



Consultative Document Document de consultation



Atomic Energy
Control Board

Commission de contrôle
de l'énergie atomique

CONSULTATIVE DOCUMENT C-6

Proposed Regulatory Guide

REQUIREMENTS FOR THE SAFETY ANALYSIS
OF CANDU NUCLEAR POWER PLANTS

Issued for comment:

June, 1980

Canada

ATOMIC ENERGY CONTROL BOARD

REQUIREMENTS FOR THE SAFETY ANALYSIS OF CANDU NUCLEAR POWER PLANTS

TABLE OF CONTENTS

PREFACE

- 1.0 Introduction
- 2.0 Definitions
- 3.0 Basic Requirements
- 4.0 General Analysis Requirements
- 5.0 Safety Analysis Rules
- 6.0 Safety Analysis Reporting Requirements
- 7.0 References

TABLE 1 Specified Events Required to Meet Table 2 Reference
Dose Limits

TABLE 2 Safety Analysis Class/Consequence Table

TABLE 3 Specified Non Design Basis Events

PREFACE

1. Siting, design, manufacture, construction, commissioning, operation, and decommissioning of nuclear facilities, or the production, possession, use and disposal of prescribed substances, in Canada or under Canadian control, are subject to the provisions of the Atomic Energy Control Act and Regulations administered by the Atomic Energy Control Board (AECB).
2. In addition to the Atomic Energy Control Regulations, three other categories of Regulatory Document are employed by the AECB. These are:

Generic Licence Conditions - standard sets of conditions that are included in particular AECB licences of a common type, unless specific circumstances indicate otherwise;

Regulatory Policy Statements - firm expressions that particular "requirements" not expressed as Regulations or Licence Conditions be complied with or that any requirements be met in a particular manner but where the AECB retains the discretion to allow deviations or to consider alternative means of attaining the same objectives where a satisfactory case is made; and

Regulatory Guides - guidance or advice on any aspect of the AECB's regulatory process that is given in a manner less rigid than that intended by Policy Statements.

3. In developing Regulatory Documents, the AECB publishes its proposals as Consultative Documents in order to solicit comments both from the nuclear industry and from the public. This is done prior to releasing any Regulatory Document in final form. In certain cases, after the period for public comment, a Consultative Document may be issued for "trial use". This is done for a limited period of time to gain practical experience. Following the period of trial use, the revised document is re-issued for further public comment prior to release in final form.
4. Comments on Consultative Documents and suggestions for new Regulatory Documents and for improvement to those that exist are encouraged and should be directed to the Regulations Development Section of the AECB.
5. Copies of Consultative Documents, Regulatory Documents and related index lists are available in both English and French on request from the Office of Public Information. Requests for technical information on and interpretation of documents should be addressed to this office.
6. The Atomic Energy Control Board may be contacted as follows:

Postal address: Atomic Energy Control Board
 P.O. Box 1046
 Ottawa, Ontario
 K1P 5S9
 CANADA

Telephone
General Inquiries: (613) 995-5894

REQUIREMENTS FOR THE SAFETY ANALYSIS OF CANDU NUCLEAR POWER PLANTS

1.0 INTRODUCTION

This document is intended to cover all CANDU designs of the type currently undergoing licensing in Canada. Since its degree of applicability to other designs will vary, the AECB should be consulted prior to an application to construct being made for any other type of reactor.

The effective date of this document shall be July 1, 1980 for all nuclear power plants not holding a Construction Licence at that time.

2.0 DEFINITIONS

2.1 Serious Process Failure

A serious process failure is any failure of process equipment or procedure which, in the absence of Special Safety System action, could lead to significant fuel failures in the reactor or a significant release of radioactive material from the station.

For the purpose of this definition:

- (a) significant fuel failures means fuel failures to the extent that the Iodine-131 content of the reactor coolant is increased by 500 curies or more.
- (b) significant release of radioactive material is one which would result in a whole body dose to the most exposed member of the public at or beyond the site boundary in excess of 0.0005 SV (50 mrem) or 0.005 SV (500 mrem) to the thyroid assuming Pasquill F weather conditions.

