traités de façon telle que leurs effets sur la population et l'environnement restent dans les limites réglementaires ou prescrites, et soient au niveau le plus faible qu'il soit raisonnablement possible d'atteindre. La gestion à long terme des déchets de haute activité doit faire appel à des installations spéciales qui devront être approuvées à cette fin.

L'exigence H.1 concerne le contrôle des rejets liquides et gazeux en conditions normales. Elle stipule que les doses au public, dues aux rejets, doivent répondre aux exigences de la section A.

L'exigence H.2 stipule qu'il faut prendre des dispositions pour l'évacuation des matières radioactives de façon à rendre lesdites matières irrécupérables.

L'exigence H.3 stipule qu'il faut établir des critères pour l'entreposage des déchets radioactifs dans une centrale nucléaire.

Les rejets de déchets non radioactifs en provenance des centrales nucléaires doivent être conformes aux limites prescrites par les autorités concernées.

I. Déclassement

Il faudrait tenir compte aux stades de la conception, de la construction et de l'exploitation, qu'il sera éventuellement nécessaire après l'exploitation d'une centrale nucléaire de la mettre dans un état sûr et de la maintenir ainsi et, au besoin, de remettre le site en état d'utilisation non restreinte.

Les exigences I.1 et I.2 visent à permettre d'atteindre ces objectifs. On ne prévoit pas que ces exigences présenteront de grandes difficultés, compte tenu de l'expérience déjà acquise à travers le monde en matière de déclassement des centrales nucléaires.

5.0 GLOSSAIRE

Activités normales d'une centrale nucléaire - Activités autres que l'exploitation normale d'une centrale nucléaire, comme la construction, la mise en service, la mise en attente, le déclassement et le démantèlement. (normale activities associated with a nuclear power plant)

ALARA - Principe de base de la radioprotection qui stipule que les rejets radioactifs en provenance des centrales nucléaires et l'exposition des personnes aux rayonnements doivent être maintenus au niveau le plus bas qu'il soit raisonnablement possible d'atteindre en deça des limites réglementaires, compte tenu de l'état de la technologie et des aspects économiques relatifs aux améliorations apportées à la santé et à la sécurité publiques, ainsi qu'à d'autres considérations socio-économiques et à l'utilisation de l'énergie nucléaire dans l'intérêt du public. (ALARA)

Atténuation du risque - Point de vue selon lequel un accident unique dont les conséquences sont très graves est plus indésirable que de nombreux petits accidents de moindre importance quant à leurs conséquences, même si le total des conséquences des nombreux petits accidents est égal ou comparable au total des conséquences de l'accident unique de grande envergure. (risk aversion)

CANDU - Filière électronucléaire développée au Canada. Elle utilise un réacteur à tubes de force, de l'eau lourde comme modérateur et de l'uranium naturel comme combustible; le réapprovisionnement en combustible se fait en cours de marche du réacteur. (CANDU)

Centrale nucléaire - Un ou plusieurs réacteurs à neutrons thermiques ainsi que toutes les structures, les systèmes et les composants nécessaires pour la sûreté et pour la production d'énergie sous forme de chaleur ou d'électricité. (nuclear power plant)

Cible - Condition qui, à la suite d'une entente, doit être réalisée autant que possible dans la conception ou dans l'exploitation d'une centrale nucléaire. Elle doit être différenciée d'une limite réglementaire qui, elle, doit être respectée en tout temps. (target)

Défaillance de cause commune - Défaillance d'au moins deux composants mis dans l'impossibilité de remplir leurs fonctions par suite d'une seule cause ou d'un seul événement précis. (common cause failure)

Défaillance de mode commun - Défaillance d'au moins deux composants qui se produit de manière identique. (common mode failure)

Défaillance opérationnelle grave - Défaillance d'un système opérationnel qui, en cas de défaillance de l'un des systèmes spéciaux de sûreté, entraînerait un rejet important de matières radioactives en provenance de la centrale nucléaire. (serious process failure)

Défaillance plausible - Défaillance d'un composant ou d'un système pouvant se produire dans des conditions raisonnablement présumées, avec une probabilité assez élevée pour justifier une analyse. (credible fault)

Défaillance corrélée - Défaillance d'un ou plusieurs composants résultant de la défaillance d'un autre composant. (cross-linked failure)

Déterministe - Lorsqu'elle s'applique à la conception et aux analyses de sûreté, la méthode déterministe ne tient formellement aucun compte des probabilités de diverses séquences d'événements. (deterministic)

