



Consultative Document  
Document de consultation



Atomic Energy  
Control Board

Commission de contrôle  
de l'énergie atomique

---

CONSULTATIVE DOCUMENT C-98

Proposed Regulatory Policy Statement

REQUIREMENTS FOR RELIABILITY  
ANALYSIS OF SAFETY-RELATED  
SYSTEMS IN NUCLEAR REACTORS

Issued for comment:

April 14, 1987

Canada

9405260150 940512  
PDR PROJ  
679A PDR

This Consultative Document is issued in order to provide an opportunity for public review of the proposal it contains before formal issue as a Regulatory Document. Comments are encouraged and should be directed to the address below before JULY 14, 1987.

Subject to the Access to Information Act, all comments will be disclosed to the public and will be placed in the AECB Public Documents Room in the AECB offices at 270 Albert Street, Ottawa. Commentators should identify those parts of their comments that should not be disclosed pursuant to the Access to Information Act, the reason why they should not be disclosed, and also identify those parts that they consent to the disclosure of.

Direct comments to:

Health Effects and Regulatory  
Documents Section  
Atomic Energy Control Board  
P.O. Box 1046  
Ottawa, Ontario  
CANADA  
K1P 5S9

## THE AECEB REGULATORY DOCUMENTS SYSTEM

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 Health Effects and Regulatory Documents 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  
CANADA  
K1P 5S9

Telephone  
General Inquiries: (613) 995-5894

TABLE OF CONTENTS

PAGE

|  |   |
|--|---|
| 1. INTRODUCTION AND SCOPE .....        | 1 |
| 2. GENERAL REQUIREMENTS .....          | 1 |
| 3. DEFINITION OF SYSTEM FAILURES ..... | 2 |
| 4. DOCUMENTATION .....                 | 2 |
| 5. RELIABILITY DATA .....              | 3 |

REQUIREMENTS FOR RELIABILITY  
ANALYSIS OF SAFETY-RELATED  
SYSTEMS IN NUCLEAR REACTORS

1. INTRODUCTION AND SCOPE

1.1 This document defines general principles for reliability analysis of safety-related systems in nuclear reactors.

1.2 This document should be used whenever a reliability analysis is carried out to support an application for approval of construction or for renewal of a licence or to fulfill a licensing requirement.

1.3 It is the responsibility of the applicant when applying for approval of construction to define to the satisfaction of the Atomic Energy Control Board how the reliability analysis will be used in the design and safety assessment of the facility. The information that shall be provided includes:

(a) the organization and interaction of the various groups involved in the design, operation, and reliability analysis;

(b) the systems which will be analyzed and their design reliability requirements;

(c) the reliability analysis techniques which will be used and a justification of their adequacy.

2. GENERAL REQUIREMENTS

2.1 Any reliability analysis performed to satisfy licensing requirements should be part of a process which starts at an early design stage and continues appropriately throughout the operating life of the analyzed system.

2.2 Reliability analyses shall be consistent with the detailed design requirements of the analyzed system, and shall address all permissible modes of operation of the system.

2.3 Boundaries between systems or subsystems shall be clearly and unambiguously defined. Reliability analyses of connected systems or subsystems shall be fully compatible and consistent with each other.

2.4 Reliability analyses shall be consistent with the approved plant design and with the operating procedures in accordance with information available at the date stated in the reliability analysis report.

2.5 A procedure shall be established for determining the changes between the information used in the analysis and the current status. This procedure should address:

(a) design changes anticipated but not implemented;

(b) design changes made subsequent to the analysis;

(c) differences between actual operating or maintenance procedures and the procedure assumed in the analysis;

(d) differences in actual component and system performances from those assumed in the analysis.

### 3. DEFINITION OF SYSTEM FAILURES

3.1 Each reliability analysis report shall clearly define what constitutes failure of the analyzed system, including failures of its components and supporting equipment. The defined system failure shall be related to the overall safety assessment of the facility (in the Safety Report or other documents submitted in support of the licence application).

3.2 The definition of system failures of special safety systems or safety-related systems should include the following.

(a) The system or equipment fails to function as required. This includes both the inability to function at the time of request, and a loss of ability to function during a period in which the function is, or may be, required.

(b) The system or equipment does not cease to function on command (if applicable).

(c) The system or equipment starts functioning spuriously (if applicable).

3.3 Where possible, failure criteria should be stated in units that can be verified in practice by inspection or testing.

3.4 The reliability analysis should provide a comprehensive coverage of all factors which could cause system failures, without a priori assumptions that certain factors can be excluded.

3.5 The reliability analysis should also identify any failures of components of the analyzed system which could have safety implications for systems or equipment other than the system being analyzed.