2.2 Special Safety Systems

The Special Safety Systems shall include:

Reactor Shutdown Systems

Emergency Core Cooling System

Containment System.

2.3 Process Protective Actions

Process protective actions are actions performed by process equipment which can reduce the frequency of serious process failures or reduce the demands placed on the special safety systems.

2.4 Safety Support Actions

Safety support actions are actions performed by equipment or structures which assist or support the Special Safety Systems in limiting the consequences of serious process failures.

2.5 Common Cause Effects

Common cause effects are effects manifested in more than one piece of equipment or structure by the same cause. Examples of such causes are aircraft crashes; earthquakes; tornadoes; fires; a common hostile environment; common design weaknesses; and common fabrication, installation, operation, or maintenance errors.

2.6 Cross-Link Effects

Cross-link effects are those effects resulting from a lack of independence or separation, either physical or functional, between systems or components or operating actions.

2.7 Normal Electrical Power

Normal electrical power is the electrical power supplied from the station turbine-generator(s) or the electrical power grid to which the station is connected.

2.8 Fire Zone

A fire zone is that portion of the plant which is separated from other zones by fire-resistant boundaries.

2.9 Design Basis Fire

The most severe fire that could occur within a fire zone.

2.10 Fire-Resistant Boundaries

Fire-resistant boundaries are physical barriers or distance which can contain the design basis fire within the fire zone.

Fire-resistant boundaries may take into account active and passive fire protection means.

3.0 BASIC REQUIREMENTS

3.1 A safety analysis shall be completed to show that the operation of the station will not pose an unacceptable risk to the public.

3.2 The safety analysis shall include:

(a) a review of the plant design, operational procedures and potential external influences to identify:

- i) all serious process failures resulting from failure of a single component or system,
- ii) all combinations of single component failures or single system failures resulting in serious process failures,
- iii) all events of i) and ii) above combined with the failure or unavailability of systems or equipment whose action would mitigate the consequences of these events,

which may pose a comparable or greater risk to the public than the events specified in Table 1.

This review shall incorporate the events specified in Table 1 and shall show that as far as practicable all potential external influences, failure initiating mechanisms internal to the plant, common cause effects and cross-link effects have been taken into account.

(b) the analysis of all events specified in Table 1. Such analysis shall demonstrate that the relevant dose limits specified in Table 2 are not exceeded and shall show, by comparison with other specified events, that the events should not be placed in a lower Table 1 class number.

(c) the analysis of all events identified in accordance with Section 3.2(a) but not specified in Table 1. Such analysis shall demonstrate that the risk posed to the public by these events is not greater than that of the events specified in Table 1.

(d) the analysis of all events specified in Table 3. The analysis of these events shall meet the requirements of Sections 3.3, 4, 5, and 6 except that the consequences shall be calculated assuming the postulated containment impairment exists for five days.

3.3 The analysis of each of the events as required by Section 3.2 shall:

- (a) determine that the reactor can be made and maintained safely subcritical;
- (b) be carried out to the point where it is shown that the reactor has achieved a safe thermal equilibrium state.
- (c) identify the reactor heat sinks credited from the start of the serious process failure until the reactor has reached a safe thermal equilibrium state;
- (d) for each of the heat sinks determined in accordance with Section 3.3(c), identify the heat transfer routes from the reactor fuel to the ultimate heat sink and evaluate the heat transferred via each route;
- (e) determine the dose to the most exposed member of the public at or beyond the site boundary either:
 - i) for 30 days from the time at which the event occurs; or
 - ii) until the dose rate to the most exposed member of the public at or beyond the site boundary is not greater than 0.0001 SV (10 mrem) per week whole body and 0.001 SV (100 mrem) per week to the thyroid;whichever is the greater time period.
- (f) show that equipment and structures required to operate following an event can be maintained.

