Canada's Nuclear Regulator

Safety Analysis

Probabilistic Safety Assessment (PSA) for Nuclear Power Plants

REGDOC-2.4.2

May 2014

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Canada

Probabilistic Safety Assessment (PSA) for Nuclear Power Plants
Regulatory Document REGDOC-2.4.2

PWGSC catalogue number CC172-108/2-2014E-PDF
ISBN 978-1-100-23791-6

Également publié en français sous le titre : Études probabilistes de sûreté (EPS) pour les centrales nucléaires

Document availability

This document can be viewed on the CNSC website at nuclearsafety.gc.ca. 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, Ontario K1P 5S9
CANADA

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

Publishing history

May 2014 Version 1.0

Preface

This regulatory document is part of the CNSC's Safety Analysis series of regulatory documents. The full list of regulatory document series is included in the back of this document and can be found on the CNSC's website

This regulatory document sets out the requirements of the Canadian Nuclear Safety Commission (CNSC) with respect to the probabilistic safety assessment.

Issued as REGDOC-2.4.2, this document is the second version of *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*. It supersedes the previous version of the same title that was identified as S-294. REGDOC-2.4.2 includes amendments to reflect lessons learned from the Fukushima nuclear event of March 2011, and to address findings from the *CNSC Fukushima Task Force Report*, as applicable to S-294.

REGDOC-2.4.2 is intended to form part of the licensing basis for a regulated facility or activity within the scope of the document. It is intended for inclusion in licences, either as part of the conditions and safety and control measures in a licence, or as part of the safety and control measures to be described in a licence application and the documents needed to support that application.

For proposed new facilities: This document will be used to assess new licence applications for reactor facilities.

Guidance contained in this document exists to inform the applicant, to elaborate further on requirements or to provide direction to licensees and applicants on how to meet requirements. It also provides more information about how CNSC staff evaluate specific problems or data during their review of licence applications. Licensees are expected to review and consider guidance; should they choose not to follow it, they should explain how their chosen alternate approach meets regulatory requirements.

For existing facilities: The requirements contained in this document do not apply unless they have been included, in whole or in part, in the licence or licensing basis.

A graded approach, commensurate with risk, may be defined and used when applying the requirements and guidance contained in this regulatory document. The use of a graded approach is not a relaxation of requirements. With a graded approach, the application of requirements is commensurate with the risks and particular characteristics of the facility or activity.

An applicant or licensee may put forward a case to demonstrate that the intent of a requirement is addressed by other means and demonstrated with supportable evidence.

The requirements and guidance in this document are consistent with modern national and international practices addressing issues and elements that control and enhance nuclear safety. In particular, they establish a modern, risk-informed approach to the categorization of accidents – one that considers a full spectrum of possible events, including events of greatest consequence to the public.

Important note: Where referenced in a licence either directly or indirectly (such as through licensee-referenced documents), this document is part of the licensing basis for a regulated facility or activity.

The licensing basis sets the boundary conditions for acceptable performance at a regulated facility or activity and establishes the basis for the CNSC's compliance program for that regulated facility or activity.

Where this document is part of the licensing basis, the word "shall" is used to express a requirement, 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

1. Introduction 1

1.1 Purpose 1

1.2 Scope 1

1.3 Relevant legislation 1

2. Background 1

3. Objectives of the Probabilistic Safety Assessment 2

4. Requirements for a Probabilistic Safety Assessment 2

4.1 Probabilistic safety assessment levels 2

4.2 Management systems or quality assurance 2

4.3 Probabilistic safety assessment models that reflect the plant 3

4.4 Update of probabilistic safety assessment models 3

4.5 Realistic assumptions and data 3

4.6 Consistent level of detail 3

4.7 Methodology and computer codes 3

4.8 Site-specific initiating events and potential hazards 4

4.9 Operational states 4

4.10 Sensitivity and uncertainty analyses 4

5. Guidance on Public Disclosure 4

Glossary 5

References 7

Probabilistic Safety Assessment (PSA) for Nuclear Power Plants

1. Introduction

1.1 Purpose

The purpose of this regulatory document, when incorporated into a licence to construct or operate a nuclear power plant (NPP) or other legally enforceable instrument, is to assure that the licensee conducts a probabilistic safety assessment (PSA) in accordance with defined requirements.

1.2 Scope

This document sets out the requirements for the PSA for a licence to construct or operate an NPP, when required by the applicable licence or other legally enforceable instrument.

