Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Regulatory Document

RD–310

Safety Analysis for Nuclear Power Plants

February 2008

Canada

CNSC REGULATORY DOCUMENTS

The Canadian Nuclear Safety Commission (CNSC) develops regulatory documents under the authority of paragraphs 9(b) and 21(1)(e) of the *Nuclear Safety and Control Act* (NSCA).

Regulatory documents provide clarifications and additional details to the requirements set out in the NSCA and the regulations made under the NSCA, and are an integral part of the regulatory framework for nuclear activities in Canada.

Each regulatory document aims at disseminating objective regulatory information to stakeholders, including licensees, applicants, public interest groups and the public on a particular topic to promote consistency in the interpretation and implementation of regulatory requirements.

A CNSC regulatory document, or any part thereof, becomes a legal requirement when it is referenced in a licence or any other legally enforceable instrument.

Regulatory Document

RD–310

SAFETY ANALYSIS FOR NUCLEAR POWER PLANTS

Published by the
Canadian Nuclear Safety Commission
February 2008

REGULATORY DOCUMENT

RD–310

SAFETY ANALYSIS FOR NUCLEAR POWER PLANTS

Published by the Canadian Nuclear Safety Commission

© Minister of Public Works and Government Services Canada 2008

Extracts from this document may be reproduced for individual use without permission, provided the source is fully acknowledged. However, reproduction in whole or in part for purposes of resale or redistribution requires prior written permission from the Canadian Nuclear Safety Commission.

Catalogue number: CC173-3/4-310E-PDF
ISBN 978-0-662-47989-5

Ce document est également disponible en français sous le titre *Analyses de la sûreté pour les centrales nucléaires*.

Document availability

The document can be viewed on the CNSC web site at www.nuclearsafety.gc.ca. Copies may be ordered in English or French using the contact information below:

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

Telephone: 613-995-5894 or 1-800-668-5284 (Canada only)
Facsimile: 613-992-2915
E-mail: info@cnsc-ccsn.gc.ca

PREFACE

This regulatory document was developed pursuant to the requirements and obligations set forth in the *General Nuclear Safety and Control Regulations* and in the *Class I Nuclear Facilities Regulations*, where a safety analysis report demonstrating the safety of the nuclear facility must be submitted to the Canadian Nuclear Safety Commission (CNSC).

The document identifies high-level regulatory information for a nuclear power plant licence applicant's preparation and presentation of a safety analysis. The information required adheres to high standards and is consistent with modern national and international practices addressing issues and elements that control and enhance nuclear safety. In particular, it establishes a more modern risk-informed approach to the categorization of accidents, one that considers a full spectrum of possible events including the events of greatest consequence to the public.

The CNSC expects proponents and applicants for new reactor licences to immediately apply this regulatory document in new-build submissions. In the context of existing reactors, CNSC expects the licensees to apply this document, in a graduated manner, to all relevant programs in future submissions.

TABLE OF CONTENTS

SAFETY ANALYSIS FOR NUCLEAR POWER PLANTS

1.0 PURPOSE

The purpose of this regulatory document is to help assure that during the construction, operation or decommissioning of a nuclear power plant (NPP), adequate safety analyses are completed by, or on behalf of, the applicant or licensee in accordance with the *Nuclear Safety and Control Act* (NSCA) and regulatory requirements.

2.0 SCOPE

This document sets out the requirements related to safety analysis, including the selection of events to be analyzed, acceptance criteria, safety analysis methods, and safety analysis documentation and review.

