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

R-7

Regulatory Document

Requirements for Containment Systems for CANDU Nuclear Power Plants

A Regulatory Policy Statement

Effective date: February 21, 1991

Canada

TABLE OF CONTENTS

This document is part of a set of regulatory documents
relating to the safety requirements for CANDU nuclear power plants:

R–7, *Requirements for Containment Systems for CANDU Nuclear Power Plants*
R–8, *Requirements for Shutdown Systems for CANDU Nuclear Power Plants*
R–9, *Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants*

These documents apply to reactors licensed for construction after January 1, 1981.

REQUIREMENTS FOR CONTAINMENT SYSTEMS FOR CANDU NUCLEAR POWER PLANTS

1. DEFINITIONS*

In this document,

"closed system" means a piping system which penetrates and forms a closed loop or an enclosed volume either inside or outside the containment structure. For closed systems inside containment, the fluid in the system does not directly communicate with either the primary coolant or the containment atmosphere; (*système fermé*)

"containment envelope" means structures and appurtenances which provide a pressure-retaining barrier to prevent or limit the escape of any radioactive matter that could be released from the fuel elements, as a result of a failure in a fuel cooling system; (*enceinte de confinement*)

"containment structure" means the concrete portion and embedded parts of the containment system; (*structure de confinement*)

"fuel cooling system" means any cooling system whose failure has the potential for release of radioactive material in excess of the limits given in the reference. Included would be the primary heat transport system, any booster fuel cooling system, and the fuelling machine cooling system. Excluded would be the irradiated fuel bay cooling system; (*système de refroidissement du combustible*)

"minimum allowable performance standards" means the set of operating limits or the range of conditions established for components or subsystems which define the minimum acceptable states for those components or subsystems as credited in the safety analyses; (*normes de rendement minimal admissible*)

"primary heat transport system" means that system of components which permit the transfer of heat from the fuel in the reactor to the steam generators or other heat exchangers employing secondary cooling. For purposes of this document, it does not necessarily include auxiliary purification and pressure control subsystems; (*circuit caloporteur primaire*)

"special safety system" means one of the following systems: shutdown systems, containment system, emergency core cooling system. (*système spécial de sûreté*)

2. BASIC REQUIREMENTS

2.1 All water-cooled nuclear power reactors shall be installed within a containment structure. All piping which is part of the main circuit of the primary heat transport system, excluding boiler tubing, shall be totally within the containment structure.

2.2 (a) Except as noted in paragraph (b), all equipment required for correct operation of the containment system shall be considered to be part of that system and shall meet all requirements of this document. This shall include:

(i) the containment structure and appurtenances,

(ii) equipment required to isolate the containment envelope and assure its completeness and continuity following an accident,

(iii) equipment required to reduce the pressure or the free radioactive material within the containment envelope, and

(iv) equipment required to limit the release of radioactive material from the containment envelope following an accident.

---

* These definitions do not constitute a complete list of terms used in this document, but are included to clarify the meaning of some terms for the assistance of the reader. A more comprehensive list of definitions of terms relating to CANDU nuclear power plants is available from the Canadian Standards Association (CSA), *Manual of Definitions for CSA Nuclear Standards Use by CSA Technical Committees*, CSA–N9409A–1989.

(b) Equipment required to supply compressed air, electrical power or cooling water to equipment for operation of the containment system shall be considered as safety support equipment. Such equipment shall meet all relevant requirements of this document with the exception of sections 3.8 and 3.13.

2.3 The containment system shall be considered to be a special safety system.

2.4 Procedures to ensure compliance with the requirements of this regulatory policy statement shall be prepared by the licensee and shall require the approval of the Atomic Energy Control Board (AECB) prior to the issuance of a construction approval (procedures relating to part 3) or an operating licence (procedures relating to parts 4 and 5)

3. DESIGN REQUIREMENTS

3.1 Containment Envelope

There shall be a clearly defined continuous containment envelope which is capable of limiting to an acceptably low value the release of radioactive material from the station for all postulated failures of a fuel cooling system as specified in Table 1. The boundary of this containment envelope shall be defined for all conditions which could exist in the operation or maintenance of the reactor, or following an accident.

3.2 Design Information

3.2.1 The Safety Report shall clearly state the values of, and bases for, the following containment system design parameters:

(a) positive design pressure(s);

(b) negative design pressure(s) where applicable, and

(c) the maximum allowable leakage rate at the positive design pressure.

3.2.2 Minimum allowable performance standards shall be defined for the containment system and shall be listed or referenced in the Safety Report and in the Operating Policies and Principles for the plant. The minimum allowable performance standards shall also be specified for all major equipment and subsystems necessary for correct operation of the containment system.

3.2.3 A report shall be submitted which clearly identifies the containment envelope as described in section 3.1.

3.3 Dose Limits under Accident Conditions

The containment system shall be capable of limiting the release of radioactive material such that the reference dose limits are not exceeded.*

3.4 Structural Integrity

3.4.1 The positive design pressure of each part of the containment envelope shall be not less than the highest pressure which could be generated in that part as a result of any postulated events specified in Tables 1 and 2 for which radioactive material may be released into the containment envelope.

3.4.2 The negative design pressure of each part of the containment envelope shall not be greater than the lowest pressure which could be generated in that part as a result of any postulated event as specified in Tables 1, 2, 3 and 4.

3.4.3 It shall be shown that, for all events specified in Tables 1, 2, 3 and 4, the structural integrity of containment will not be impaired to a degree that consequential damage to reactor systems could result.

3.4.4 It shall be shown that, for all events specified in Tables 1, 2 and 3, no damage to the containment structure will occur.

3.5 Leakage Criteria

3.5.1 The maximum allowable leakage rate from the containment envelope shall be the value used in the safety analyses which demonstrate that the reference dose limits are not exceeded.

3.5.2 A test acceptance leakage rate shall be established, giving the maximum acceptable leakage rate under actual measurement tests. The margin between the maximum allowable leakage rate defined in subsection 3.5.1 and the test acceptance leakage rate shall require approval by the AECB prior to the first leakage rate tests.

---

* This regulatory document does not define comprehensive requirements for safety analysis and reference dose limits. The reference dose limits referred to in section 3.3 are those contained in the reference, or any subsequent AECB regulatory document, or as otherwise agreed in writing between the licensee and the AECB.

3.6 Environmental Requirements

3.6.1 All parts of the containment system which may be required to operate, or to continue operating, in response to any event specified in Tables 1, 2, 3 and 4 shall be designed to meet all necessary performance requirements while subjected to the most severe environmental conditions which could be present when or before such operation is required. These conditions may include, but are not necessarily limited to, the effects of debris, steam, water, high temperature, radiation, and pressure differentials.

Qualification is required for all containment equipment which may be required to operate, or to continue operating, following exposure to any of the above conditions. Qualification shall consist of tests to demonstrate to the extent practicable that the type of equipment can operate under conditions similar to those which would exist during or following the events listed in Tables 1, 2, 3 and 4. Where such tests are impracticable, analysis is required to demonstrate that this requirement is met.