Déviations opérationnelles prévues - Toutes les opérations qui dévient des conditions normales au-delà des conditions et des limites opérationnelles prescrites, et qui peuvent se produire une ou plusieurs fois pendant l'exploitation de la centrale, d'une part sans causer de dommage important aux systèmes spéciaux de sûreté et à l'équipement et aux systèmes reliés à la sûreté et, d'autre part, sans entraîner de séquences de défaillances tel qu'indiqué en D.2. (anticipated operational occurrences)

Dose à la population - Produit de la dose moyenne reçue par un membre d'une population donnée et du nombre de personnes dans cette population. Elle est mesurée en personnes-sieverts. On l'appelle également "dose collective". (population dose)

Dose absorbée - Quotient obtenu en divisant la quantité d'énergie absorbée dans le corps ou dans un organe ou tissu du corps due aux rayonnements ionisants, par la masse respective du corps, de l'organe ou du tissu. La dose absorbée s'exprime en grays, 1 gray étant égal à un joule par kilogramme. (absorbed dose)

Dose collective - Voir "Dose à la population". (collective dose)

Engagement d'équivalent de dose - Intégration à l'infini par rapport au temps du débit moyen d'équivalent de dose dQ à une pratique donnée, et reçu par un organe ou un tissu donné pour une population précise. (dose equivalent commitment)

Équivalent de dose - Produit obtenu en multipliant la dose absorbée dans le corps, dans un organe ou dans un tissu par un facteur de qualité qui rend compte du différent potentiel de lésion des divers types de rayonnements, et par un facteur représentant tous les autres facteurs de modification recommandés par la Commission internationale de protection radiologique. L'équivalent de dose s'exprime en sieverts (1 sievert équivaut à un joule par kilogramme). (dose equivalent)

Équivalent de dose effectif - Somme des équivalents de dose, en sieverts, pour chacun des divers organes ou tissus, multipliés par le facteur de pondération approprié à chaque organe ou tissu. Les facteurs de pondération que recommande la Commission internationale de protection radiologique (voir réf. 18) assurent un détriment égal, que le corps entier soit irradié uniformément ou non. (effective dose equivalent)

Équivalent de dose engagé - Équivalent de dose reçu par un organe ou un tissu donné qui sera accumulé pendant 50 ans, représentant une vie de travail, à partir d'une seule incorporation de matière radioactive dans le corps. (committed dose equivalent)

Ergonomie - Discipline s'occupant de l'interaction des êtres humains avec les systèmes technologiques, soit l'"interaction de l'homme et de la machine". (ergonomics)

État d'arrêt sûr - État dans lequel on maintient indéfiniment un réacteur à l'arrêt, de façon telle qu'un démarrage spontané soit impossible. (safe shut-down state)

Évacuation - Stockage des déchets nucléaires dans une installation ne permettant pas de les récupérer. L'installation est conçue de façon à assurer que tout rejet de radioactivité ou de matières radioactives hors de l'installation ne présente aucun danger important pour le public. (disposal)

Événement externe - Événement naturel ou provoqué par l'homme, engendré à l'extérieur d'une centrale nucléaire, pouvant nuire à la sûreté de la centrale, par exemple un tremblement de terre, une inondation, une tempête ou la chute d'un aéronef. (external event)

Événement interne - Événement se produisant à l'intérieur d'une centrale nucléaire et pouvant nuire à la sûreté de la centrale, par exemple un incendie ou une erreur commise par un opérateur. (internal event)

Exploitation normale - Exploitation d'une centrale nucléaire dans certaines conditions et limites opérationnelles et selon certaines déviations opérationnelles prévues comme le démarrage, le fonctionnement, la mise à l'arrêt, l'état d'arrêt, la maintenance et les essais. (normal operation)

Indisponibilité - Fraction de temps pendant laquelle un système ou un composant est dans l'impossibilité de fonctionner comme prévu à cause d'une défaillance, connue ou non, ou d'une réparation. (unavailability)

Point de déclenchement d'arrêt - Dans un instrument, le point de déclenchement est le niveau de la quantité mesurée par l'instrument qui provoquerait un arrêt automatique d'un réacteur nucléaire. (trip-point)

Points ou conditions de défaillance d'un système - Paramètres qui caractérisent l'état d'un système où des défaillances l'empêcheront de remplir ses fonctions. (failure points or conditions of a system)

Dose absorbée - Quotient obtenu en divisant la quantité d'énergie absorbée dans le corps ou dans un organe ou tissu du corps due aux rayonnements ionisants, par la masse respective du corps, de l'organe ou du tissu. La dose absorbée s'exprime en grays, 1 gray étant égal à un joule par kilogramme. (absorbed dose)

Dose collective - Voir "Dose à la population". (collective dose)