3.0 RELEVANT LEGISLATION

The relevance of the NSCA and the regulations made under the NSCA to this regulatory document is as follows:

1. Subsection 24(4) of the NSCA provides that the Commission may only issue, renew or amend licences if the licensee or the applicant is (a) qualified to carry on the activity that the licence authorizes the licensee to carry on, and (b), in carrying out 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;
2. Subsection 24(5) of the NSCA authorizes the Commission to include in a licence any term or condition that the Commission considers necessary for the purposes of the Act;
3. Paragraph 3(1)(*i*) of the *General Nuclear Safety and Control Regulations* provides that an application for a licence shall contain, in addition to other information, "a description and the results of any test, analysis or calculation performed to substantiate the information included in the application";
4. Paragraph 5(*f*) of the *Class I Nuclear Facilities Regulations* provides that an application for a licence to construct a Class I nuclear facility shall contain, in addition to other information, information on "a preliminary safety analysis report demonstrating the adequacy of the design of the nuclear facility";

5. Paragraph 5(*i*) of the *Class I Nuclear Facilities Regulations* provides that an application for a licence to construct a Class I nuclear facility shall contain, in addition to other information, information on "the effects on the environment and the health and safety of persons that may result from the construction, operation and decommissioning of the nuclear facility…";
6. Paragraph 6(*c*) of the *Class I Nuclear Facilities Regulations* provides that an application for a licence to operate a Class I nuclear facility shall contain, in addition to other information, information on "a final safety analysis report demonstrating the adequacy of the design of the nuclear facility";
7. Paragraph 6(*h*) of the *Class I Nuclear Facilities Regulations* provides that an application for a licence to operate a Class I nuclear facility shall contain, in addition to other information, information on "the effects on the environment and the health and safety of persons that may result from the operation and decommissioning of the nuclear facility…"; and
8. Paragraph 7(*f*) of the *Class I Nuclear Facilities Regulations* provides that an application for a licence to decommission a Class I nuclear facility shall contain, in addition to other information, information on "the effects on the environment and the health and safety of persons that may result from the decommissioning of the nuclear facility…"

4.0 SAFETY ANALYSIS OBJECTIVES

Safety analysis is an essential element of a safety assessment. It is an analytical study used to demonstrate how safety requirements are met for a broad range of operating conditions and various initiating events. Safety analysis involves deterministic and probabilistic analyses in support of the siting, design, commissioning, operation or decommissioning of a nuclear power plant. The requirements for probabilistic safety assessment (PSA) for NPPs are provided in regulatory standard S-294, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*. Regulatory Document RD-310 focuses on the deterministic safety analysis used in the evaluation of event consequences. The objectives of deterministic analysis are to:

1. Confirm that the design of a nuclear power plant meets design and safety requirements;
2. Derive or confirm operational limits and conditions that are consistent with the design and safety requirements for the NPP;
3. Assist in establishing and validating accident management procedures and guidelines; and
4. Assist in demonstrating that safety goals, which may be established to limit the risks posed by the nuclear power plant, are met.

This document identifies high-level requirements for conducting and presenting a safety analysis, taking into account best national and international practices.

5.0 SAFETY ANALYSIS REQUIREMENTS

5.1 Responsibility

The licensee is responsible for ensuring that the safety analysis meets all regulatory requirements. The licensee shall:

1. Maintain adequate capability to perform or procure safety analysis;
2. Establish a formal process to assess and update safety analysis, which takes into account operational experience, research findings and identified safety issues; and
3. Establish and apply a formal quality assurance (QA) process that meets the QA standards established for safety analysis in Canadian Standards Association (CSA) publication N286.7-99, *Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants*.

5.2 Events to be Analyzed

5.2.1 Identifying Events

The licensee shall use a systematic process to identify events, event sequences, and event combinations ("events" hereafter in this document) that can potentially challenge the safety or control functions of the NPP. This process shall be based on regulatory requirements and guidance, past licensing precedents, operational experience, engineering judgment, results of deterministic and probabilistic assessments, and any other systematic reviews of the design.

The identification of events shall account for all operating modes, and the list of identified events shall be reviewed for completeness during the design and analysis process and modified as necessary.

In addition to events that could challenge the safety or control functions of the NPP, safety analysis shall be performed for normal operation.

