Canada's Nuclear Regulator

Safety Analysis

Safety Analysis for Class IB Nuclear Facilities

REGDOC-2.4.4

October 2022

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Canada

Safety Analysis for Class IB Nuclear Facilities
Regulatory document REGDOC-2.4.4

© Canadian Nuclear Safety Commission (CNSC) 2022
Cat. No. CC172-243/2022E-PDF
ISBN 978-0-660-45597-6

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 CNSC.

Également publié en français sous le titre : Analyse de la sûreté pour les installations nucléaires de catégorie IB

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, Stn B
Ottawa, ON K1P 5S9
CANADA

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

Publishing history
October 2022 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, probabilistic safety assessment 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-2.4.4, *Safety Analysis for Class IB Nuclear Facilities*, clarifies requirements and provides guidance for applicants and licensees on how to demonstrate the safety of a Class IB nuclear facility, including information relating to:

- the safety analysis program (the managed process that governs the conduct of a safety analysis)
- the conduct of a safety analysis (the systematic evaluation of the potential hazards)
- safety analysis documents, records and reporting

This document is the first version of REGDOC-2.4.4, *Safety Analysis for Class IB Nuclear Facilities*.

Class IB nuclear facilities have risk profiles that vary significantly, depending on the particular characteristics of the activity or facility. The licensee may propose specific design measures, analyses or other measures that are commensurate with the level of risk posed, based on the CNSC's risk-informed graded approach, if they provide adequate justification.

For additional information on safety analysis for the post-closure phase of a disposal facility, see REGDOC-2.11.1, *Waste Management, Volume III: Safety Case for the Disposal of Radioactive Waste*.

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

1. Introduction ... 1

1.1 Purpose ... 1
1.2 Scope ... 1
1.3 Relevant legislation ... 2

2. Safety Objectives ... 2

2.1 Defence in depth ... 2
2.2 Safety analysis objectives ... 3

3. Safety Analysis Program ... 4

4. Safety Analysis ... 5

4.1 Classification of events into facility states ... 5
4.2 Safety analysis assumptions ... 6
4.3 Postulated initiating events ... 6
4.3.1 Identification of postulated initiating events ... 7
4.3.2 Classification of postulated initiating events ... 7
4.4 Safety assessment ... 8
4.4.1 Assessment of consequences ... 8
4.4.2 Assessment of likelihood ... 8
4.5 Identification of structures, systems and components important to safety ... 9
4.6 Operational limits and conditions ... 9
4.7 Acceptance criteria ... 10
4.8 Safety goals ... 11

5. Safety Analysis Documents and Records ... 11

5.1 Purpose and scope of safety analysis documents and records ... 11
5.2 Content of safety analysis documents and records ... 12
5.3 Documenting and recording postulated initiating events and design-basis accidents ... 13
5.4 Maintaining safety analysis documents and records ... 13

6. Validation and Verification of Safety Analysis Tools ... 14

7. Graded Approach ... 14

Appendix A: Sample Structure and Content for a Safety Analysis Report ... 15

Appendix B: Sample Parameters for Operational Limits and Conditions ... 18

Appendix C: Postulated Initiating Events 20

C.1 Selected postulated initiating events 20

C.2 Range of selected events to be considered for applicability 21

References 24

Additional Information 26

Safety Analysis for Class IB Nuclear Facilities

1. Introduction

1.1 Purpose

This regulatory document clarifies requirements and provides guidance for applicants and licensees on how to demonstrate the safety of a Class IB nuclear facility, including information relating to:

- the safety analysis program (the managed process that governs the conduct of a safety analysis)
- the conduct of a safety analysis (the systematic evaluation of the potential hazards)
- safety analysis documents, records and reporting

Note: Throughout this regulatory document, the term "nuclear facility" means a Class IB nuclear facility.

1.2 Scope

This document provides requirements and guidance for the safety analysis of the following Class IB nuclear facilities:

- a facility for the processing, reprocessing or separation of an isotope of uranium, thorium or plutonium
- a facility for the manufacture of a product from uranium, thorium or plutonium
- a facility, other than a Class II nuclear facility as defined in section 1 of the *Class II Nuclear Facilities and Prescribed Equipment Regulations*, for the processing or use, in a quantity greater than 10^{15} Bq per calendar year, of nuclear substances other than uranium, thorium or plutonium
- a facility for the disposal of a nuclear substance generated at another nuclear facility
  - **note:** this regulatory document applies to the operational phase, which includes the licensed activities conducted up to the closure of the disposal facility
- a facility prescribed by paragraph 19(a) or (b) of the *General Nuclear Safety and Control Regulations*:
  - a facility for the management, storage or disposal of waste containing radioactive nuclear substances at which the resident inventory of radioactive nuclear substances contained in the waste is 10^{15} Bq or more
    [**note:** for the scope of this regulatory document, some examples of these facilities include:
    - any facility for the storage of fissionable material before and after irradiation
    - any facility for associated waste conditioning or effluent treatment, and facilities for storage of waste that allow for retrieval of the waste for later disposal]
  - a plant for the production of deuterium or deuterium compounds using hydrogen sulphide

For additional information on safety analysis for the post-closure phase of a disposal facility, see REGDOC-2.11.1, *Waste Management, Volume III: Safety Case for the Disposal of Radioactive Waste* [1].

