Regulatory Document

Texte de réglementation

Atomic Energy Control Board

Commission de contrôle de l'énergie atomique

REGULATORY DOCUMENT R-10

Regulatory Policy Statement

# THE USE OF TWO SHUTDOWN SYSTEMS IN REACTORS

Effective date:

January 11, 1977

Canada

# PREFACE

1. Siting, design, manufacture, construction, commissioning, operation, and decommissioning of nuclear facilities, or the production, possession, use and disposal of prescribed substances, in Canada or under Canadian control, are subject to the provisions of the Atomic Energy Control Act and Regulations administered by the Atomic Energy Control Board (AECB).

2. In addition to the Atomic Energy Control Regulations, three other categories of Regulatory Document are employed by the AECB. These are:

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

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

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

3. In developing Regulatory Documents, the AECB publishes its proposals as Consultative Documents in order to solicit comments both from the nuclear industry and from the public. This is done prior to releasing any Regulatory Document in final form. In certain cases, after the period for public comment, a Consultative Document may be issued for "trial use". This is done for a limited period of time to gain practical experience. Following the period of trial use, the revised document is re-issued for further public comment prior to release in final form.

4. Comments on Consultative Documents and suggestions for new Regulatory Documents and for improvement to those that exist are encouraged and should be directed to the Regulations Development Section of the AECB.

5. Copies of Consultative Documents, Regulatory Documents and related index lists are available in both English and French on request from the Office of Public Information. Requests for technical information on and interpretation of documents should be addressed to this office.

6. The Atomic Energy Control Board may be contacted as follows:

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

   Telephone
   General Inquiries: (613) 995-5894

DATE: 11, January 1977

# THE USE OF TWO SHUTDOWN SYSTEMS IN REACTORS

## PART I - Licensing Requirements

Pursuant to Section 10 Subsection (4) of the Atomic Energy Control Regulations SOR/74-334 the Atomic Energy Control Board gives notice of the following requirements for protective shutdown systems in nuclear power reactors.

1) All nuclear power reactors licensed for construction in Canada after January 1, 1977 shall incorporate two independent protective shutdown systems unless otherwise approved by the Board.

2) The quality of the detailed design, construction, commissioning, testing, maintenance and operation of each protective shutdown system shall be at least equal to the quality expected of the protective shutdown system in plants licensed for operation prior to January 1, 1976. Compliance with applicable codes, standards and practices in effect at the time of licensing will be required.

3) The protective shutdown systems shall be of diverse designs and each shall be physically and functionally separate from the other, from process systems, and from other special safety systems.

4) The applicant for an operating licence shall show by analysis, adequately supported by experimental evidence that when protective shutdown action is necessary, the combined action of the two protective shutdown systems is not required to prevent the consequences of a failure from exceeding those shown in Table 1. This requires that the applicant show that:

   i) the consequences of all serious process failures can be limited by at least one of the two protective shutdown systems acting alone to shut down the reactor to less than those shown in Table 1 for Class 1 failures, assuming proper operation of the containment and emergency core cooling system;

   ii) the consequences of all serious process failures can be limited by each of the protective shutdown systems acting alone to shut down the reactor to less than those shown in Table 1 for Class 2 failures, assuming proper operation of the containment and assuming unavailability of the emergency core cooling system;

iii) the consequences of all serious process failures can be limited by each of the shutdown systems acting alone to shut down the reactor to less than those shown in Table 1 for Class 2 failures, assuming proper operation of the emergency core cooling systems and assuming impairment of the containment.

Table 1: Reference Dose Limits for Postulated Failure Conditions

| Situation | Meteorology to be used in Calculation | Maximum Individual Dose Limits | Maximum Total Population Dose Limits[c] |
|---|---|---|---|
| Class 1 Failure | Either worst weather existing at most 10% of time or Pasquill F condition if local data incomplete | 0.5 rem whole body<br>3 rem to thyroid[a] | $10^4$ man-rem<br>$10^4$ thyroid-rem |
| Class 2 Failure | Either worst weather existing at most 10% of time or Pasquill F condition if local data incomplete | 25 rem whole body<br>250 rem thyroid[b] | $10^6$ man-rem<br>$10^6$ thyroid-rem |

[a] For other organs use 1/10 ICRP occupation values.