3.6.2 The containment system shall be designed such that, for all events specified in Tables 1, 2, 3 and 4, dynamic effects or jet forces caused by the event cannot result in impairment of the containment system to an extent that the relevant requirements in subsections 3.3, 3.4 and 3.5 would not be met.

3.7 Availability Requirements

3.7.1 The containment system shall be designed such that the fraction of time for which it is not available can be demonstrated to be less than 10^{-3} years per year. The system shall be considered available only if it can be demonstrated to meet all the minimum allowable performance standards as defined in accordance with subsection 3.2.2.

The availability of safety support equipment necessary for correct operation of the containment system shall be commensurate with the availability requirements of the containment system.

Availability calculations to demonstrate that this requirement can be met shall be included or referenced in the Safety Report. Such calculations shall be based on direct experience or reasonable extrapolations therefrom.

3.7.2 The design of the containment system and safety support equipment shall take into account the long-term reliability requirements of those components which must continue to function following an accident. Standards for the long-term reliability of such components shall be prepared and shall require approval by the AECB prior to the issuance of a construction approval.

3.7.3 The design shall have sufficient redundancy such that no failure of any single component of the containment system can result in impairment of the system to an extent that it will not meet its minimum allowable performance standards under accident conditions.

This requirement does not apply to components which are not required to change state and which do not depend on safety support equipment in order to perform their design functions, provided that they are designed, manufactured, inspected and maintained to standards acceptable to the AECB.

3.7.4 Correct operation of the containment system following an accident shall not be dependent on power supplies from the electrical grid or from the turbine generators associated with any reactor unit within that containment system.

3.7.5 As far as practicable, all containment equipment shall be designed such that its most probable failure modes will not result in a reduction in safety.

3.7.6 As far as practicable, the design shall be such that all maintenance and unavailability testing which may be required when the containment is required to be available can be carried out:

(a) without impairment of the containment envelope, and

(b) without a reduction in the effectiveness of the containment system below its minimum allowable performance standards.

3.7.7 As far as practicable, the design shall be such that a failed component can be put into a safe state, or such that the failure can be converted to a safe failure in some other manner.

3.7.8 The design shall be such that all necessary actions of containment equipment which are initiated by automatic control logic in response to an accident can also be initiated manually from the appropriate control room.

3.8 Separation and Independence Requirements

3.8.1 As far as practicable, the containment system shall be physically and operationally independent from other special safety systems. No equipment which is part of the containment system shall be used as part of another special safety system.

3.8.2 As far as practicable, the containment system shall be independent from all process systems. This requirement does not apply to equipment discussed in subparagraphs 2.2(a)(iii) and (iv) provided that such equipment is normally operating when the reactor is operating.

3.8.3 Design principles for separation of redundant instrument channels and the services to them, associated with the containment system, shall be prepared and shall require approval by the AECB prior to the issuance of a construction approval.

3.8.4 If subsystems of containment are considered to be independent for the purpose of the safety analyses, principles for separation and independence of such subsystems shall be prepared and shall require approval by the AECB prior to the issuance of a construction approval.

3.9 Requirements for Penetrations of the Containment Structure

Piping systems which penetrate the containment structure shall be designed to meet the requirements specified in the Appendix.

3.10 Containment Atmosphere Control

3.10.1 Systems shall be incorporated into the containment design to assist in the control of the internal pressure and to control the release of radioactive material to the environment following an accident.

3.10.2 Provision shall be made for controlling the concentration of hydrogen and/or oxygen following an accident to prevent explosion or deflagration, unless it is demonstrated that there is no possibility of such an explosion or deflagration as a result of any event specified in Table 1.

3.10.3 The design of the plant shall be such that, following an accident, it is possible to isolate all engineered sources of compressed air and other non-condensable gases leading into the containment atmosphere, other than those required for the operation of necessary equipment.

3.11 Shielding Requirements

3.11.1 The design of the containment system and associated equipment shall incorporate sufficient provision for shielding to ensure that radiation fields would not be excessive in areas of the plant to which access might be required following an accident.

3.11.2 A report demonstrating the adequacy of the shielding provisions* shall be prepared and shall specify:

(a) the postulated accident which results in the largest release of radioactive material inside the containment envelope;

(b) all areas to which access might be required following such an accident, with the frequency and duration of necessary access, and

(c) the maximum radiation fields expected in such areas when access might be required.

3.12 Status Monitoring Requirements

3.12.1 The design shall be such that the status of all important equipment can be monitored or inferred from the appropriate control room.

3.12.2 The design shall be such that any gross breach of the containment envelope can be readily and reliably detected.

3.13 Codes and Standards

3.13.1 The application for a construction approval shall identify any aspects of the design which fail to comply with the applicable requirements of the following codes and standards:

(a) CSA N287: Series on *Concrete Containment Structures for CANDU Nuclear Power Plants*, and

(b) CAN3–N285.0: ***General Requirements for Pressure-Retaining Systems and Components in CANDU Nuclear Power Plants.***

All exceptions to the requirements of these standards shall require approval by the AECB prior to their implementation.

---

* Equipment required only for shielding purposes need not be considered as part of the containment system.

3.13.2 A list of additional codes and standards to be applied to the containment system and the extent of their application shall be prepared and shall require approval by the AECB prior to the issuance of a construction approval.

3.14 Seismic Requirements

All parts of the containment system credited in the safety analysis following a design basis seismic ground motion for that plant site shall be designed to remain fully functional following such an event.

4. OPERATING REQUIREMENTS

4.1 Requirements for Normal Operation

4.1.1 The containment system shall not be intentionally made unavailable, unless all of the following conditions are met:

(a) all reactors within the containment envelope are in a guaranteed shutdown state approved by the AECB,

(b) all reactor cooling systems are sufficiently cooled and depressurized in accordance with procedures approved by the AECB, and

(c) all irradiated fuel within the containment envelope is adequately cooled and has an alternate cooling supply available.

Procedures for intentionally making the containment system unavailable shall be prepared and shall require the approval of the AECB prior to the issuance of an operating licence.

The containment system shall be considered to be available only when it meets all the minimum allowable performance standards as defined in accordance with subsection 3.2.2.

4.1.2 Procedures for taking corrective action, in the event that the containment system is found to be impaired when the conditions mentioned in subsection 4.1.1 are not met, shall be prepared and shall require approval by the AECB prior to the issuance of an operating licence.

4.1.3* If any component of the containment system is found to be inoperable or impaired below its minimum allowable performance standards, the component and its associated equipment shall, as far as practicable, immediately be put in a safe condition, except as approved in accordance with subsection 4.1.2.

4.1.4* As far as practicable, maintenance on a containment system component shall be carried out only when that component and its associated equipment have been put in a state which does not reduce the availability of the containment system.

4.1.5* If redundant components require maintenance, each component shall be thoroughly tested following its maintenance prior to the start of work on a subsequent component.

4.1.6 When maintenance on a component is completed, it shall be tested to the extent practicable to demonstrate that it and its associated equipment function in accordance with design requirements.

4.1.7 The standard of maintenance shall be such that the reliability and effectiveness of all equipment, as claimed in the Safety Report and other documentation in support of an operating licence, are assured.