3.4 Massive failure of all pressure vessels shall be analyzed unless it can be demonstrated that such a failure is of an acceptably low expected frequency of occurrence. If this is to be achieved, the following shall be taken as minimum requirements:

- (a) design, fabrication, installation and operation in accordance with the requirements of Section III Class I of the ASME code and other requirements as the AECB may deem appropriate;
- (b) the vessel connections are relatively few (reactor headers shall not be considered as vessels for the purpose of safety analysis);
- (c) an in-place inservice inspection program;
- (d) a critical crack length such that a detectable leak will occur at normal operating pressure well in advance of the critical crack length being reached.
- (e) equipment in place which will detect the presence of a leak (as identified in accordance with Section 3.4(d)) and alert the operator, and to have procedures for action to be taken following the detection of a leak.

4.0 GENERAL ANALYSIS REQUIREMENTS

The following requirements pertain to the events requiring analysis under Section 3.2;

- 4.1 Each event shall be analyzed crediting the following:
- (a) each reactor shutdown system in turn;
 - (b) of the reactor shutdown system assumed available, the less effective of the two trip parameters provided in accordance with the requirements of Reference 3.
- 4.2 Each event shall be analyzed with and without credit for process protective actions and with action by process systems where it cannot be shown by inspection that such actions would be beneficial. For events specified in Table 1, the reference dose limits given in Table 2 shall apply to both of the above postulated cases. For events identified in accordance with the requirements of Section 3.2(a) the same approach shall apply.
- 4.3 The analysis of each event shall include the determination of the following except for those items which are not applicable:
- (a) the reactor physics transient;
 - (b) the transient behaviour of the reactor fuel;
 - (c) the reactor trip times for:
 - i) the full range of reactor power
 - ii) the full range of failure potential of the event;
 - (d) the pressure and temperature transients of the pressure retaining components showing that the appropriate service limits of the applicable code for pressure retaining components are not exceeded;
 - (e) the pressure, temperature and flow transients within the pressure retaining systems which affect the outcome of the event.

- (f) the pressure, temperature and flow transients within containment;
- (g) the release of radioactive material from the fuel;
- (h) the release of radioactive material into containment;
- (i) the distribution of radioactive material within containment;
- (j) the release of radioactive material from containment;
- (k) the necessary operator actions, indications available to identify the need for such action, and the period of time between the indication and the point when the operator must begin taking action.

4.4 The values of input parameters used in the analysis of each event shall ensure that the predictions of consequences is conservative and applicable at all times by taking account of:

- (a) the different plant states for which continued operation will be permitted by the operating procedures;
- (b) the uncertainties associated with each parameter.

4.5 Mathematical models and associated calculational methods used shall satisfy the following requirements:

- (a) conservative prediction is obtained;
- (b) all important physical phenomena shall be represented;
- (c) simplifications shall be justified as being appropriate and conservative;
- (d) adequate numerical accuracy shall be demonstrated;
- (e) as far as practicable mathematical modes shall be verified by operating experience or experimental evidence;

(f) changes, arising from the event, in the effectiveness of processes shall be accounted for. These shall include but not be limited to:

i) adverse environmental conditions such as steam, dousing, flooding and radiation.

ii) changes in support system performance e.g. electrical power, cooling water and instrument air supplies.

4.6 Empirical correlations shall be conservatively based on relevant experiments done, to the extent practicable, in the applicable range of operating parameters. Scaling of results beyond the range of experimental data must be justified.

4.7 Where neither a mathematical model nor a correlation is suitable to simulate a physical phenomenon, limiting assumptions shall be used, such that the prediction is demonstrably conservative.

4.8 The analysis of each event shall consider the partial and total loss of the function provided by the component or systems whose failure defines the event. The worst case shall meet the applicable reference dose limits given in Table 2. Where only the worst case is analyzed the basis on which it is chosen shall be given.

4.9 The analysis of each event shall include the determination of:

a) the expected frequency of occurrence of the event taking into account all credible failure mechanisms as far as practicable.

b) the credible event sequences following the event for the time specified under Section 3.3(e) taking into account as far as practicable:

- i) the event initiating mechanisms,
- ii) common cause effects,
- iii) cross-link effects,
- iv) operator errors,
- v) equipment unavailability.