### 4. DOCUMENTATION

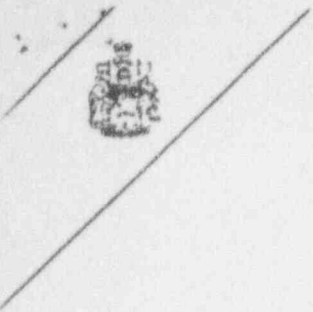
4.1 Each reliability analysis performed to satisfy licensing requirements shall be documented with sufficient clarity that it can be readily and reliably used and audited by personnel other than the analysts.

4.2 A reliability analysis used in the licensing process shall be documented in such a way that it can be verified as far as practicable by test and observation during the complete life of the analyzed system, and in such a way that it can be maintained in an up-to-date state if design or operational changes are made to the system, its components, or supporting equipment, or if reliability data for any components or systems require modification.

4.3 Each event or other factor in a reliability analysis shall be identified in accordance with a defined scheme. Such a scheme should provide for the assignment of a unique identification to each different event or factor. If the same event or factor occurs more than once in the analysis, it should be assigned the same identification. The scheme should make it possible to relate each event to the specific component or components to which it refers.

#### 5. RELIABILITY DATA

Data used in a reliability analysis shall be demonstrably valid.



Consultative Document  
Document de consultation



Atomic Energy  
Control Board

Commission de contrôle  
de l'énergie atomique

---

CONSULTATIVE DOCUMENT C-98

Proposed Regulatory Policy Statement

REQUIREMENTS FOR RELIABILITY  
ANALYSIS OF SAFETY-RELATED  
SYSTEMS IN NUCLEAR REACTORS

Issued for comment:

April 14, 1987

Canada



This Consultative Document is issued in order to provide an opportunity for public review of the proposal it contains before formal issue as a Regulatory Document. Comments are encouraged and should be directed to the address below before JULY 14, 1987.

Subject to the Access to Information Act, all comments will be disclosed to the public and will be placed in the AECB Public Documents Room in the AECB offices at 270 Albert Street, Ottawa. Commentators should identify those parts of their comments that should not be disclosed pursuant to the Access to Information Act, the reason why they should not be disclosed, and also identify those parts that they consent to the disclosure of.

Direct comments to:

Health Effects and Regulatory  
Documents Section  
Atomic Energy Control Board  
P.O. Box 1046  
Ottawa, Ontario  
CANADA  
K1P 5S9

## THE AECB REGULATORY DOCUMENTS SYSTEM

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 Health Effects and Regulatory Documents 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  
   CANADA  
   K1P 5S9

Telephone  
General Inquiries:                (613) 995-5894

TABLE OF CONTENTS

PAGE

|  |   |
|--|---|
| 1. INTRODUCTION AND SCOPE .....        | 1 |
| 2. GENERAL REQUIREMENTS .....          | 1 |
| 3. DEFINITION OF SYSTEM FAILURES ..... | 2 |
| 4. DOCUMENTATION .....                 | 2 |
| 5. RELIABILITY DATA .....              | 3 |

REQUIREMENTS FOR RELIABILITY  
ANALYSIS OF SAFETY-RELATED  
SYSTEMS IN NUCLEAR REACTORS

1. INTRODUCTION AND SCOPE

1.1 This document defines general principles for reliability analyses of safety-related systems in nuclear reactors.

1.2 This document should be used whenever a reliability analysis is carried out to support an application for approval of construction or for renewal of a licence or to fulfill a licensing requirement.

1.3 It is the responsibility of the applicant when applying for approval of construction to define to the satisfaction of the Atomic Energy Control Board how the reliability analysis will be used in the design and safety assessment of the facility. The information that shall be provided includes:

(a) the organization and interaction of the various groups involved in the design, operation, and reliability analysis;

(b) the systems which will be analyzed and their design reliability requirements;

(c) the reliability analysis techniques which will be used and a justification of their adequacy.

2. GENERAL REQUIREMENTS

2.1 Any reliability analysis performed to satisfy licensing requirements should be part of a process which starts at an early design stage and continues appropriately throughout the operating life of the analyzed system.

2.2 Reliability analyses shall be consistent with the detailed design requirements of the analyzed system, and shall address all permissible modes of operation of the system.

2.3 Boundaries between systems or subsystems shall be clearly and unambiguously defined. Reliability analyses of connected systems or subsystems shall be fully compatible and consistent with each other.

2.4 Reliability analyses shall be consistent with the approved plant design and with the operating procedures in accordance with information available at the date stated in the reliability analysis report.

2.5 A procedure shall be established for determining the changes between the information used in the analysis and the current status. This procedure should address:

(a) design changes anticipated but not implemented;

(b) design changes made subsequent to the analysis;

4.3 Each event or other factor in a reliability analysis shall be identified in accordance with a defined scheme. Such a scheme should provide for the assignment of a unique identification to each different event or factor. If the same event or factor occurs more than once in the analysis, it should be assigned the same identification. The scheme should make it possible to relate each event to the specific component or components to which it refers.

#### 5. RELIABILITY DATA

Data used in a reliability analysis shall be demonstrably valid.