4.2 Requirements for Accident Conditions

If operator action is required for actuation of any containment equipment, all of the following requirements must be met:

(a) there shall be instrumentation to give the operator clear and unambiguous indication of the necessity for operator action;

(b) the reliability of such instrumentation shall be commensurate with the requirements for availability of the containment system as specified in section 3.7. If indication of only a single parameter is required, the instrumentation shall be part of the containment system;

(c) there shall be 15 minutes available following such clear and unambiguous indication before the operator action is required, and

(d) there shall be clear, well-defined and readily available operating procedures to identify the necessary actions.

---

* Requirements 4.1.3, 4.1.4 and 4.1.5 do not apply during periods when the containment system has been made unavailable in accordance with procedures approved pursuant to subsection 4.1.1.

5. TESTING REQUIREMENTS

5.1 Commissioning Tests

5.1.1 Pressure Proof Tests

Prior to first criticality of any reactor, positive pressure proof tests shall be done to demonstrate the structural integrity of all parts of the containment envelope and the containment system. If the design specifications include a negative design pressure, a negative pressure proof test shall also be done.

Positive pressure proof tests shall be done at a pressure not less than 1.15 times the positive design pressure for each part of the containment envelope.

Negative pressure proof tests shall be done at a pressure not greater than the negative design pressure.

If any of the above tests are impracticable, testing of representative equipment in a laboratory may be accepted, if approved by the AECB.

5.1.2 Leakage Rate Tests

Prior to first criticality of any reactor, the leakage rate of its containment envelope shall be measured to demonstrate that it is not greater than the test acceptance leakage rate. Measurements shall be made at a range of pressures up to and including the positive design pressure for each part of the containment envelope. The test shall be conducted with containment components in a state sufficiently representative of those which would exist following an accident to demonstrate that the appropriate leakage rate would not be exceeded under such conditions.

Testing of individual penetrations, isolating devices and airlocks shall be done for those penetrations for which it is necessary to obtain baseline leakage measurements against which the future in-service leakage tests specified in subsection 5.2.4 may be compared.

5.1.3 Tests of Containment Equipment

Prior to first criticality of any reactor, tests of the containment system equipment shall be performed to verify that all design requirements have been achieved. Exceptions to this requirement will be allowed only if it is shown to the satisfaction of the AECB that some operational characteristics are impracticable to demonstrate under non-accident conditions or that such tests would have a detrimental effect on safety.

5.1.4 Wiring Tests

Prior to first criticality of any reactor, tests shall be carried out on all electrical wiring associated with the containment system to demonstrate that all connections are in accordance with the design.

5.2 In-Service Tests and Inspections

5.2.1 Pressure Proof Tests

Pressure proof tests, as specified in subsection 5.1.1, shall be repeated following any major modification of the containment envelope or after the containment system has been subjected to elevated pressure differentials as a result of an accident or after the containment system has been subjected to any severe environmental effects.

5.2.2 Leakage Tests

In-service leakage rate tests shall be carried out in accordance with one of the following alternative methods:

(a) a leakage rate test shall be carried out at full design pressure at least once every three years to demonstrate that the measured leakage rate is not greater than the maximum allowable leakage rate. If the measured leakage rate is in excess of the test acceptance leakage rate, the frequency of such tests shall be increased to once every two years, or

(b) a leakage rate test shall be carried out at a frequency of not less than once per two years to demonstrate that the leakage rate is not greater than the maximum allowable leakage rate. Such tests may be carried out at reduced or negative pressures. However, if the test results, when extrapolated to full design pressure, indicate leakage in excess of the test acceptance leakage rate, a leakage rate test at the full positive design pressure shall be carried out to demonstrate that the maximum allowable leakage rate is not exceeded. A leakage test at full design pressure shall be carried out a minimum of once per six years in any case.

In addition to the above routinely scheduled leakage rate tests, a leakage rate test at the full design pressure shall be performed in conjunction with any pressure proof test required under subsection 5.2.1.

5.2.3 Containment Equipment

To the maximum extent practicable (see subsection 5.1.3), tests to demonstrate that containment equipment meets its minimum allowable performance standards shall be carried out at a frequency of not less than once per six years.

5.2.4 Tests of Penetrations and Isolating Devices

An in-service test program for penetrations, airlocks and isolating devices shall be prepared. The program shall detail for each type of penetration, isolating device and airlock to be tested, the nature of the test, test frequency, and leakage acceptance criteria. This program shall require the approval of the AECB prior to the issuance of an operating licence.

5.2.5 Visual Inspections

External visual inspections of the containment envelope, including appurtenances and penetrations shall be carried out in conjunction with each of the tests required by subsections 5.2.1, 5.2.2 and 5.2.4.

The interior of this envelope shall be visually inspected at a frequency and to an extent approved by the AECB prior to the issuance of an operating licence.

5.2.6 Reporting Requirements

The results of all in-service tests and inspections of the containment system shall be reported in the annual reports for the station.

5.3 Availability Tests

5.3.1 All containment equipment shall be monitored or tested at a frequency which is adequate to demonstrate compliance with the availability requirements specified in subsection 3.7.1.

5.3.2 A report on the availability of the containment system shall be included in each annual report on the operation of the station. This report shall include:

(a) a statement of the total fraction of time in the year during which the containment system was not demonstrated to be available, as defined in subsection 3.7.1. Only periods during which the containment system is intentionally made unavailable, in accordance with the conditions of section 4.1, shall be excluded from such calculations,

(b) a comparison of the failure modes and failure frequencies observed in operation of the station with the failure modes and failure frequencies used in the availability calculations prepared in accordance with subsection 3.7.1, and

(c) availability calculations sufficient to demonstrate that the availability requirement of subsection 3.7.1 can continue to be satisfied based on observed failure modes and failure frequencies.

REFERENCE

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

TABLES *

TABLE 1

1. Failure of any pipe or header in any fuel cooling system
2. Failure of a pressure tube and the associated calandria tube
3. Failure of an end fitting
4. Fuel channel flow blockage
5. Failure of a fuelling machine to replace a closure plug
6. Inadvertent opening of pressure relief or control valves on the primary heat transport system or associated systems
7. Failure of steam generator tubes
8. Any of events 1 to 7 occurring coincidentally with impairment of the emergency core cooling system
9. Inadvertent opening of pressure relief valves connecting to a vacuum building

TABLE 2

Any of events 1 to 7 in Table 1 accompanied by complete failure of dousing.

TABLE 3

Failure of any pipe in the steam generator feedwater or steam systems.

TABLE 4

Failure of any pipe in the steam generator feedwater or steam systems accompanied by complete failure of dousing.

---

* In these tables, "failure" means both total failure and partial failure.