4.10 The analysis of events for which it is desired to take credit for the continued availability of normal electrical power shall include the following:

- (a) analysis assuming the continued availability of normal power except where Reference 1, 2 or 3 specify that such power shall not be credited.
- (b) a reliability analysis determining the likelihood of continued availability of normal electrical power during the event taking into account common cause and cross-link effects.
- (c) analysis assuming the failure of all sources of normal electrical power supply to the unit.

In determining the appropriate event class for the combination, the credit given the availability of normal electrical power shall take into account the outcome of the reliability analysis of Section 4.10(b) but shall not exceed that given by the following table:

| <u>Initiating Event Class</u> | <u>Event Class for Combination</u> |
|-------------------------------|------------------------------------|
| 1 | 3 |
| 2 | 4 |
| 3 | 5 |
| 4 | 5 |
| 5 | 5* |

* Where it can be shown that the occurrence of the event and normal electrical power failure is of an order of likelihood less than that expected for Class 5 events, the combined failure need not be analyzed.

4.11 Pipe failure analysis shall consider both circumferential and longitudinal failures at any location in a system.

(a) For circumferential pipe failures a discharge area up to and including twice the cross-sectional area of the pipe shall be analyzed.

(b) Failures resulting from longitudinal cracks shall also be considered and justification given for the maximum crack size postulated.

4.12 The analysis of all events leading to calculated fuel sheath failures shall assume the maximum steam generator tube leakage for which continued reactor operation is permitted.

4.13 The analysis of each event shall only take credit for the continued operation of equipment which is both designed and qualified to withstand the effects of the event.

4.14 In the analysis of each event, the credited effectiveness of equipment shall be based on:

(a) for process systems, the minimum intended operational availability.

(b) for special safety systems, the minimum allowable performance standards specified in accordance with the requirements of Reference 1, 2 and 3.

(c) performance to an acceptable confidence level.

5.0 SAFETY ANALYSIS RULES

The applicant shall define the rules that lay out the principles and practices which will be followed in the safety analysis to ensure that the requirements of Sections 3 and 4 will be met. Such rules shall be approved by the AECB and shall include but not be limited to:

(a) the method of review of the plant design, operational procedures, and potential external influences to ensure the requirements of Section 3.2(a) are met;

(b) the method of categorization of the events and event combinations identified in accordance with Section 3.2(a) into the classes of Table 1;

(c) the method of taking into account common cause and cross-link effects.

- (d) the assumptions regarding safety support actions and process protective actions;
- (e) the assumptions regarding the responses (both success and failure) of all operationally and functionally interrelated systems, equipment and structures;
- (f) the application of the service limits of the applicable code for pressure retaining components to the events defined by Section 3.2;
- (g) the assumed response of the operator taking into account items such as plant indications, response time and procedures;
- (h) the treatment of the subsequent effects of pressure boundary failures such as pipe whip, jet impingement forces, high temperature, flooding and radiation;
- (i) the method of selection of input parameter values to satisfy the requirements of Section 4.4. These methods shall address but not be limited to input parameters such as:
 - weather conditions,
 - reactor power,
 - maximum channel power,
 - fission product inventory of the core,
 - tritium content of the moderator system
 - plant operating mode (reactor leading or following turbine),
 - reactor core flow rate,
 - reactor main coolant system temperature and pressure,
 - steam generator pressure and level,
 - dousing tank water level,

coolant void reactivity coefficient

trip signal delays,

shut-off rod characteristics,

fuel temperature coefficient,

flux distribution in the core.

(j) the use of mathematical models, associated calculational methods, and empirical correlations which satisfy the requirements of Sections 4.5, 4.6 and 4.7.

(k) assumptions in the analysis pertaining to the operation of overpressure relief devices, in particular for the following:

- failure to open when called upon
- failure to reclose.

6.0 SAFETY ANALYSIS REPORTING REQUIREMENTS

6.1 General

6.1.1 Sufficient information shall be submitted to the AECB to show that the requirements of Sections 3, 4 and 5 have been met such that a comprehensive independent assessment of the adequacy and acceptability of the analysis can be done.

