Canada's Nuclear Regulator

Safety Analysis

Probabilistic Safety Assessment (PSA) for Reactor Facilities

REGDOC-2.4.2, Version 2

Month 20xx

DRAFT

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Canada

Probabilistic Safety Assessment (PSA) for Reactor Facilities
Regulatory document REGDOC-2.4.2

Cat. No. NNNNN
ISBN NNNNN

Également publié en français sous le titre : Études probabilistes de sûreté (EPS) pour une installation dotée de réacteurs

Document availability
This document can be viewed on the CNSC website. To request a copy of the document in English or French, please contact:

Canadian Nuclear Safety Commission
280 Slater Street
P.O. Box 1046, Station B
Ottawa, ON K1P 5S9
Canada

Tel.: 613-995-5894 or 1-800-668-5284 (in Canada only)
Fax: 613-995-5086
Email: cnsc.info.ccsn@canada.ca
Website: nuclearsafety.gc.ca
Facebook: facebook.com/CanadianNuclearSafetyCommission
YouTube: youtube.com/cnscccsn
Twitter: @CNSC_CCSN
LinkedIn: linkedin.com/company/cnsc-ccsn

Publishing history
May 2014 Version 1.0

Preface

This regulatory document is part of the CNSC's safety analysis series of regulatory documents, which also covers deterministic safety analysis and nuclear criticality safety. The full list of regulatory document series is included at the end of this document and can also be found on the CNSC's website.

Regulatory document REGDOC-2.4.2, *Probabilistic Safety Assessment for Reactor Facilities*, Version 2, sets out requirements and guidance for probabilistic safety assessments (PSA) for reactor facilities.

This document is the third version and supersedes S-294, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*, published in April 2005 and REGDOC-2.4.2, *Probabilistic Safety Assessment for Nuclear Power Plants*, published in May 2014.

A document that shows the changes made to REGDOC-2.4.2, *Probabilistic Safety Assessment for Nuclear Power Plants*, is available from the CNSC upon request.

For information on the implementation of regulatory documents and on the graded approach, see REGDOC-3.5.3, *Regulatory Fundamentals*.

The words "shall" and "must" are used to express requirements to be satisfied by the licensee or licence applicant. "Should" is used to express guidance or that which is advised. "May" is used to express an option or that which is advised or permissible within the limits of this regulatory document. "Can" is used to express possibility or capability.

Nothing contained in this document is to be construed as relieving any licensee from any other pertinent requirements. It is the licensee's responsibility to identify and comply with all applicable regulations and licence conditions.

Table of Contents

Probabilistic Safety Assessment (PSA) for Reactor Facilities

1. Introduction

1.1 Purpose

The purpose of this regulatory document, when incorporated into a licence to construct or operate a reactor facility or other legally enforceable instrument, is to ensure that the licensee conducts a probabilistic safety assessment (PSA) in accordance with defined requirements. In addition, this document provides guidance on the conduct of PSA for new reactor facilities.

1.2 Scope

This document sets out the requirements and guidance for the PSA for a licence to construct or operate a reactor facility.

The requirements and guidance contained in this regulatory document are applicable to all reactor facilities, including nuclear power plants, small reactor facilities, or research reactors, using a graded approach. For more information on the graded approach, refer to REGDOC-3.5.3, *Regulatory Fundamentals*.

1.3 Relevant legislation

The following provisions of the *Nuclear Safety and Control Act* (NSCA) and the regulations made under it are relevant to this document:

- NSCA, section 3 and subsections 24(4) and (5)

1.4 National and international standards

Key principles and elements used in developing this document are consistent with national and international standards.

The following standards are relevant to this regulatory document:

- IAEA Safety Standard SSG-3, *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants* [1]
- IAEA Safety Standard SSG-4, *Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants* [2]
- CSA N290.17-17, *Probabilistic safety assessment for nuclear power plants* [3]