APPENDIX

REQUIREMENTS FOR METAL EXTENSIONS OF THE CONTAINMENT ENVELOPE

1. CODE REQUIREMENTS

Systems or portions of systems which form part of the containment envelope shall be constructed to the requirements of the *ASME Boiler and Pressure Vessel Code*, Section III, Division 1, Subsection NC (Class 2 components) or Subsection NE (Class MC components) except for:

(a) those systems whose process requirements are Class 1 or 2 in accordance with CAN3–N285.0;

(b) those closed systems inside the containment structure which have a design pressure greater than 0.5 MPa(g) and are continuously operated at or above the positive design pressure of the containment at all points in the system, and which can be monitored for leaks. Such systems may be constructed to the process systems requirements, but they shall be constructed to not less than the non-nuclear requirements of CSA B51.

Closed systems inside the containment structure which do not meet the requirements in paragraphs (a) and (b) may be built to the requirements of Class 3 if it can be shown to the satisfaction of the AECB that, due to smallness of size or other factors, the proposed design provides an adequate barrier.

2. ISOLATION

Piping systems shall be provided with isolation devices having redundancy, reliability, and performance capabilities which reflect the importance to safety of isolating the various types of piping systems penetrating containment. Where isolation in a piping system is provided by valves, provisions shall be made to test the valve operability periodically, to check that the valve leakage is within acceptable limits and to allow maintenance of the valve without causing a breach of the containment envelope. In order for a manual isolation valve to be considered closed, it shall be either locked closed or continuously monitored to show that the valve is in the closed position.

The various types of piping systems penetrating containment shall be provided with the following isolation unless it can be shown that, for a specific type of line, other isolation provisions would be acceptable.

2.1 Primary Heat Transport Auxiliary Systems Penetrating Containment

Each line that is connected to the primary heat transport system pressure boundary and that penetrates the containment structure shall be provided with two isolation valves in series. The valves shall normally be arranged with one inside and one outside the containment structure. If it can be shown that two valves inside the containment structure or two valves outside the containment structure can provide an equivalent barrier in certain applications, then this may also be an acceptable arrangement.

A check valve may be used as one of the isolation barriers but it shall be located inside the containment structure. Two check valves in series are not considered an acceptable barrier.

Where the valves provide isolation of the heat transport system during normal operation of the station, then both valves shall normally be in the closed position.

Systems directly connected to the heat transport system and which may be open during normal operation of the station shall also be provided with the same isolation as the normally closed system except that manual isolating valves inside the containment structure shall not be used. At least one of the two isolation valves shall be either an automatic isolation valve (for instance, a check valve) or a powered isolation valve operable from the control room.

For small lines of 25 mm in nominal diameter or less, a single closed isolation valve inside containment may be used provided the line is connected to a closed system outside containment.

The line up to and including the second isolation valve, or the first valve in the case of small lines 25 mm in nominal diameter or less shall be constructed to the requirements of Class 1 in accordance with CAN3–N285.0.

2.2 Systems Connected to Containment Atmosphere

Each line that connects directly to the containment atmosphere, that penetrates the containment structure, and that is not part of a closed system, shall be provided with two isolation barriers as follows:

(a) two automatic isolation valves in series for those lines which may be open to the containment atmosphere;

(b) two closed isolation valves in series for those lines that are normally closed to the containment atmosphere;

(c) one closed isolation valve for lines of 50 mm in nominal diameter or less, which are normally closed to the containment atmosphere and connected to an easily defined closed system outside containment.

The line up to and including the second valve, or the first valve in the case of paragraph (c), shall be part of the containment envelope and shall be constructed to the requirements of *ASME Code*, (Section III, Class 2).

2.3 Closed Systems

Closed systems inside or outside the containment structure which form part of the containment envelope and which meet the requirements of Class 2 and can be continuously monitored for leaks need no further isolation. All other closed systems shall be provided with a single isolation valve on each line penetrating containment. The valves shall be located outside containment as close as practicable to the containment structure. Valves required for process purposes may be used as the isolation valves for these closed loops.

2.4 Small Lines

For ductile piping of small bore, crimping of the pipe is a possible means of providing an isolation barrier instead of a valve. For this to be acceptable, the details of its application shall be submitted for approval in each case of its proposed use. In particular, the method of crimping, the location of the part to be crimped and the method of identifying the failed line shall be shown to be satisfactory. In the case of primary heat transport system instrument lines, the following extra conditions are required:

(a) space must be available for crimping the tubes where they penetrate through the containment structure.

(b) the quality of the lines is to be as good as the rest of the primary heat transport system.

(c) the relevant release limits must 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, and

(d) any outflow from the breaks can be filtered before release to the atmosphere to control the escape of fission products.

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

R-8

Regulatory Document

Requirements for Shutdown Systems for CANDU Nuclear Power Plants

A Regulatory Policy Statement

Effective date: February 21, 1991

Canada

TABLE OF CONTENTS

This document is part of a set of regulatory documents
relating to the safety requirements for CANDU nuclear power plants:

R–7, *Requirements for Containment Systems for CANDU Nuclear Power Plants*
R–8, *Requirements for Shutdown Systems for CANDU Nuclear Power Plants*
R–9, *Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants*

These documents apply to reactors licensed for construction after January 1, 1981.

This regulatory document is the second document issued by the AECB on the subject of shutdown system requirements. It does not conflict with the previous one, AECB Regulatory Document R–10, *The Use of Two Shutdowns Systems in Reactors*, which was issued in January 1977.

REQUIREMENTS FOR SHUTDOWN SYSTEMS FOR CANDU NUCLEAR POWER PLANTS

1. DEFINITIONS*

"minimum allowable performance standards" means the set of operating limits or the range of conditions established for components or subsystems which define the minimum acceptable states for those components or subsystems as credited in the safety analyses; *(normes de rendement minimal admissible)*

"primary heat transport system" means that system of components which permit the transfer of heat from the fuel in the reactor to the steam generators or other heat exchangers employing secondary cooling. For purposes of this document, it does not necessarily include auxiliary purification and pressure control subsystems; *(circuit caloporteur primaire)*

"special safety system" means one of the following systems: shutdown systems, containment system, emergency core cooling system; *(système spécial de sûreté)*

"fuel failure" means any rupture of the fuel sheath such that fission products may be released. *(défaillance de combustible)*

2. BASIC REQUIREMENTS

2.1 All CANDU nuclear power reactors shall be equipped with two independent and diverse shutdown systems,** each of which must conform to the requirements of this document.

2.2 Each shutdown system shall be a special safety system.

2.3 Procedures to ensure compliance with the requirements of this regulatory policy statement shall be prepared by the licensee and shall require the approval of the Atomic Energy Control Board (AECB) prior to the issuance of a construction approval (procedures relating to part 3) or an operating licence (procedures relating to parts 4 and 5).

3. DESIGN REQUIREMENTS

3.1 Minimum Allowable Performance Standards

Minimum allowable performance standards shall be defined for each shutdown system and shall be listed or referenced in the Safety Report and in the Operating Policies and Principles for the plant. The minimum allowable performance standards shall also be specified for all major equipment necessary for correct operation of each shutdown system.