6.2 Additional Specific Reporting Requirements

The following apply to the reporting of the analysis of each of the events required under Section 3.2:

- (a) a listing of the input assumptions and data;
- (b) an estimate of the uncertainty in the results with identification of the contributing factors;

- (c) a listing of the conservatisms (this should include factors of conservatism used in correlations, mathematical models and failure rates with the rationale for the values chosen);
- (d) a listing of the mathematical models, calculational methods and correlations used indicating the range and conditions of applicability of each;
- (e) a listing of the parameters to which the results are relatively sensitive including the degree of sensitivity of each;
- (f) identification of simplifications and approximations used in mathematical models and calculational methods;
- (g) an estimation of the numerical accuracy of the calculational methods.

6.3 Mathematical Models, Calculational Methods and Correlations

Each mathematical model, calculational method and correlation used in the safety analysis of the plant shall be documented and submitted to the AECB. They shall reference all the material on which the models are based. In the case of computerized models the program descriptions and computer listings shall be submitted.

7.0

REFERENCES

Reference 1

Criteria for Reactor Containment Systems for Nuclear Power Plants
Atomic Energy Control Board - October 16, 1979.

Reference 2

Requirements for Emergency Core Cooling Systems for Candu Nuclear
Power Plants

Atomic Energy Control Board - November 27, 1979.

Reference 3

Requirements for Shutdown Systems for Candu Nuclear Power Plants
Atomic Energy Control Board - January 2, 1980.

TABLE 1

SPECIFIED EVENTS REQUIRED TO MEET TABLE 2 REFERENCE DOSE LIMITS

NOTES:

- (a) Not all events in this table will be applicable to a specific design.
- (b) Where more than one process system is provided to carry out a function, each fully capable and available, and where each can be shown to be sufficiently independent and diverse that the failure of one cannot result in failure of the other(s), the failure of only one needs to be postulated as a single process failure.
- (c) The multiple events involving failure of subsystems of Special Safety Systems assume sufficient independence and diversity between the subsystems that each may be considered as a Special Safety System for the purpose of safety analysis. Where such independence and diversity cannot be shown the analysis must assume failure of all such subsystems. (For example, under Class 5 a feeder failure is to be analyzed with a failure of rapid cooldown of the steam generators and separately with a failure to close of the isolation devices on the interconnects between the reactor main coolant loops. If there is insufficient independence and diversity between the subsystems giving rapid cooldown and loop isolation, then a feeder failure is to be analyzed with failure of rapid cooldown and failure of loop isolation.)
- (d) Where more than one subsystem of a Special Safety System is provided to perform a safety function and each subsystem has a high degree of independence and diversity from each other, then each may be considered as a Special Safety System for the purpose of safety analysis. For such designs, events specifying the failure of a Special Safety System function need only consider the failure of each of the subsystems in turn.

Class 1

Failure of control¹

Failure of normal electrical power

Failure of the normal steam generator feedwater flow

Failure of a service water flow²

Failure of the instrument air

Failure of reactor moderator flow

Turbine-generator load rejection

Fuelling machine backing off the reactor without the fuel channel
assembly closure plug being replaced

Failure of a single steam generator tube

Failure resulting in the opening of the instrumented pressure relief
valves of the reactor main coolant system

Failure of the cooling of a fuelling machine when off reactor
containing a full complement of irradiated fuel

Failure resulting in the opening of a pressure relief valve in a
subatmospheric pressure containment system³

Failure at any location of any small pipe connected to the reactor
main coolant system (such as an instrument line) where crimping is
the accepted method of isolation⁴.