Note: Given the wide range of Class IB nuclear facilities, a graded approach may be proposed by the licensee in accordance with REGDOC-3.5.3, *Regulatory Fundamentals* [2].

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, subsections 24(4) and 24(5)
- *General Nuclear Safety and Control Regulations*, paragraph 3(1)(i)
- *Class I Nuclear Facilities Regulations*, paragraphs 5(f) and (i); paragraphs 6(c) and (h); and paragraph 7(f)

2. Safety Objectives

Safety analysis is a systematic evaluation of the potential hazards associated with the conduct of a proposed activity or facility, and that considers the effectiveness of preventive measures and strategies in reducing the effects of such hazards.

A safety analysis program is designed, developed and maintained by the licensee, and is reviewed by CNSC staff. It is documented in a safety analysis report (SAR). As stated in paragraphs 5(f) and 6(c) of the *Class I Nuclear Facilities Regulations*:

- "An application for a licence to construct a Class I nuclear facility shall contain the following information... (f) a preliminary safety analysis report demonstrating the adequacy of the design of the nuclear facility;"
- "An application for a licence to operate a Class I nuclear facility shall contain the following information... (c) a final safety analysis report demonstrating the adequacy of the design of the nuclear facility;"

The SAR may reference other safety analysis documentation.

A facility's SAR forms an important part of the licensing basis for the facility. It is used to:

- establish limits for the safe operation of the facility
- assess proposed changes to the facility
- develop and maintain the licensee's policies, processes and procedures for the safe conduct of the licensed activities
- confirm that the design of the facility meets design and safety requirements

2.1 Defence in depth

Requirements

The licensee shall address the concept of defence in depth when developing a safety analysis for a nuclear facility.

Guidance

Five levels of defence in depth are normally defined for nuclear facilities, in accordance with the guidance provided in REGDOC-3.5.3, *Regulatory Fundamentals* [2]. Safety analysis plays a major role in demonstrating that levels 1 to 4 have been achieved. The applicability of safety analysis to these levels is as follows:

Level 1 The aim of the first level of defence is to prevent deviations from normal operation, and to prevent failures of structures, systems and components (SSCs) relied upon for safety.

Level 2 The aim of the second level of defence is to detect, intercept and control deviations from normal operation in order to prevent anticipated operational occurrences (AOOs) from escalating to accident conditions, and to return the facility to a state of normal operation.

Level 3 The aim of the third level of defence is to minimize the onsite consequences of accidents by providing inherent safety features, fail-safe design, additional equipment and mitigating procedures. The most important objective for this level is to prevent releases of nuclear and associated hazardous substances or radiation levels that require offsite protective actions.

Level 4 The aim of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth. The most important objective for this level is to maintain the containment function, thus ensuring that radioactive releases are kept as low as reasonably achievable.

Level 5 The aim of the fifth level of defence is to mitigate the radiological consequences and associated chemical consequences of releases or radiation levels that may result from accidents by means of adequately equipped emergency response facilities, emergency plans, and emergency procedures for onsite and offsite emergency response.

For more information on defence in depth, including means of achieving its aims (such as good design and proven engineering practices), see:

- REGDOC-3.5.3, *Regulatory Fundamentals* [2]
- IAEA Specific Safety Requirements No. SSR-4, *Safety of Nuclear Fuel Cycle Facilities* [3]

2.2 Safety analysis objectives

The objectives of a safety analysis are to:

- state the safety goals, objectives and acceptance criteria (the safety requirements) that the facility is designed to meet
- demonstrate that the safety goals, objectives and acceptance criteria are met
- derive or confirm operational limits and conditions (OLCs) that are consistent with the design and safety requirements of the facility
- identify the SSCs important to safety [4] (that is, the SSCs that are relied upon for the safety of the facility)
- provide results for use in establishing and validating operating and emergency procedures and guidelines

Requirements

The licensee shall maintain adequate capability to perform or procure a safety analysis to:

- resolve technical issues that arise over the life of the nuclear facility
- ensure the safety analysis requirements are met (whether the safety analysis has been developed by the licensee or procured from a third party)

The licensee shall establish a process to assess and update the safety analysis to ensure that the safety analysis reflects:

- current configuration (for existing facilities)
- current operating limits and conditions (for existing facilities)
- operating experience, including experience from similar facilities and any applicable experience from other nuclear or industrial facilities
- if applicable to the specific Class IB nuclear facility, results from experimental research, improved theoretical understanding or new modelling capabilities to assess potential effects on the conclusions of safety analyses
- if applicable to the specific Class IB nuclear facility, considerations of human factors to ensure that credible estimates of human performance are used in the analysis

The licensee shall systematically review the safety analysis results to ensure that they remain valid and continue to meet the safety goals, objectives and acceptance criteria.