1.3 Relevant legislation

The *Nuclear Safety Control Act* (NSCA) and its regulations do not contain explicit references to PSA for NPPs. However, the following provisions are relevant to this document:

- Section 3 of the NSCA, which sets out the purpose of the Act, provides for "the limitation to a reasonable level and in a manner that is consistent with Canada's international obligations of the risks to national security, the health and safety of persons and the environment that are associated with the development, production and use of nuclear energy".
- Subsection 24(4) of the NSCA stipulates that "No licence may be issued, renewed, amended or replaced unless, in the opinion of the Commission, the applicant
    a. is qualified to carry on the activity that the licence authorizes the licensee to carry on; and
    b. will, in carrying on that activity, make adequate provision for the protection of the environment, the health and safety of persons and the maintenance of national security and measures required to implement international obligations to which Canada has agreed"
- Subsection 24(5) of the NSCA stipulates that a licence that is issued by the Commission "may contain any term or condition that the Commission considers necessary for the purposes of this act."

2. Background

The following 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*
- IAEA Safety Standard SSG-4, *Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants*

3. Objectives of the Probabilistic Safety Assessment

The objectives of the probabilistic safety assessment (PSA) are:

a. to provide a systematic analysis, to give confidence that the design will align with the fundamental safety objectives; the fundamental safety objective, as established in IAEA N-SF-1, is to protect people and the environment from harmful effects of ionizing 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, and the first two levels of defence in depth bear the burden of ensuring nuclear safety; reference IAEA INSAG 10 for defence in depth
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 probabilities of occurrence for severe core damage states, and assessments of the risks of major radioactive releases to the environment; severe core damage, for CANDU reactors, is defined as a condition where there is extensive physical damage to multiple fuel channels, leading to loss-of-core structural integrity; risks of major radioactive releases would include small and large release frequencies as defined in RD-337 (or proposed successor document) 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; PSA insights should be used as part of the system for maintaining the emergency operating procedures, as these procedures are subject to improvements throughout an NPP's lifetime
h. to provide insights into the severe accident management program; level 2 PSA can support severe accident management programs; i.e., the development, implementation, training and optimization of accident management strategies and measures

4. Requirements for a Probabilistic Safety Assessment

The licensee shall carry out the following activities:

4.1 Probabilistic safety assessment levels

Perform a level 1 and level 2 PSA for each NPP.

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, with the agreement of persons authorized by the Commission, choose an alternate analysis method to conduct the assessment.

4.2 Management systems or quality assurance

Conduct the PSA under the management system or quality assurance program established in the licensing basis.

Guidance:

The CSA N286 management system requirements standard and CSA N286.7, *Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants*, are referenced in the licensing basis of operating nuclear power plants. The PSA should be developed in a manner that is consistent with the management system.

4.3 Probabilistic safety assessment models that reflect the plant

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.

4.4 Update of probabilistic safety assessment models

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

Guidance:

Update the PSA models so that they adequately represent the as-operated plant conditions.

4.5 Realistic assumptions and data

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.

4.6 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.

4.7 Methodology and computer codes

Seek CNSC acceptance of the methodology and computer codes to be used for the PSA before using them for the purposes of this document.

Guidance:

The methodology should be suitable to support the objectives of the PSA (set forth in section 3 of this document) and to support the intended PSA applications.

Acceptance of the methodology prior to actual PSA development aims to help ensure the methodology can support the PSA's objectives. For example, the computer codes that support the analytical methods should be adequate for the purpose and scope of the analysis.

Note: At the time of publication, the CNSC was reviewing the methodology for developing multi-unit PSA to evaluate the site integrated risk. The CNSC will establish the safety goals for site-wide PSA, which may consider:

- interactions between the units, due to an initiating event (single-unit events and common-mode events), or as a result of the accident progression

- aggregation of risk from internal events, internal hazards, and external hazards during all operating modes for all units at a site
- radioactive sources other than the reactor cores (noting that alternate analysis methods may be used if accepted by the CNSC)

4.8 Site-specific initiating events and potential hazards

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, with the agreement of "persons authorized" by the Commission, choose an alternate analysis method to conduct the assessment of internal hazards and external hazards.

Guidance:

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, 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.

4.9 Operational states

Include at-power and shutdown states. A PSA shall also be performed 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.

4.10 Sensitivity and uncertainty analyses

Include sensitivity analysis, uncertainty analysis and importance measures in the PSA.

5. Guidance on Public Disclosure

In accordance with licensees' public information programs established under RD/GD-99.3, *Public Information and Disclosure*, a summary of the results and assumptions of 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 include security-sensitive information and is subject to applicable information security provisions.