Class 2

Failure at any location of any reactor fuel channel assembly feeder pipe (hereafter referred to as "feeder failure")

Failure of the end fitting of any reactor fuel channel assembly (hereinafter referred to as "end fitting failure")

Failure of the pressure tube of any reactor fuel channel assembly followed immediately by the failure of the calandria tube through which the pressure tube runs (hereafter referred to as "pressure tube/calandria tube failure")

Flow blockage in any single reactor fuel channel assembly

Seizure of a single reactor coolant main circulating pump

Failure resulting in the opening of the instrumented pressure relief valves of the reactor main coolant system + failure of the relief valves on the blowdown tank to reclose

Failure of all mechanical seals on a reactor main coolant pump

Failure at any location of any pipe or component in the system which controls the inventory and pressure in the reactor main coolant system

Failure at any location of any pipe of the service water systems

Design basis fires

Class 3

Failure at any location of any pipe of the reactor main coolant system considering failure sizes from the size greater than a fuel channel assembly feeder up to and including the largest pipe (hereafter referred to as a "reactor main coolant system large LOCA")⁵

Failure of a large number of steam generator tubes⁶

Failure at any location of any pipe or header carrying steam from the steam generators to the turbine generator

Failure at any location of any pipe or header carrying feedwater to the steam generators

Failure at any location of any pipe of the reactor moderator system

Failure of control of the reactor main coolant pressure and inventory control system + failure of the reactor main coolant system instrumented pressure relief valves to open

Failure of the end fitting of any fuel channel assembly followed immediately by the failure of the lattice tube of the end shield through which the end fitting runs (hereafter referred to as "end fitting/lattice tube failure")⁷

Design Basis Earthquake

Failure of a large number of tubes in any heat exchanger, except the steam generators, which is connected to the reactor main coolant system⁸

Class 4

Fuelling machine backing off the reactor without the fuel channel assembly closure plug being replaced plus each of the following in turn:

- failure of emergency coolant injection
- failure to close of the isolation devices on the interconnects between the reactor main coolant loops
- failure of rapid cooldown of the steam generators

Class 4 (Continued)

- one door open of the airlock or transfer chamber most critical for radioactive releases from containment and the seals on the second door deflated
 - failure to close of the containment isolation devices associated with a single containment subsystem for the subsystem most critical for radioactive releases from containment
 - degraded operation of containment atmosphere cooling equipment
 - for a subatmospheric pressure containment system, failure of one bank of pressure relief valves with operation of the second bank at the minimum level acceptable for continued station operation
 - for a subatmospheric pressure containment system, failure of the bypass relief valves to open on increasing or decreasing pressure in the valve manifold
 - the largest containment leak that could not be detected quickly by a monitoring system, or the largest leak for which continued reactor operation for more than four hours would be proposed
 - failure of containment dousing assuming the more severe of the following:
 - i) a douse has occurred prior to the accident
 - ii) the dousing system is unavailable following the accident
- Failure of the cooling of a fuelling machine when off reactor containing a full complement of irradiated fuel plus each of the following in turn:
- failure to close of the containment isolation devices associated with a single containment subsystem for the subsystem most critical for radioactive releases from containment

Class 4 (Continued)

- one door open of the airlock or transfer chamber most critical for radioactive releases from containment and the seals on the second door deflated

Failure of the drive shaft of a reactor coolant main circulating pump

Class 5

Failure inside containment of any pipe or header carrying steam from the steam generators to the turbine-generator plus

Failure at any location of any pipe or header carrying feedwater to the steam generators plus

Failure of all mechanical seals on a reactor main coolant pump plus

Feeder failure plus

Flow blockage in any single reactor fuel channel assembly plus

End fitting failure plus

End fitting/lattice tube failure plus

Pressure tube/calandria tube failure plus

Reactor main coolant system large LOCA plus

Failure at any location of a pipe in the system which controls the pressure and inventory in the reactor main coolant system plus

each of the following in turn:

- failure of emergency coolant injection
- failure to close of the isolation devices on the interconnects between the reactor main coolant loops
- failure of rapid cooldown of the steam generators
- one door open of the airlock or transfer chamber most critical for radioactive releases from containment and the seals on the second door deflated

Class 5 (Continued)