Engagement d'équivalent de dose - Intégration à l'infini par rapport au temps du débit moyen d'équivalent de dose dû à une pratique donnée, et reçu par un organe ou un tissu donné pour une population précise. (dose equivalent commitment)

Équivalent de dose - Produit obtenu en multipliant la dose absorbée dans le corps, dans un organe ou dans un tissu par un facteur de qualité qui rend compte du différent potentiel de lésion des divers types de rayonnements, et par un facteur représentant tous les autres facteurs de modification recommandés par la Commission internationale de protection radiologique. L'équivalent de dose s'exprime en sieverts (1 sievert équivaut à un joule par kilogramme). (dose equivalent)

Équivalent de dose effectif - Somme des équivalents de dose, en sieverts, pour chacun des divers organes ou tissus, multipliés par le facteur de pondération approprié à chaque organe ou tissu. Les facteurs de pondération que recommande la Commission internationale de protection radiologique (voir réf. 18) assurent un détriment égal, que le corps entier soit irradié uniformément ou non. (effective dose equivalent)

Équivalent de dose engagé - Équivalent de dose reçu par un organe ou un tissu donné qui sera accumulé pendant 50 ans, représentant une vie de travail, à partir d'une seule incorporation de matière radioactive dans le corps. (committed dose equivalent)

Ergonomie - Discipline s'occupant de l'interaction des êtres humains avec les systèmes technologiques, soit l'"interaction de l'homme et de la machine". (ergonomics)

État d'arrêt sûr - État dans lequel on maintient indéfiniment un réacteur à l'arrêt, de façon telle qu'un démarrage spontané soit impossible. (safe shut-down state)

Évacuation - Stockage des déchets nucléaires dans une installation ne permettant pas de les récupérer. L'installation est conçue de façon à assurer que tout rejet de radioactivité ou de matières radioactives hors de l'installation ne présente aucun danger important pour le public. (disposal)

Événement externe - Événement naturel ou provoqué par l'homme, engendré à l'extérieur d'une centrale nucléaire, pouvant nuire à la sûreté de la centrale, par exemple un tremblement de terre, une inondation, une tempête ou la chute d'un aéronef. (external event)

Événement interne - Événement se produisant à l'intérieur d'une centrale nucléaire et pouvant nuire à la sûreté de la centrale, par exemple un incendie ou une erreur commise par un opérateur. (internal event)

Exploitation normale - Exploitation d'une centrale nucléaire dans certaines conditions et limites opérationnelles et selon certaines déviations opérationnelles prévues comme le démarrage, le fonctionnement, la mise à l'arrêt, l'état d'arrêt, la maintenance et les essais. (normal operation)

Indisponibilité - Fraction de temps pendant laquelle un système ou un composant est dans l'impossibilité de fonctionner comme prévu à cause d'une défaillance, connue ou non, ou d'une réparation. (unavailability)

Point de déclenchement d'arrêt - Dans un instrument, le point de déclenchement est le niveau de la quantité mesurée par l'instrument qui provoquerait un arrêt automatique d'un réacteur nucléaire. (trip-point)

Points ou conditions de défaillance d'un système - Paramètres qui caractérisent l'état d'un système où des défaillances l'empêcheront de remplir ses fonctions. (failure points or conditions of a system)

Probabiliste - Lorsqu'elle s'applique à la conception et aux analyses de sûreté, la méthode probabiliste prend en considération les probabilités de diverses séquences d'événements. (probabilistic)

Probabilité - Propriété numérique se rattachant à une activité ou à un événement et permettant d'évaluer les chances que cette activité ou cet événement se produise. (probability)

Public (membre du) - Toute personne autre qu'un travailleur sous rayonnements. (public (member of))

Risque - Produit de la probabilité d'un événement et de l'ampleur des conséquences résultant dudit événement. (risk)

Système opérationnel - Système requis pour l'exploitation normale du réacteur, par exemple le circuit primaire de caloportage et le système de régulation du réacteur. (process system)

Travailleur sous rayonnements - Toute personne qui, dans l'exploitation de son entreprise ou au cours de son travail ou de son occupation, est susceptible de recevoir une dose de rayonnements ionisants dépassant toute dose indiquée à la colonne IV de l'annexe II du Règlement (DORS/74-334, Gazette du Canada, Partie II, volume 108, n° 12, 4 juin 1974, dans sa version modifiée) établi conformément à la Loi sur le contrôle de l'énergie atomique. (atomic radiation worker)

6.0 RÉFÉRENCES

1. Projet de déclaration de principe sur les objectifs de sûreté relatifs aux activités nucléaires au Canada, Rapport du Comité consultatif de la sûreté nucléaire, CCSN-2, INFO-0055(F), juin 1981, modifié en avril 1982.