2. Objectives of the Probabilistic Safety Assessment

The objectives of the probabilistic safety assessment are:

a. to provide a systematic analysis in order to give confidence that the reactor facility's design will align with the fundamental safety objectives as established in IAEA N-SF-1, Fundamental Safety Principles [4], including to protect people and the environment from radiation

b. to demonstrate that a balanced design has been achieved; this can be demonstrated as achieved if no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risk
c. to provide confidence that small changes of conditions that may lead to a catastrophic increase in the severity of consequences (cliff-edge effects) will be prevented
d. to provide assessments of the quantitative safety goals (the probabilities of occurrence for severe core damage states, and the assessments of the risks of radioactive releases to the environment) as defined in REGDOC-2.5.2, *Design of Reactor Facilities* [5], or as established in licensing basis for the facility
e. to provide site-specific assessments of the probabilities of occurrence and the consequences of external hazards
f. to identify plant vulnerabilities and systems for which design improvements or modifications to operational procedures could reduce the probabilities of severe accidents, or mitigate their consequences
g. to assess the adequacy of emergency operating procedures
h. to provide insights into the severe accident management program

3. Requirements for a Probabilistic Safety Assessment

3.1 Probabilistic safety assessment program

The licensee shall establish a program for the development and use of PSA as a means to manage radiological risks and to contribute to safe design and operation of reactor facilities.

The PSA program may include the following elements:

- preparation, maintenance and application of the PSA
- safety goals and numerical criteria, both the year average and instantaneous risk, against which the PSA results are compared, as well as the actions to be taken when these numerical criteria are exceeded.
- management of Incremental Risk from Abnormal Plant Configurations, and risk input to decision-making

3.2 Probabilistic safety assessment levels

The licensee shall perform a level 1 and level 2 PSA[1] for each reactor facility.

Considerations shall include the reactor core and other radioactive sources such as the spent fuel pool (also called irradiated fuel bay). Multi-unit impacts, if applicable, shall be included.

For radioactive sources outside the reactor core, the licensee may, subject to Section 3.8 choose an alternate analysis method to conduct the assessment.

[1] Definitions for level 1 and level 2 PSA can be found in REGDOC-3.6, *Glossary*

3.3 Management systems or quality assurance

The licensee shall conduct the PSA under the management system or quality assurance program established in the licensing basis.

Licensees should refer to REGDOC-2.1.1, Management System [6], CSA N286-12, Management system requirements for nuclear facilities [7] and CSA N286.7, Quality assurance of analytical, scientific and design computer programs for nuclear power plants [8] for guidance. The PSA should be developed in a manner that is consistent with the management system.

3.4 Probabilistic safety assessment models that reflect the facility

The PSA models shall reflect the plant as built and operated (including multi-unit impacts), as closely as reasonably achievable within the limitations of PSA technology, and consistent with the risk impact.

3.5 Update of probabilistic safety assessment models

The licensee shall update the PSA models every five years. The models shall be updated sooner if the facility undergoes major changes.

The licensee shall update the PSA models so that they adequately represent the as-operated plant conditions. The licensee shall inform the CNSC of the impacts of the update in models on the results of the level 1 and level 2 PSA.

3.6 Site-specific initiating events and potential hazards

The licensee shall include all potential site-specific initiating events and potential hazards, namely:

- internal initiating events and internal hazards
- external hazards, both natural and human-induced, but non-malevolent

Include potential combinations of the external hazards.

The screening criteria of hazards shall be acceptable to the CNSC.

The licensee may, subject to Section 3.8, choose an alternate analysis method to conduct the assessment of internal and external hazards.

Examples of external hazards are seismic hazards, external fires (e.g. fires affecting the site and originating from nearby forest fires), external floods, high winds, off-site transportation accidents, releases of toxic substances from off-site storage facilities, and severe weather conditions.

Examples of internal hazards are internal fires, internal floods, turbine missiles, onsite transportation accidents, and releases of toxic substances from onsite storage facilities.

3.7 Realistic assumptions and data

The licensee shall ensure the PSA models are developed using assumptions and data that are realistic and practical and, where required, supported by deterministic safety analysis or engineering assessments.

3.8 Consistent level of detail

The level of detail of the PSA shall be consistent with the facility testing, maintenance and configuration management programs, and should be consistent with the intended uses of the PSA.

3.9 Methodology and computer codes

The licensee shall seek CNSC staff acceptance of the methodology and computer codes to be used for the PSA before using them to fulfill the requirements of this document.

The methodology should be suitable to support the objectives of the PSA (set forth in Section 2 of this document) and to support the intended PSA applications. The computer codes that support the analytical methods should be adequate for the purpose and scope of the analysis.