- failure to close of the containment isolation devices associated with a single containment subsystem for the subsystem most critical for radioactive releases from containment
- degraded operation of containment atmosphere cooling equipment
- for a subatmospheric pressure containment system, failure of one bank of pressure relief valves with operation of the second bank at the minimum level acceptable for continued station operation
- for a subatmospheric pressure containment system, failure of the bypass relief valves to open on increasing or decreasing pressure in the valve manifold
- the largest containment leak that could not be detected quickly by a monitoring system or the largest leak for which continued reactor operation for more than four hours would be proposed
- failure of containment dousing assuming the more severe of the following:

1) a douse has occurred prior to the accident

ii) the dousing system is unavailable following the accident

Failure of a large number of steam generator tubes⁹ plus each of the following in turn:

- failure of rapid cooldown of the steam generator
- failure of emergency coolant injection
- failure to close of the isolation devices on the interconnects between the reactor main coolant loops
- failure to close of the isolation devices on the pipe carrying steam from the steam generators

Class 5 (Continued)

Failure of a large number of tubes in any heat exchanger, except the steam generators, which is connected to the reactor main coolant system¹⁰ plus each of the following in turn:

- failure of rapid cooldown of the steam generators
- failure of emergency coolant injection
- failure to close of the isolation devices on the interconnects between the reactor main coolant loops
- failure to close of the isolation devices on the pipes carrying service water to and from the heat exchangers

Design Basis Earthquake plus each of the following in turn:

- one door open of the airlock or transfer chamber most critical for radioactive releases from containment and the seals on the second door deflated
- failure to close of the containment isolation devices associated with a single containment subsystem for the subsystem most critical for radioactive releases from containment
- degraded operation of containment atmosphere cooling equipment
- for a subatmospheric pressure containment system, failure of one bank of pressure relief valves with operation of the second bank at the minimum level acceptable for continued station operation
- for a subatmospheric pressure containment system, failure of the bypass relief valves to open on increasing or decreasing pressure in the valve manifold
- the largest containment leak that could not be detected quickly by a monitoring system, or the largest leak for which continued reactor operation for more than four hours would be proposed

Class 5 (Continued)

- failure of containment dousing assuming the more severe of the following:

i) a douse has occurred prior to the DBE

ii) the dousing system is unavailable following the DBE

| | |
|-----------------------------------------------------------|------|
| Flow blockage in any single reactor fuel channel assembly | plus |
| End fitting failure | plus |
| Pressure tube/calandria tube failure | plus |
| Feeder failure | plus |

- for a subatmospheric pressurized containment, pressure in the main vacuum building chamber at atmospheric pressure prior to the accident

Turbine-generator load rejection + failure of turbine overspeed protection

Turbine breakup

Design Basis Tornado

Failure of the mechanical joint between the pump cover and the pump casing of a reactor coolant main circulating pump

Large load dropped on the reactor reactivity mechanism deck¹¹

Failure of a steam generator support¹¹

Massive failure of the pump casing of a reactor coolant main circulating pump¹¹

Massive failure of the pump cover of a reactor coolant main circulating pump¹¹

Massive failure of the station cooling water intake tunnel¹¹

Massive failure of the station cooling water discharge duct¹¹

FOOTNOTES

1. "Failure of control" denotes the loss of the ability of control equipment to maintain system or equipment operation in a predetermined state. "Failure of control" shall include:
 - 1.1 Failure of reactivity control including:
 - a) positive reactivity insertion from all power levels for normal and distorted flux shapes at a range of rates up to and including the maximum credible rate
 - b) positive reactivity insertion to give a constant log rate for a range of log rates up to a value just below the point at which the automatic neutron detection devices of the Special Safety Systems would shut down the reactor
 - c) positive reactivity insertion at a range of rates up to and including the maximum credible rate while the reactor is subcritical.
 - 1.2 Failure of computer control (except as covered by Section 1.1 above) including:
 - i) failure to control a single parameter
 - ii) sudden total computer control failure
 - iii) gradual computer control deterioration leading to total control failure*
 - iv) failure to control more than a single parameter*
 - v) programming errors*
 - 1.3 Failure of each analogue control system.