3.2 Performance Requirements***

3.2.1 For events specified in Tables 1 and 2 requiring prompt shutdown action, each shutdown system shall be designed such that, acting alone, it can ensure that:

(a) the reactor is rendered subcritical and is maintained subcritical;

(b) the reference dose limits are not exceeded,**** and

---

* These definitions do not constitute a complete list of terms used in this document, but are included to clarify the meaning of some terms for the assistance of the reader. A more comprehensive list of definitions of terms relating to CANDU nuclear power plants is available from the Canadian Standards Association (CSA), *Manual of Definitions for CSA Nuclear Standards Use by CSA Technical Committees*, CSA-N9409A-1989.

** For postulated events requiring action by a shutdown system, it is accepted that at least one of the shutdown systems will operate in accordance with its minimum allowable performance standards as defined pursuant to section 3.1.

*** The performance requirements of a shutdown system refer only to its role in shutting the reactor down. For those requirements whose attainment also depends on fuel cooling or containment functions, credit for these functions may be taken in demonstrating that the performance requirements are met.

**** This regulatory document does not define comprehensive requirements for safety analysis and reference dose limits. The reference dose limits referred to in paragraph 3.2.1(b) are those contained in the reference or any subsequent AECB regulatory document, or as otherwise agreed in writing between the licensee and the AECB.

(c) a loss of primary heat transport system integrity shall not result from any fuel failure mechanism.*

3.2.2 For relevant events listed in Table 1, each shutdown system shall ensure that fuel in the reactor with no defects prior to the event does not fail as a consequence of the event.*

3.3 Environmental Requirements

3.3.1 All parts of each shutdown system which may be required to operate in response to any event specified in Tables 1 and 2 shall be designed to meet all necessary performance requirements while subjected to the most severe environmental conditions which could be present when or before such operation is required. These conditions may include, but are not necessarily limited to, the effects of steam, water, high temperature and radiation.

Qualification is required for all shutdown system equipment which may be required to operate following exposure to any of the above conditions. Qualification shall consist of tests to demonstrate to the extent practicable that the type of equipment can operate under conditions similar to those which would exist during or following the events specified in Tables 1 and 2. Where such tests are impracticable, analysis is required to demonstrate that this requirement is met.

3.3.2 Each shutdown system shall be designed such that, for all events in Tables 1 and 2, dynamic effects or jet forces caused by the events cannot result in impairment of the shutdown system to an extent that relevant requirements in section 3.2 would not be met.

3.4 Availability Requirements

3.4.1 Each shutdown system shall be designed such that the fraction of time for which it is not available can be demonstrated to be less that 10^{-3} years per year. A system shall be considered available only if it can be demonstrated to meet all the minimum allowable performance standards as defined in accordance with section 3.1. The unavailability of a system shall be determined by combining the maximum unavailability of any of the parameters required in accordance with section 3.6 with the unavailability of the rest of the shutdown system.

The availability of any safety support equipment necessary for actuation of a shutdown system shall be commensurate with the availability requirements of the shutdown system.

Availability calculations to demonstrate that this requirement can be met shall be included or referenced in the Safety Report. Such calculations shall be based on direct experience or reasonable extrapolations therefrom.

3.4.2 The design shall have sufficient redundancy such that no failure of any single component of a shutdown system can result in impairment of that system to an extent that the system will not meet its minimum allowable performance standards under accident conditions.

This requirement does not apply to components which are not required to change state and which do not depend on safety support equipment in order to perform their design functions, provided that they are designed, manufactured, inspected and maintained to standards acceptable to the AECB.

3.4.3 Actuation of a shutdown system shall not be dependent on any electrical power supply unless the electrical supply is designed to be continuously available during normal operation and anticipated operational transients.

3.4.4 As far as practicable, all shutdown system equipment shall be designed such that its most probable failure modes will not result in a reduction in safety.

3.4.5 As far as practicable, the design shall be such that all maintenance and availability testing which may be required when the shutdown systems are required to be available can be carried out without a reduction in the effectiveness of each shutdown system below its minimum allowable performance standards.

3.4.6 As far as practicable, the design shall be such that a failed component can be put into a safe state, or such that the failure can be converted to a safe failure in some other manner.

3.4.7 The design shall be such that each shutdown system can be actuated manually from the main control room. It shall also be possible to manually initiate shutdown system action for each shutdown system from a location remote from the main control room.

---

* For those events where the initiating failure is in a single fuel channel or its appurtenances, requirements 3.2.1(c) and 3.2.2 do not apply to that channel or the fuel therein.

3.4.8 The design shall be such that it is not readily possible for an operator to prevent actuation of a shutdown system when such actuation is required.

3.5 Separation and Independence Requirements

3.5.1 As far as practicable, the shutdown systems shall be of diverse designs and shall be physically and operationally independent from each other, from process systems and from other special safety systems.

3.5.2 Principles for the prevention of failures in more than one shutdown system as a result of the use of common equipment, procedures, or personnel, in design, construction, commissioning or operation, shall be prepared and shall require approval by the AECB prior to the issuance of a construction approval.

3.5.3 Design principles for the separation of redundant instrument channels and the services to them, associated with shutdown systems, shall be prepared and shall require approval by the AECB prior to the issuance of a construction approval.

3.5.4 The effectiveness of a shutdown system in shutting the reactor down in accordance with section 3.2 shall not be dependent on the correct functioning of any process system or any other special safety system.

3.5.5 The design shall be such that normal functioning of process systems cannot reduce the effectiveness of a shutdown system such that the requirements of section 3.2 would not be met.

3.6 Actuation Instrumentation Requirements

3.6.1 For each event specified in Tables 1 and 2 for which action by a shutdown system is required, there shall be at least two diverse parameters on each shutdown system, each designed to detect the need for and automatically initiate shutdown action such that all requirements for effectiveness are met. Exceptions to this requirement may be permitted only if it can be shown to the satisfaction of the AECB that incorporation of a second parameter for protection against an event is impracticable, or detrimental to safety.

3.6.2 Manual actuation may be considered acceptable in place of one of the automatic parameters provided it is shown to the satisfaction of the AECB that all of the following requirements are met.

(a) There is instrumentation designed to give the operator clear and unambiguous indication of the need to actuate the shutdown system.

(b) The reliability of such instrumentation is commensurate with the requirements for availability of the shutdown system as specified in Section 3.4. If indication of only a single parameter is required, the instrumentation shall be part of the shutdown system.

(c) There shall be 15 minutes available following such clear and unambiguous indication before the operator action is required.

(d) There are clear, well-defined and readily available operating procedures to identify the necessary actions.

3.7 Status Monitoring Requirements

3.7.1 The design of a shutdown system shall be such that the status of all important equipment required for its actuation can be monitored or inferred from the control room.

3.7.2 As far as practicable, all failures of shutdown system components which may interfere with proper functioning of the shutdown systems shall be annunciated in the control room.

3.8 Codes and Standards

3.8.1 The application for a construction approval shall identify any aspects of the design which fail to comply with the applicable requirements of the following codes and standards:

(a) CSA–N290.1: *Requirements for the Shutdown Systems of CANDU Nuclear Power Plants*, and

(b) CAN3–N285.0: *General Requirements for Pressure-Retaining Systems and Components in CANDU Nuclear Power Plants*.

All exceptions to the requirements of these standards shall require approval by the AECB prior to their implementation.