The following domestic and International Atomic Energy Agency (IAEA) Safety Standards documents or updated versions provide general guidance for conducting high-quality PSAs:

- IAEA Safety Standard SSG-3, *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants* [1]
- IAEA Safety Standard SSG-4, *Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants* [2]
- CSA N290.17-17, *Probabilistic safety assessment for nuclear power plants* [3]

Information and guidance on how to apply the above standards using a graded approach is included in those standards.

3.10 Operational states

The licensee shall include at-power and shutdown states.

The licensee shall perform a PSA for other states where the reactor is expected to operate for extended periods of time and that are not covered by the at-power and shutdown PSAs. Definitions of operating states are found in REGDOC-3.6, *Glossary of CNSC Terminology* [9].

3.11 Sensitivity and uncertainty analyses

The licensee shall include sensitivity analysis, uncertainty analysis and importance measures in the PSA.

4. Guidance on Public Disclosure

In accordance with licensees' public information programs established under REGDOC 3.2.1, *Public Information and Disclosure* [10], a summary of the results and assumptions of a PSA should be made available to interested stakeholders. It should be noted that any information

pertaining to the specific fault sequences and vulnerabilities of a facility includes security-sensitive information and is subject to applicable information security provisions.

The public information should include high-level summaries of the PSA, including those for methodologies and screening criteria (subject to necessary security considerations).

Glossary

For definitions of terms used in this document, see REGDOC-3.6, *Glossary of CNSC Terminology*, which includes terms and definitions used in the *Nuclear Safety and Control Act* and the regulations made under it, and in CNSC regulatory documents and other publications. REGDOC-3.6 is provided for reference and information.

References

The CNSC may include references to information on best practices and standards such as those published by CSA Group. With permission of the publisher, CSA Group, all nuclear-related CSA standards may be viewed at no cost through the CNSC Web page "How to gain free access to all nuclear-related CSA standards".

1. International Atomic Energy Agency (IAEA), Safety Standard SSG-3, *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants*, 2010.
2. IAEA. Safety Standard SSG-4, *Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants*, 2010.
3. CSA Group. N290.17-17, Probabilistic Safety Assessment for Nuclear Power Plants, 2019.
4. IAEA, Safety Fundamentals No. SF-1, *Fundamental Safety Principles*, 2006.
5. CNSC, REGDOC-2.5.2, *Design of Reactor Facilities*, Ottawa, 2020.
6. CNSC, REGDOC-2.1.1, *Management System*, Ottawa, 2019.
7. CSA Group, N286-12, *Management System Requirements for Nuclear Facilities*, 2012.
8. CSA Group, N286.7-99, *Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants*, 1999.
9. CNSC, REGDOC-3.6, *Glossary of CNSC Terminology*, 2019.
10. CNSC, REGDOC 3.2.1, *Public Information and Disclosure*, Ottawa, 2018.

Additional Information

The following documents provide additional information that may be relevant and useful for understanding the requirements and guidance provided in this regulatory document:

- IAEA, INSAG-10, Defence in Depth in Nuclear Safety, A report by the International Nuclear Safety Advisory Group, 1996.

CNSC Regulatory Document Series

Facilities and activities within the nuclear sector in Canada are regulated by the CNSC. In addition to the *Nuclear Safety and Control Act* and associated regulations, these facilities and activities may also be required to comply with other regulatory instruments such as regulatory documents or standards.

CNSC regulatory documents are classified under the following categories and series:

1.0 Regulated facilities and activities

Series 1.1 Reactor facilities
1.2 Class IB facilities
1.3 Uranium mines and mills
1.4 Class II facilities
1.5 Certification of prescribed equipment
1.6 Nuclear substances and radiation devices

2.0 Safety and control areas

Series 2.1 Management system
2.2 Human performance management
2.3 Operating performance
2.4 Safety analysis
2.5 Physical design
2.6 Fitness for service
2.7 Radiation protection
2.8 Conventional health and safety
2.9 Environmental protection
2.10 Emergency management and fire protection
2.11 Waste management
2.12 Security
2.13 Safeguards and non-proliferation
2.14 Packaging and transport

3.0 Other regulatory areas

Series 3.1 Reporting requirements
3.2 Public and Indigenous engagement
3.3 Financial guarantees
3.4 Commission proceedings
3.5 CNSC processes and practices
3.6 Glossary of CNSC terminology

Note: The regulatory document series may be adjusted periodically by the CNSC. Each regulatory document series listed above may contain multiple regulatory documents. Visit the CNSC's website for the latest list of regulatory documents.