5.2.2 Scope of Events

The list of events identified for the safety analysis shall include all credible:

1. Component and system failures or malfunctions;
2. Operator errors; and
3. Common-cause internally and externally initiated events.

A cut-off frequency shall be selected so that events with a frequency of occurrence less than the cut-off limit provide only a negligible contribution to the overall risk posed by the NPP. The elimination of such events from the analysis scope shall be justified and the reasons for eliminating them documented.

5.2.3 Classification of Events

The identified events shall be classified, based on the results of probabilistic studies and engineering judgement, into the following three classes of events:

1. Anticipated Operational Occurrences (AOOs) include all events with frequencies of occurrence equal to or greater than 10^{-2} per reactor year;
2. Design Basis Accidents (DBAs) include events with frequencies of occurrence equal to or greater than 10^{-5} per reactor year but less than 10^{-2} per reactor year; and
3. Beyond Design Basis Accidents (BDBAs) include events with frequencies of occurrence less than 10^{-5} per reactor year.

Other factors to be considered in the event classification are any relevant regulatory requirements or historical practices. Events with a frequency on the border between two classes of events, or with substantial uncertainty over the predicted event frequency, shall be classified into the higher frequency class.

Credible common-cause events shall also be classified within the AOO, DBA and BDBA classes.

5.3 Acceptance Criteria

5.3.1 Normal Operation

Analysis for normal operation of the NPP, performed during the design phase, shall demonstrate that:

1. Radiological doses to workers and members of the public are within the limits acceptable to the CNSC; and
2. Releases of radioactive material into the environment fall within the allowable limits for normal operation.

5.3.2 Anticipated Operational Occurrences and Design Basis Accidents

Analysis for AOOs and DBAs shall demonstrate that:

1. Radiological doses to members of the public do not exceed the established limits; and
2. The derived acceptance criteria, established in accordance with 5.3.4 are met.

5.3.3 Beyond Design Basis Accidents

Analysis for BDBAs shall be performed as part of the safety assessment to demonstrate that:

1. The nuclear power plant as designed can meet the established safety goals; and
2. The accident management program and design provisions, put in place to handle the accident management needs, are effective.

5.3.4 Acceptance Criteria for AOOs and DBAs

Qualitative acceptance criteria shall be established for each AOO and DBA to confirm the effectiveness of plant systems in maintaining the integrity of physical barriers against releases of radioactive material. These qualitative acceptance criteria shall satisfy the following general principles:

1. Avoid the potential for consequential failures resulting from an initiating event;
2. Maintain the structures, systems and components in a configuration that permits the effective removal of residual heat;
3. Prevent development of complex configurations or physical phenomena that cannot be modeled with high confidence; and
4. Be consistent with the design requirements for plant systems, structures and components.

To demonstrate that these qualitative acceptance criteria applicable to the analyzed AOO or DBA are met, quantitative derived acceptance criteria shall be identified prior to performing the analysis. Such derived acceptance criteria shall be supported by experimental data.

The results of safety analysis shall meet appropriate derived acceptance criteria with margins sufficient to accommodate uncertainties associated with the analysis.

The analysis shall be performed for the event that poses the most challenges in demonstrating the meeting of derived acceptance criteria (i.e., the limiting event in an event category).

5.4 Safety Analysis Methods and Assumptions

5.4.1 General

The analysis shall provide the appropriate level of confidence in demonstrating conformity with the acceptance criteria. To achieve the appropriate level of confidence, the safety analysis shall:

1. Be performed by qualified analysts in accordance with an approved QA process;
2. Apply a systematic analysis method;

3. Use verified data;
4. Use justified assumptions;
5. Use verified and validated models and computer codes;
6. Build in a degree of conservatism; and
7. Be subjected to a review process.