3.8.2 A list of any additional codes and standards to be applied to the shutdown systems and the extent of their application shall be prepared and shall require approval by the AECB prior to the issuance of a construction approval.

3.9 Seismic Requirements

Each shutdown system shall be designed such that it can perform the functions defined in section 3.2 during and following the design basis seismic ground motion for the site. The design shall be such that it is possible to manually actuate each shutdown system from a seismically qualified area following a design basis seismic event.

4. OPERATING REQUIREMENTS

4.1 Requirements for Normal Operation

4.1.1 Procedures for putting the reactor in a guaranteed shutdown state shall be prepared and shall require approval by the AECB prior to the issuance of an operating licence. Such procedures shall specify at least two independent means of ensuring that the reactor remains subcritical.

4.1.2 A shutdown system shall not be intentionally made unavailable at any time when there is fuel in the reactor except when the reactor is in an approved guaranteed shutdown state. A shutdown system shall be considered to be available only when it meets all its minimum allowable performance standards as defined in accordance with section 3.1.

4.1.3 When the reactor in is an approved guaranteed shutdown state, not less than one shutdown system shall be available at all times when this is practicable.

4.1.4 Requirements 4.1.2 and 4.1.3 do not apply to the period immediately after a shutdown system has operated. In the event that a shutdown system operates, it shall be returned to the poised state as soon as practicable without causing criticality, or the reactor shall be placed in an approved guaranteed shutdown state.

4.1.5 Procedures for taking corrective action, in the event that a shutdown system is found to be impaired when the reactor is not in a guaranteed shutdown state, shall be prepared and shall require approval by the AECB prior to the issuance of an operating licence.

4.1.6* If any component of a shutdown system is found to be inoperable, or impaired below its minimum allowable performance standards, that component and its associated equipment shall immediately be put in a safe condition, except as otherwise approved in accordance with subsection 4.1.5.

4.1.7* As far as practicable, maintenance of a shutdown system component shall be carried out only when that component and its associated equipment have been put in a state which does not reduce the availability of the shutdown system.

4.1.8* Maintenance of shutdown system components shall be carried out only on one channel at a time and with the affected channel placed in a safe state.

4.1.9 When maintenance on a channel is completed, it shall be thoroughly tested to demonstrate to the extent practicable that the equipment associated with that channel is capable of functioning in accordance with its design requirements. This shall be done prior to returning the channel to its poised state.

4.1.10 Maintenance on instrumentation associated with the measurement of neutron power shall be carried out as far as practicable when the reactor is at a power level at which the instrumentation gives sensible indications.

4.1.11 The standard of maintenance shall be such that the reliability and effectiveness of all equipment, as claimed in the Safety Report and other documentation in support of an operating licence, are assured.

4.2 Requirements for Accident Conditions

Operator action shall not be necessary for any function associated with shutting down the reactor in accident conditions except as approved in accordance with section 3.6.

5. TESTING REQUIREMENTS

5.1 Commissioning Tests

5.1.1 Performance Tests

Commissioning tests shall be done to demonstrate as far as practicable that all design requirements of each shutdown system have been achieved. Those tests which are possible when the reactor is subcritical shall be done prior to first criticality, and with the reactor in an approved guaranteed shutdown state. Procedures for performing commissioning tests when the reactor is critical shall be prepared and shall require approval by the AECB prior to the issuance of an operating licence.

---

* Requirements 4.1.6, 4.1.7 and 4.1.8 apply only when the shutdown system is required to be available as specified in requirements 4.1.2 and 4.1.3.

5.1.2 Wiring Tests

Prior to first criticality of the reactor, tests shall be carried out on all electrical wiring associated with each shutdown system to demonstrate that all connections are in accordance with the design.

5.2 In-Service Tests

Complete operational tests to demonstrate the effectiveness of each shutdown system shall be carried out at least once every two years.

5.3 Availability Tests

5.3.1 All shutdown system equipment shall be monitored or tested at a frequency which is adequate to demonstrate compliance with the availability requirement specified in subsection 3.4.1.

5.3.2 A report on the availability of each shutdown system shall be included in each annual report on the operation of the station. This report shall include:

(a) a statement of the total fraction of time in the year during which a shutdown system was not demonstrated to be available, as defined in section 3.4.1. Only periods during which a shutdown system is intentionally made unavailable, in accordance with the conditions of section 4.1, or is being repoised subsequent to actuation, shall be excluded from such calculations,

(b) a comparison of the failure modes and failure frequencies observed in the operation of the station with the failure modes and failure frequencies used in the availability calculations prepared in accordance with subsection 3.4.1,

(c) availability calculations sufficient to demonstrate that the availability requirement of subsection 3.4.1 can continue to be satisfied based on observed failure modes and failure frequencies.

REFERENCE

D.G. Hurst and F.C. Boyd, *Reactor Licensing and Safety Requirements*, AECB–1059, June 1972.

TABLES *

TABLE 1

1. Failure of reactor control systems.
2. Failure of normal electric power.
3. Seizure of a primary heat transport system main pump.
4. Failure of any feeder pipe in the primary heat transport system.
5. Failure of an end fitting.
6. Failure of a pressure tube and its associated calandria tube.
7. Blockage of a fuel channel.
8. Failure of a fuelling machine to replace a closure plug.
9. Inadvertent opening of pressure relief or control valves on the primary heat transport system or associated systems.
10. Failure of steam generator tubes.
11. Failure of feedwater/steam system.
12. Failure of moderator system.
13. Failure of service water system.
14. Failure of any other equipment in reactor systems which, in the absence of shutdown action, could result in damage to fuel in the reactor.

TABLE 2

Failure of any pipe or header in any fuel cooling system.

---

* In these tables, "failure" means both total failure and partial failure. For cooling systems, "failure" includes:
  (a) failure of system piping,
  (b) failure of circulation, and
  (c) failure of heat removal capability.

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

R-9

Regulatory Document

Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants

A Regulatory Policy Statement

Effective date: February 21, 1991

Canada

TABLE OF CONTENTS

This document is part of a set of regulatory documents
relating to the safety requirements for CANDU nuclear power plants:

R-7, *Requirements for Containment Systems for CANDU Nuclear Power Plants*
R-8, *Requirements for Shutdown Systems for CANDU Nuclear Power Plants*
R-9, *Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants*

These documents apply to reactors licensed for construction after January 1, 1981.

REQUIREMENTS FOR EMERGENCY CORE COOLING SYSTEMS FOR CANDU NUCLEAR POWER PLANTS

1. DEFINITIONS*

In this document,

"minimum allowable performance standards" means the set of operating limits or the range of conditions established for components or subsystems which define the minimum acceptable states for those components or subsystems as credited in the safety analyses; (*normes de rendement minimal admissible*)

"primary heat transport system" means that system of components which permit the transfer of heat from the fuel in the reactor to the steam generators or other heat exchangers employing secondary cooling. For purposes of this document, it does not necessarily include auxiliary purification and pressure control subsystems; (*circuit caloporteur primaire*)

"special safety system" means one of the following systems: shutdown systems, containment system, emergency core cooling system. (*système spécial de sûreté*)

2. BASIC REQUIREMENTS

2.1 All CANDU nuclear power reactors shall be equipped with an alternate means of cooling the reactor fuel in the event that the inventory of fuel coolant is depleted to an extent that fuel cooling is not assured. In this document, such a system shall be referred to as the emergency core cooling system** (ECCS).