2. Paskievici, W., "Risks from Energy Production and Supply", Risk-Risque, Compte-rendu d'un symposium relatif à l'évaluation et à la perception du risque pour la santé humaine au Canada, octobre 1982. J.T. Rogers et D.V. Bates (éd.), Société royale du Canada, Conseil des sciences du Canada, avril 1983.

3. Cohen, A.V. et D.K. Pritchard, Comparative Risk of Electricity Production Systems: A Critical Survey of the Literature, Research Paper N° 11, UK Health and Safety Executive, décembre 1980.

4. Niehaus, F. et A. Novegno, "Optimal Allocation of Resources for Safety", Risk-Risque, Compte-rendu d'un symposium relatif à l'évaluation et à la perception du risque pour la santé humaine au Canada, octobre 1982. J.T. Rogers et D.V. Bates (éd.), Société royale du Canada, Conseil des sciences du Canada, avril 1983.

5. Hamilton, L.D., "Comparative Risks from Different Energy Systems: Evolution of the Methods of Studies", Nuclear Safety, vol. 24, n°2, mars-avril 1983.

6. McConnell, L.G., L.W. Woodhead, G.R. Fanjoy, CANDU Operating Experience, IAEA-CN-42/68, Proceedings of International Conference on Nuclear Power Experience, vol. 2, p. 103, Agence internationale de l'énergie atomique, Vienne, septembre 1982.

7. Revue de l'industrie nucléaire; problèmes et perspectives 1981-2000, ministère de l'Énergie, des Mines et des Ressources, Canada, 1982.

8. Siddall, E., Risques, craintes et sécurité du public, EACL-7404, avril 1981.

9. Siddall, E., Safety Policy in the production of Electricity, Proceedings of the International Meeting on Thermal Nuclear Reactor Safety, Chicago, septembre 1982.

10. Meinel, M.P. et A.B. Meinel, "Energy for the Future: The World View", Annals of Nuclear Energy, vol. 10, nos 3-4, 1983, p. 209.

11. Laurence, G.C., Reactor Siting in Canada, L'Énergie atomique du Canada, Limitée, document n° AECL-1375, octobre 1961.

12. Siddall, E. et W.B. Lewis, Reactor Safety Standards and their Attainment, AECL-498, septembre 1957.

13. Siddall, E., "Statistical Analysis of Reactor Safety Standards", Nucleonics, vol. 17, n° 2, février 1959, p. 64-69.

14. CCEA, Reactor Siting and Design Guide, novembre 1964.

15. Hurst, D.G. et F.C. Boyd, Reactor Licensing and Safety Requirements, Document présenté à la conférence de l'Association nucléaire canadienne, AECB-1059, juin 1972.

16. Paskievici, W., Exigences proposées en matière de sûreté pour l'obtention du permis d'exploitation d'une centrale nucléaire CANDU, Rapport du Groupe de travail interorganisationnel, CCEA-1149, novembre 1978.

17. Paskievici, W., Proposed General Principles and Safety Requirements for CANDU Nuclear Power Plants, Proceedings of Symposium on CANDU Reactor Safety Design, Association nucléaire canadienne, novembre 1978.

18. CIPR, Annales de la CIPR, Recommandations de la Commission Internationale de Protection Radiologique, Publication CIPR 26, vol. 1, n°3, Pergamon Press, 1977.

19. CCEA, L'Analyse de sûreté des centrales nucléaires CANDU, document de consultation n°C-6, (ancien Guide d'autorisation n°39), juin 1980.

20. Webb, J.R., Protection from Common Mode Events, Proceedings of Symposium on CANDU Reactor Safety Design, Association nucléaire canadienne, novembre 1978.

21. Duncan, D.S., Conditions of Design for Thermal Reactors, A Revised Approach, Generic Atomic Company, San Diego, California, GA-A14131, août 1977.

22. Cox, D.C. et P. Baybutt, "Limit Lines for Risk", Nuclear Technology, vol. 57, juin 1982, p. 320.

23. Butler, C.C., La radioactivité dans l'environnement canadien, Comité associé sur les critères scientifiques concernant l'état de l'environnement, Conseil national de recherches du Canada, CNRC n°18135, 1980.

24. Reactor Safety Study. An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400, août 1975.

25. The German Risk Study, Sommaire, ministère fédéral de la Recherche et de la Technologie, août 1979.

26. Meneley, D.A. et W.T. Hancox, LOCA Consequence Predictions in a CANDU-PHWR, Paper 145, IAEA International Conference on Nuclear Power Experience, Vienne, septembre 1982.