5.4.2 Analysis Method

The analysis method shall include the following elements:

1. Identifying the scenarios to be analyzed as required to attain the analysis objectives;
2. Identifying the applicable acceptance criteria, safety requirements, and limits;
3. Identifying the important phenomena of the analyzed event;
4. Selecting the computational methods or computer codes, models, and correlations that have been validated for the intended applications;
5. Defining boundary and initial conditions;
6. Conducting calculations, including sensitivity cases, to predict the event transient, starting from the initial steady state up to the pre-defined end-state;
7. Accounting for uncertainties in the analysis data and models;
8. Verifying calculation results for physical and logical consistency; and
9. Processing and documenting the results of calculations to demonstrate conformance with the acceptance criteria.

5.4.3 Analysis Data

The safety analysis shall be based on complete and accurate design and operational information.

The boundary and initial conditions used as the analysis input data shall:

1. Reflect accurately the NPP configuration;
2. Account for the effects of aging of systems, structures and components;
3. Account for various permissible operating modes; and
4. Be supported by experimental data, where operational data is not available.

Significant uncertainties in analysis data, including those associated with nuclear power plant performance, operational measurements, and modeling parameters, shall be identified.

5.4.4 Analysis Assumptions

Assumptions made to simplify the analysis, as well as assumptions concerning the operating mode of the nuclear power plant, the availability and performance of the systems, and operator actions, shall be identified and justified.

The analysis of AOO and DBA shall:

1. Apply the single-failure criterion to all safety systems and their support systems;
2. Account for consequential failures that may occur as a result of the initiating event;
3. Credit actions of systems only when the systems are qualified for the accident conditions, or when their actions could have a detrimental effect on the consequences of the analyzed accident;
4. Account for the possibility of the equipment being taken out of service for maintenance; and
5. Credit operator actions only when there are
    a) unambiguous indications of the need for such actions,
    b) adequate procedures and sufficient time to perform the required actions, and
    c) environmental conditions that do not prohibit such actions.

For the analysis of BDBA, it is acceptable to use a more realistic analysis methodology consisting of assumptions which reflect the likely plant configuration, and the expected response of plant systems and operators in the analysed accident.

5.4.5 Computer Codes

Computer codes used in the safety analysis shall be developed, validated, and used in accordance with a quality assurance program that meets the requirements of CSA N286.7-99.

5.4.6 Conservatism in Analysis

The safety analysis shall build in a degree of conservatism to off-set any uncertainties associated with both NPP initial and boundary conditions and modeling of nuclear power plant performance in the analyzed event. This conservatism shall depend on event class, and shall be commensurate with the analysis objectives.

5.5 Safety Analysis Documentation

The safety analysis documentation shall be comprehensive and sufficiently detailed to allow for a conclusive review. The document shall include:

1. The technical basis for the analyzed event and key phenomena and processes;

2. A description of the analyzed facility, including important systems and their performance, as well as operator actions;
3. Information describing the analysis method and assumptions;
4. A description of the assessments of code applicability for the analyzed event and computer code uncertainty; and
5. A description of the analysis results in a manner that facilitates their understanding and the drawing of conclusions related to conformance with acceptance criteria.

Analysis documentation shall facilitate the update of the analysis when new results become available.

5.6 Safety Analysis Review and Update

5.6.1 Review of Safety Analysis Results

The licensee shall systematically review the safety analysis results to ensure that they are correct and meet the objectives set for the analysis. The results shall be assessed against the relevant requirements, applicable experimental data, expert judgment, and comparison with similar calculations and sensitivity analyses.

The licensee shall review the analysis results using one or more of the following techniques, depending on the objectives of the analysis:

1. Supervisory review;
2. Peer review;
3. Independent review by qualified individuals; and
4. Independent calculations using alternate tools and methods to the extent practicable.

5.6.2 Update of Safety Analysis

The safety analysis shall be periodically reviewed and updated to account for changes in NPP configuration, conditions (including those due to aging), operating parameters and procedures, research findings, and advances in knowledge and understanding of physical phenomena, in accordance with CNSC regulatory standard S-99, *Reporting Requirements for Operating Nuclear Power Plants*.