2.2 (a) Except as noted in paragraphs (b) and (c), all equipment required for correct operation of the ECCS shall be considered to be part of the ECCS and shall meet all requirements of this document.

(b) Equipment required to supply compressed air, electrical power or cooling water to equipment for operation of the ECCS shall be considered as safety support equipment. Such equipment shall meet all relevant requirements of this document with the exception of sections 3.5 and 3.10.

(c) Equipment which is part of normal plant process systems and which is not specifically designed to mitigate the consequences of accidents, but which contributes to the cooling of the fuel following an accident, shall be considered as process equipment contributing to fuel cooling. Such equipment shall meet all relevant requirements of this document with the exception of subsections 3.4.1 to 3.4.9 and sections 3.5, 3.6 and 3.10.

2.3 The design requirements of the ECCS shall be based on the assumption that the least effective of the shutdown systems has operated successfully.

2.4 The ECCS shall be considered to be a special safety system.

2.5 Procedures to ensure compliance with the requirements of this regulatory policy statement shall be prepared by the licensee and shall require the approval of the Atomic Energy Control Board (AECB) prior to the issuance of a construction approval (procedures relating to part 3) or an operating licence (procedures relating to parts 4 and 5).

---

* These definitions do not constitute a complete list of terms used in this document, but are included to clarify the meaning of some terms for the assistance of the reader. A more comprehensive list of definitions of terms relating to CANDU nuclear power plants is available from the Canadian Standards Association (CSA), *Manual of Definitions for CSA Nuclear Standards Use by CSA Technical Committees*, CSA–N9409A–1989.

** Current CANDU reactor designs incorporate various systems for emergency coolant injection supply, recovery, circulation and heat removal. In this regulatory document, all necessary subsystems and components performing these functions shall be collectively referred to as the emergency core cooling system (ECCS).

3. DESIGN REQUIREMENTS

3.1 Minimum Allowable Performance Standards

Minimum allowable performance standards shall be defined for the ECCS and shall be listed or referenced in the Safety Report and in the Operating Policies and Principles for the plant. The minimum allowable performance standards shall also be specified for all major equipment and subsystems necessary for correct operation of the ECCS.

3.2 Cooling Requirements

For all events specified in Tables 1 and 2, the ECCS shall be capable of maintaining or re-establishing sufficient cooling of the fuel and fuel channels so as to limit the release of radioactive material from the fuel in the reactor and to maintain fuel channel integrity. For such events, the ECCS shall meet all of the following requirements:

(a) the release of radioactive material from the fuel in the reactor shall be limited such that the reference dose limits are not exceeded;*

(b) for events listed in Table 1, there shall be no failure of fuel in the reactor due to lack of adequate cooling;**

(c) all fuel in the reactor and all fuel channels shall be kept in a configuration such that continued removal by the ECCS of the decay heat produced by the fuel can be maintained,** and

(d) after adequate cooling of the fuel is re-established by the ECCS, the system shall be capable of continuing to supply sufficient cooling flow for as long as it is required to prevent further damage to the fuel.**

3.3 Environmental Requirements

3.3.1 All parts of the ECCS which may be required to operate, or to continue operating in response to any event specified in Tables 1 and 2 shall be designed to meet all necessary performance requirements while subjected to the most severe environmental conditions which could be present when or before such operation is required. These conditions may include, but are not necessarily limited to, the effects of debris, steam, water, high temperature and radiation.

Qualification is required for all ECCS equipment which may be required to operate, or to continue operating, following exposure to any of the above conditions. Qualification shall consist of tests to demonstrate to the extent practicable that the type of equipment can operate under conditions similar to those which would exist during or following the events specified in Tables 1 and 2. Where such tests are impracticable, analysis is required to demonstrate that this requirement is met.

3.3.2 The ECCS shall be designed such that, for all events specified in Tables 1 and 2, dynamic effects or jet forces caused by the events cannot result in impairment of the ECCS to an extent that relevant requirements in section 3.2 would not be met.

3.4 Availability Requirements

3.4.1 The ECCS shall be designed such that the fraction of time for which it is not available can be demonstrated to be less that 10^{-3} years per year. The system shall be considered available only if it can be demonstrated to meet all the minimum allowable performance standards as defined in accordance with section 3.1.

The availability of safety support equipment necessary for correct operation of the ECCS shall be commensurate with the availability requirements of the ECCS.

Availability calculations to demonstrate that this requirement can be met shall be included or referenced in the Safety Report. Such calculations shall be based on direct experience or reasonable extrapolations therefrom.

---

* This regulatory document does not define comprehensive requirements for safety analysis and reference dose limits. The reference dose limits referred to in paragraph (a) are those contained in the reference or in any subsequent AECB regulatory document, or as otherwise agreed in writing between the licensee and the AECB.

** The cooling requirements specified in paragraphs (b), (c) and (d) apply only to fuel in the reactor. For events where the initiating failure is in a single fuel channel or its appurtenances, these requirements do not apply to that channel or the fuel associated with it.

3.4.2 The design of the ECCS and safety support equipment shall take into account the long-term reliability requirements of those components which must continue to function following an accident. Standards for the long-term reliability of such components shall be prepared and shall require approval by the AECB prior to the issuance of a construction approval.

3.4.3 The design shall have sufficient redundancy such that no failure of any single component of the ECCS can result in impairment of the ECCS to an extent that the system will not meet its minimum allowable performance standards under accident conditions.

This requirement does not apply to components which are not required to change state and which do not depend on safety support equipment in order to perform their design functions, provided that they are designed, manufactured, inspected and maintained to standards acceptable to the AECB.

3.4.4 Correct operation of ECCS equipment following an accident shall not be dependent on power supplies from the electrical grid or from the turbine generators associated with any reactor unit sharing the same containment system as the reactor involved in the accident, unless it is shown to the satisfaction of the AECB that the availability of such power supplies could not be impaired by the consequences of any accident for which the ECCS is required to operate.

3.4.5 As far as practicable, all ECCS equipment shall be designed such that its most probable failure modes will not result in a reduction in safety.

3.4.6 As far as practicable, the design shall be such that all maintenance and availability testing which may be performed when the ECCS is required to be available, can be carried out without a reduction in the effectiveness of the system below its minimum allowable performance standards.

3.4.7 As far as practicable, the design shall be such that a failed component can be put into a safe state, or such that the failure can be converted to a safe failure in some other manner.

3.4.8 The design shall be such that all necessary actions of ECCS equipment which are initiated by automatic control logic in response to an accident can also be initiated manually from the appropriate control room.

3.4.9 The design shall be such that, in the event of an accident, it is not readily possible for an operator to prevent injection of emergency coolant from taking place when such injection is required.

3.4.10 Reliability standards for process equipment contributing to fuel cooling, as defined in paragraph 2.2(c), shall be prepared and shall require approval by the AECB prior to the issuance of a construction approval.