[b] For other organs use 5 times ICRP annual occupational dose.

(c) For purposes of safety analysis the population dose is integrated from the station boundary out to a distance where the individual dose is 1% of the dose to an individual at the boundary.

PART II - Application of Part I

1) Preamble

1.1) It is considered credible that any one of the special safety systems may fail to perform its required function when called upon to counteract any serious process system failure. Consequently, a plant design must ensure that under such circumstances the release of radioactive material will be within the limits specified by the Atomic Energy Control Board. Because of the particular importance of reactor protective shutdown action the application of the single failure/dual failure approach previously used in assessing nuclear plant safety is modified when two protective shutdown systems are incorporated as part of the plant design.

1.2) For those plant designs incorporating two independent reactor protective shutdown systems of suitable design amongst the special safety systems, it is accepted that at least one of them will operate as designed when protective shutdown action is required.

1.3) The design and performance of each protective shutdown system should meet the requirements of Part II of this document unless otherwise specifically approved.

2) Definitions

2.1) A serious process system failure means any failure of process equipment or procedure which could lead to a significant release of radioactive material from the station in the absence of special safety system action.* A significant release is one which would result in individual or population doses in excess of those given in Table 1 for Class 1 failures.

2.2) A Class 1 failure means a serious process failure with the following assumptions regarding performance of the special safety systems:

(a) Protective Shutdown System 1 operates as designed, the containment operates as designed and the emergency core cooling system operates as designed;

or

(b) Protective Shutdown System 2 operates as designed, the containment operates as designed and the emergency core cooling system operates as designed

2.3) A Class 2 failure means a serious process failure with the following assumptions regarding performance of the special safety systems:

*The identification of those serious process system failures which must be considered in the design of the plant is outside the scope of the document.

(a) Protective Shutdown System 1 operates as designed, the containment operates as designed and the emergency core cooling system is unavailable;
or

(b) Protective Shutdown System 2 operates as designed, the containment operates as designed and the emergency core cooling system is unavailable;
or

(c) Protective Shutdown System 1 operates as designed, the emergency core cooling system operates as designed and the containment is impaired;*
or

(d) Protective Shutdown System 2 operates as designed, the emergency core cooling system operates as designed and the containment is impaired.*

3) Design Requirements

3.1) Each of the two protective shutdown systems, acting alone to shut down the reactor, shall be capable of preventing failure of the primary heat transport system due to overpressure, excessive fuel temperatures or fuel break-up. The action of safety-related devices, such as overpressure relief valves, may be taken into account if the design of such devices is commensurate with the design of special safety systems.

*The identification of those modes of containment failure which must be considered in the design of the plant is outside the scope of this document.

3.2) Following a serious process failure, each of the two protective shutdown systems, acting alone to shut down the reactor shall be capable of limiting both the rate of energy production and the total energy production to the extent that the integrity of the containment system is not jeopardized.

3.3) Each of the two protective shutdown systems, acting alone, shall be capable of maintaining the reactor in a suitable subcritical shutdown state indefinitely or, alternatively for a period long enough to permit the protective shutdown system to be supplemented reliably.

3.4) Each protective shutdown system shall incorporate sufficient redundancy to ensure that no single failure results in the loss of its protective action.

3.5) Where practicable, two diverse trip parameters shall be incorporated into the sensing and control logic of each protective shutdown system for each of the serious process failures requiring shutdown action. Manual actuation is acceptable as a "trip parameter" provided it is shown that adequate information and time are available to alert an operator and to permit him to assess the need for intervention and to actuate the protective shutdown system manually.

3.6) Each protective shutdown system shall be readily testable at a frequency sufficient to demonstrate to the extent practicable that its unavailability is less than $1 \times 10^{-3}$ years per year.

3.7) Each protective shutdown system shall be readily maintainable without increasing the probability that the system may become unavailable.

3.8) Each protective shutdown system shall be designed to fail in the safe direction unless the required availability can be otherwise demonstrated.

3.9) The design of each protective shutdown system shall be such that partial or incomplete operation of one system will not render the other system ineffective.

3.10) In the safety analysis the action of process systems to complement or supplement the safety action of one or both of the protective shutdown systems shall not be taken into account except to show that normal functioning of process systems does not impair the effectiveness of one or both of the protective shutdown systems.