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

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.

TABLE OF CONTENTS

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.