3.5 Separation and Independence Requirements

3.5.1 As far as practicable, the ECCS shall be physically and operationally independent from other special safety systems. No equipment which is part of the ECCS shall be used as part of another special safety system.

3.5.2 As far as practicable, the ECCS shall be independent from all process systems.

3.5.3 Design principles for the separation of redundant instrument channels and the services to them, associated with the ECCS, shall be prepared and shall require approval by the AECB prior to the issuance of a construction approval.

3.5.4 If subsystems of the ECCS are considered to be independent for the purpose of the safety analyses, principles for separation and independence of such subsystems shall be prepared and shall require approval by the AECB prior to the issuance of a construction approval.

3.6 Leakage Control Requirements

ECCS components located exterior to the reactor containment structure, and which may contain radioactive material following a loss of coolant accident (LOCA), shall be located such that any leakage (liquid, vapour or gas) which may occur is confined to the immediate vicinity of the components or is directed in a controlled fashion to appropriate leakage collection facilities. This requirement does not apply to fully welded piping and components.

3.7 Inadvertent Operation

The ECCS shall be designed as far as practicable such that inadvertent operation of all or part of the system shall not have a detrimental effect on plant safety.

3.8 Shielding Requirements

There shall be provision for adequate shielding of any ECCS equipment which could contain radioactive material following an accident, to permit personnel access to plant equipment for which such access might be required.

3.9 Status Monitoring Requirements

3.9.1 The design of the ECCS shall be such that the status of all important equipment required for operation of the ECCS can be monitored or inferred from the control room.

3.9.2 As far as practicable, all failures of ECCS components which may interfere with proper functioning of the ECCS shall be annunciated in the control room.

3.10 Codes and Standards

3.10.1 The application for a construction approval shall identify any aspects of the design which fail to comply with the applicable requirements of CAN3–N285.0–M81, *General Requirements for Pressure-Retaining Systems and Components in CANDU Nuclear Power Plants.* All exceptions to the requirements of this standard shall require approval by the AECB prior to their implementation.

3.10.2 The minimum acceptable standards for pressure-retaining components of the ECCS shall be CAN3–N285.0 Class 3.

3.10.3 The rules of the CAN3–N285.0 Class 2 shall be applied, as a minimum, to those portions of the ECCS which may be outside containment and which could contain appreciable quantities of radioactive materials as a result of an accident.

3.10.4 A list of any additional codes and standards to be applied to the ECCS, and the extent of their application, shall be prepared and shall require approval by the AECB prior to the issuance of a construction approval.

3.11 Seismic Requirements

All equipment required for continued fuel cooling after such cooling has been re-established shall be designed to remain functional following the site design earthquake for the plant site.

4. OPERATING REQUIREMENTS

4.1 Requirements for Normal Operation

4.1.1 The ECCS shall not be intentionally made unavailable at any time when its operation could potentially be required except in accordance with procedures which shall be prepared and which shall require approval by the AECB prior to the issuance of an operating licence. The ECCS shall be considered to be available only when it meets all the minimum allowable performance standards as defined in accordance with section 3.1.

4.1.2 Procedures for taking corrective action, in the event that the ECCS is found to be impaired during periods when availability is required, shall be prepared and shall require approval by the AECB prior to the issuance of an operating licence.

4.1.3* If any component of the ECCS is found to be inoperable, or impaired below its minimum allowable performance standards, the component and its associated equipment shall, as far as practicable, immediately be put in a safe condition, except as approved in accordance with subsection 4.1.2.

4.1.4* As far as practicable, maintenance on an ECCS component shall be carried out only when that component and its associated equipment have been put in a state which does not reduce the availability of the ECCS.

4.1.5* If redundant components require maintenance, each component shall be thoroughly tested following its maintenance, prior to the start of work on a subsequent component.

---

* Requirements 4.1.3, 4.1.4 and 4.1.5 do not apply during periods when the ECCS has been made unavailable in accordance with procedures approved pursuant to subsection 4.1.1.

4.1.6 When maintenance on a component is completed, it shall be tested to the extent practicable to demonstrate that it and its associated equipment function in accordance with design requirements.

4.1.7 The standard of maintenance shall be such that the reliability and effectiveness of all equipment, as claimed in the Safety Report and other documentation in support of an operating licence, are assured.

4.2 Requirements for Accident Conditions

If operator action is required for actuation of any ECCS equipment, all of the following requirements must be met:

(a) there shall be instrumentation to give the operator clear andunambiguous indication of the necessity for operator action;

(b) the reliability of such instrumentation shall be commensurate with the requirements for availability of emergency core cooling, as specified in section 3.4. If indication of only a single parameter is required, the instrumentation shall be part of the emergency core cooling system;

(c) there shall be 15 minutes available following such clear and unambiguous indication before the operator action is required, and

(d) there shall be clear, well-defined and readily available operating procedures to identify the necessary actions.

5. TESTING REQUIREMENTS

5.1 Commissioning Tests

5.1.1 Performance Tests

Prior to first criticality of any reactor, tests of the ECCS equipment shall be performed to verify that all design requirements have been achieved. Exceptions to this requirement will be allowed only if it is shown to the satisfaction of the AECB that some operational characteristics are impracticable to demonstrate under non-accident conditions, or that such tests would have a detrimental effect on safety.

5.1.2 Wiring Tests

Prior to first criticality of the reactor, tests shall be carried out on all electrical wiring associated with the ECCS to demonstrate that all connections are in accordance with the design.

5.2 Availability Tests

5.2.1 All ECCS equipment shall be monitored or tested at a frequency which is adequate to demonstrate compliance with the availability requirements specified in subsection 3.4.1.

5.2.2 A report on the availability of the ECCS shall be included in each annual report on the operation of the station. This report shall include:

(a) a statement of the total fraction of time in the year during which the ECCS was not demonstrated to be available, as defined in subsection 3.4.1. Only periods during which the ECCS is intentionally made unavailable, in accordance with the conditions of section 4.1 shall be excluded from such calculations;

(b) a comparison of the failure modes and failure frequencies observed in the operation of the station with the failure modes and failure frequencies used in the availability calculations prepared in accordance with subsection 3.4.1, and

(c) availability calculations sufficient to demonstrate that the availability requirement of subsection 3.4.1 can continue to be satisfied, based on observed failure modes and failure frequencies.

REFERENCE

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

TABLES *

TABLE 1

1. Failure of any feeder pipe in the primary heat transport system
2. Failure of an end fitting
3. Failure of a pressure tube and its associated calandria tube
4. Fuel channel flow blockage
5. Failure of a fuelling machine to replace a closure plug
6. Inadvertent opening of pressure relief or control valves on the primary heat transport system
7. Failure of steam generator tubes
8. Failure of feedwater/steam system
9. Any of events 1 to 8 above accompanied by an impairment of the containment system.

TABLE 2

1. Failure of any pipe or header in the primary heat transport system
2. Event 1 accompanied by an impairment of the containment system.

---

* In these tables, "failure" means both total failure and partial failure.