In addition to periodic updates, the safety analysis shall also be updated following the discovery of information that may reveal a hazard that is different in nature, greater in probability, or greater in magnitude than was previously presented to the CNSC in the licensing documents.

5.7 Quality of Safety Analysis

Safety analysis shall be subject to a comprehensive QA program applied to all activities affecting the quality of the results. The QA program shall identify the quality assurance standards to be applied and shall include documented procedures and instructions for the complete safety analysis process, including, but not limited to:

1. Collection and verification of NPP data;
2. Verification of the computer input data;
3. Validation of NPP and analytical models;
4. Assessment of simulation results; and
5. Documentation of analysis results.

GLOSSARY

Acceptance criteria
Specified bounds on the value of a functional or conditional indicator used to assess the ability of a system, structure or component to meet its design and safety requirements.

Accident
Any unintended event, including operating errors, equipment failures or other mishaps, the consequences or potential consequences of which are not negligible from the point of view of protection or safety.

Anticipated operational occurrence (AOO)
An operational process deviating from normal operation that is expected to occur once or several times during the operating lifetime of the NPP but which, in view of the appropriate design provisions, does not cause any significant damage to items important to safety nor lead to accident conditions.

Best estimate method
A method designed to give realistic results.

Beyond design basis accident (BDBA)
Accident conditions less frequent and more severe than a design basis accident. A BDBA may or may not involve core degradation.

Common cause
A cause for a concurrent failure of two or more structures, systems or components, such as natural phenomena (earthquakes, tornadoes, floods, etc.), design deficiency, manufacturing flaws, operation and maintenance errors, human-induced destructive events and others.

Conservative method
A method deliberately leading to results that are intended to be limiting relative to specified acceptance criteria.

Design basis accident (DBA)
Accident conditions against which an NPP is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.

Deterministic safety analysis
An analysis of nuclear power plant responses to an event, performed using predetermined rules and assumptions (e.g., those concerning the initial operational state, availability and performance of the systems and operator actions). Deterministic analysis can use either conservative or best estimate methods.

Event category
A group of events characterized by the same, or similar, cause and similarity in the governing phenomena.

Normal operation
Operation of an NPP within specified operational limits and conditions including start-up, power operation, shutting down, shutdown, maintenance, testing and refuelling.

NPP
See nuclear power plant.

Nuclear power plant
Also referred to as an NPP, a nuclear power plant is any fission-reactor installation that has been constructed to generate electricity on a commercial scale. A nuclear power plant is a Class IA nuclear facility, as defined in the Class I Nuclear Facilities Regulations.

Operational limits and conditions
A set of rules setting forth parameter limits or conditions that ensures the functional capability and the performance levels of equipment for safe operation of an NPP.

Operational mode
Operational mode may include start-up, operation at various power levels, shutting down, shutdown, maintenance, testing and refuelling.

Safety analysis
Evaluation of the potential hazards associated with the conduct of a proposed activity.

Safety assessment
Assessment of all aspects of the siting, design, commissioning, operation or decommissioning of an authorized facility that is relevant to safety.

Sensitivity analysis
A quantitative examination of how the behaviour of a system varies with change, usually in the values of the governing parameters.

Single-failure criterion
The criterion used to determine whether a system is capable of performing its function in the presence of a single failure.

Structures, systems and components (SSCs)
A general term encompassing all of the elements (items) of a facility or activity which contribute to protection and safety, except human factors.

Support features of safety systems
The collection of equipment that provides services such as cooling, lubrication and energy supply required by the protection system and the safety actuation systems.

ASSOCIATED DOCUMENTS

1. *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*, S-294. Canadian Nuclear Safety Commission, Ottawa, 2005.

2. *Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants*. N286.7-99. Canadian Standards Association, 2003.

3. *Reporting Requirements for Operating Nuclear Power Plants*, S-99. Canadian Nuclear Safety Commission, Ottawa, 2003.