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

Glossary

at power
A plant state characterized by the following conditions:

- the reactor being critical at 100% power
- automatic actuation of safety systems not blocked
- essential support systems aligned in their normal power configuration

cliff-edge effects
A small change of conditions that may lead to a catastrophic increase in the severity of consequences.
Note: Cliff-edge effects can be caused by changes in any of the following: characteristics of the environment; the event; or the plant response.

configuration management
The process of identifying and documenting the characteristics of a facility's structures, systems and components (including computer systems and software), and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation.

external event
An event unconnected with the operation of a facility or with the conduct of an activity and that could have an effect on the safety of the facility or activity.
Note: Typical examples of external events for nuclear facilities include earthquakes, tornadoes, tsunamis and aircraft crashes.

e**xternal hazard**
An event of natural or human-induced origin that originates outside the site and whose effects on the reactor facility are considered as potentially hazardous.

graded approach
A method or process by which elements such as the level of analysis, the depth of documentation and the scope of actions necessary to comply with requirements are commensurate with:

- the relative risks to health, safety, security, the environment, and the implementation of international obligations to which Canada has agreed
- the particular characteristics of a facility or activity

importance measures
Indices that indicate the importance of an event or group of events. These comprise the following three importance measures:

- Fussel-Vesely Importance: for a specific basic event, the fractional contribution to PSA results for all accident sequences containing that basic event
- Risk Increase Ratio (RIR), also referred to as Risk Achievement Worth (RAW): indicates the factor by which the PSA results would increase if the basic event is assumed to happen with certainty (failure probability = 1.0)
- Risk Decrease Ratio (RDR), also referred to as Risk Reduction Worth (RRW): indicates the amount of reduction in the PSA results to be gained if the basic event is assumed to be available (failure probability = 0.0)

internal event
Any event that proceeds from a human error or from a failure of a structure, system or component.

internal hazards
Hazards that originate from the sources located on the site of the reactor facility (both inside and outside plant buildings).

licensing basis
A set of requirements and documents for a regulated facility or activity, comprising:

- the regulatory requirements set out in the applicable laws and regulations
- the conditions and safety and control measures described in the facility's or activity's licence and the documents directly referenced in that licence
- the safety and control measures described in the licence application and the documents needed to support that licence application

nuclear power plant (NPP)
Any nuclear fission reactor installation that has been constructed to generate electricity on a commercial scale and is a Class IA nuclear facility, as defined in the *Class I Nuclear Facilities Regulations*.

probabilistic safety assessment (PSA)
A comprehensive and integrated assessment of the safety of a reactor facility. The safety assessment considers the probability, progression and consequences of equipment failures or transient conditions to derive numerical estimates that provide a consistent measure of the safety of reactor facility, as follows:

- A level 1 PSA identifies and quantifies the sequences of events that may lead to the loss of core structural integrity and massive fuel failures.
- A level 2 PSA starts from the level 1 results, and analyses the containment behaviour, evaluates the radionuclides released from the failed fuel, and quantifies the releases to the environment.
- A level 3 PSA starts from the level 2 results, and analyses the distribution of radionuclides in the environment and evaluates the resulting effect on public health.

Note: A PSA may also be referred to as a probabilistic risk assessment.

sensitivity analysis
The process of assessing the impact on the PSA results from a variation in the probability of an event or a modelling assumption would affect the results of a probabilistic safety analysis.

shutdown state
A subcritical reactor state with a defined margin to prevent a return to criticality without external actions.

uncertainty analysis
The process of identifying and characterizing the sources of uncertainty in the safety analysis, evaluating their impact on the analysis results, and developing, to the extent practicable, a quantitative measure of this impact.

References

- IAEA Safety Standard SSG-3, *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants,* 2010.
- IAEA Safety Standard SSG-4, *Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants,* 2010.
- IAEA INSAG-10, *Defence in Depth in Nuclear Safety, A report by the International Nuclear Safety Advisory Group,* 1996.
- CSA Group, N286-05 (R2011), *Management System Requirements for Nuclear Power Plants*, 2011.
- CSA Group, N286-12, *Management System Requirements for Nuclear Facilities*, 2012.
- CSA Group, N286.7-99, *Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants*, 1999.

CNSC Regulatory Document Series

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

Effective April 2013, the CNSC's catalogue of existing and planned regulatory documents has been organized under three key categories and twenty-five series, as set out below. Regulatory documents produced by the CNSC fall under one of the following 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 Aboriginal engagement
3.3 Financial guarantees
3.4 Commission proceedings
3.5 Information dissemination

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