* Specific cases within these categories may be placed in other than Class 1.

FOOTNOTES (Continued)

2. "Service water" is the water normally taken from the sea, lake or river and used directly for the cooling of plant equipment.
3. This event shall be shown not to result in a serious process failure or damage to the Special Safety Systems
4. The reference dose limit shall be shown not to be exceeded during the period in which the reactor is shut down consequent to the failure, and the crimping is executed. The system which controls the inventory and pressure in the reactor main coolant system may not be credited during this period.
5. The analysis shall assume the reactor coolant main circulating pumps do not continue to operate unless the following can be shown to the satisfaction of the AECB:
 - a) the main circulating pumps are qualified to run under the conditions of a large LOCA
 - b) cavitation effects will not trip the main circulating pumps
 - c) administrative rules ensure the pumps will not be shutdown during that portion of the event where their continued operation is credited.Where the above have been shown to the satisfaction of the AECB, reactor main coolant system large LOCA + loss of reactor coolant main circulating pumps must be considered as a Class 4 event.
6. For this event the consequences of failure of a large number of steam generator tubes shall be determined and justification given for the number of tubes chosen.

FOOTNOTES (Continued)

In addition, the following shall be shown:

- a) the number of steam generator tubes required to fail in order to exceed the capability of the pressure and inventory control system of the reactor main coolant system assuming it operates as designed.
 - b) the number of steam generator tube failures necessary to result in calculated fuel sheath failures.
7. This analysis is not required if it can be shown that a lattice tube cannot fail following the failure of the end fitting or pressure tube of any fuel channel assembly.
 8. The consequences of failure of a large number of heat exchanger tubes shall be determined and justification given for the number of tubes chosen.
 9. The number of steam generator tubes failed shall be those determined in accordance with the requirements of Footnote 6.
 10. The number of heat exchanger tubes failed shall be those determined in accordance with the requirements of Footnote 9.

FOOTNOTES (Continued)

11. For each of these events either of the following shall be shown:
- a) the consequences will not exceed the Class 5 reference dose limits
 - b) the postulated event should not be regarded as a design basis event and therefore does not require consequence analysis. To be considered, arguments supporting this position shall include:
 - design, manufacture, installation and operating considerations and features
 - the predicted failure frequency based upon direct operating experience or reasonable extrapolation therefrom.

TABLE 2

Safety Analysis Class/Consequence Table

The following table gives the maximum permissible reference doses to the most exposed member of the public at or beyond the site boundary for each class of postulated event.

| <u>Class</u> | <u>Reference Dose Limit</u> | |
|--------------|-----------------------------|------------------------|
| | <u>Whole Body</u> | <u>Thyroid</u> |
| 1* | .0005 Sv (50 mrem) | 0.005 Sv (500 mrem) |
| 2* | 0.005 Sv (500 mrem) | 0.05 Sv (5 rem) |
| 3 | .03 Sv (3 rem) | 0.3 Sv (30 rem) |
| 4 | 0.1 Sv (10 rem) | 1.0 Sv (100 rem) |
| 5 | 0.25 Sv (25 rem) | 2.5 Sv (250 rem) |

* Class 1 and Class 2 events other than single channel events shall be shown to have no systematic fuel pin failures.

TABLE 3

SPECIFIED NON DESIGN BASIS EVENTS

The events of Table 3 consist of those single failures combined with massive containment impairments which could result in very large releases of radioactive material from containment. These events are not considered as design basis because of their expected very low frequency of occurrence.

However, in the interest of fully assessing the risk to the public posed by the station, the consequences of these very low probability events shall be determined. The AECB shall judge the acceptability of the consequences of these events on a case-by-case basis.

| | |
|-----------------------------------------------------------|------|
| Flow blockage in any single reactor fuel channel assembly | plus |
| End fitting failure | plus |
| Pressure tube/calandria tube failure | plus |
| Reactor main coolant system large LOCA | plus |

each of the following in turn:

- total failure of containment atmosphere cooling equipment
- both doors open of the airlock or transfer chamber most critical for the release of radioactive material from containment.