Guidance

The licensee is responsible for the safety analysis whether it is performed by staff or by a service that is procured to do so. Supplier qualification requirements help to ensure an adequate selection is made for the provision of a service, such as a safety analysis. Therefore, it is necessary for the licensee to possess the ability to:

- qualify the supplier
- assess the sufficiency of the service provided

For more information on demonstrating the capability of a licensee's staff to perform a safety analysis, or on procuring safety analysis as a service, see:

- CSA N286-12, *Management System Requirements for Nuclear Facilities* [5]
- IAEA Safety Guide No. GS-G-3.5, *The Management System for Nuclear Installations* [6]

3. Safety Analysis Program

Requirements

The licensee shall develop, implement, conduct and maintain a safety analysis program for the nuclear facility.

In support of the program, the licensee shall establish one or more internal safety committees to advise the organization's management on safety issues related to the commissioning, operation and modification of the facility. The licensee shall ensure that the committee has the necessary breadth of knowledge and experience to provide appropriate advice. The members shall, to the extent necessary, be independent of the operations management raising the safety issue.

Essential elements of a safety analysis program are the statements made by the licensee about the licensee's safety, health and environmental policies [3]. The licensee shall provide these statements in the licence application as a declaration of the organization's objectives and the public commitment of corporate management. To put these statements into effect, the licensee shall also specify and put in place organizational structures, standards and management arrangements capable of meeting the organization's objectives and public commitments.

The licensee shall demonstrate that the safety analysis program is governed by the licensee's management system and is consistent with the applicable requirements of CSA N286-12, *Management System Requirements for Nuclear Facilities* [5].

Guidance

For more information on establishing internal safety committees, see IAEA Specific Safety Requirements No. SSR-4, *Safety of Nuclear Fuel Cycle Facilities* [3].

The licensee is not required to create a separate document for the safety analysis program – neither as a standalone document nor within the SAR.

The CNSC accepts that the licensee's safety analysis program may not map exactly onto the CNSC's requirements and expectations for this area. However, the licensee should be able to demonstrate how all the requirements and expectations are addressed by various programs under the overall management system.

In establishing internal safety committees, the licensee should involve staff with a variety of perspectives; for example, employee representatives.

4. Safety Analysis

Requirements

The licensee shall perform a safety analysis for normal operation, and for internal and external events that deviate from normal operation and belong to a category of credible abnormal events [7].

4.1 Classification of events into facility states

Requirements

The licensee shall classify events into one of the facility states: anticipated operational occurrence (AOO), design-basis accident (DBA), beyond-design-basis accident (BDBA) and specific ranges within BDBA referred to as design extension conditions (DEC), or equivalent classification scheme.

The licensee shall ensure that the safety analysis examines the following facility states:

- normal operational modes (including maintenance and shutdown)
- AOO
- DBA
- DEC

For additional information on classification and ranges of events, refer to appendix C.

Guidance

The licensee may use an alternative classification scheme, provided the classifications meet the same risk-based intent.

4.2 Safety analysis assumptions

Safety analysis assumptions depend on a number of factors:

- the overall risk profile of the nuclear facility
- the event being analyzed (AOO, DBA or DEC)
  - for AOO and DBA, conservative assumptions are to be used (to demonstrate the effectiveness of the safety systems)
  - for DEC, a best-estimate approach and assumptions are to be used
- state of knowledge of the event progression and consequences

Requirements

The licensee shall not credit systems that are not qualified to operate in a post-accident environment.

To credit operator action, the licensee shall demonstrate that the following are in place:

- clear, well-defined, validated and readily available operating procedures that identify the necessary actions
- instrumentation at the control location to provide clear and unambiguous indications of the need for operator action
- a credible, protected and accessible path for the operator to safely carry out the actions required in the procedures
- training for any person who may be expected to perform the operator actions

The licensee shall set operator action times. The licensee shall add additional time to include, as appropriate, dressing in protective equipment; accessing remote equipment; and transporting, connecting and operating temporary equipment. The SAR shall justify the operator action time.

Guidance

After an indication of the need for operator action, the operator action credited in the safety analysis report should be delayed by:

- at least 15 minutes at the control location
- at least 30 minutes outside the control location

These operator action times are for the start of the action.

For more information on crediting SSCs important to safety, see REGDOC-2.5.2, *Design of Reactor Facilities* [8]. **Note:** This reference is provided only as a source of information; the licensee does not need to apply the requirements or other guidance in REGDOC-2.5.2 to its safety analysis for a Class IB nuclear facility.

4.3 Postulated initiating events

Guidance

A postulated initiating event (PIE) is not necessarily an accident itself. A PIE is the event that initiates a sequence that may lead to an AOO, a DBA, or a BDBA, depending on the additional failures that occur.

The primary causes of PIEs may be credible equipment failures and worker errors, human-induced events or natural events.

The safety analysis and design for the nuclear facility shall consider not only the facility itself, but also the interfaces with other facilities and installations that may affect its safety. For more information, refer to IAEA Specific Safety Requirements No. SSR-4, *Safety of Nuclear Fuel Cycle Facilities* [3].

For additional information on types of PIEs and ranges of conditions, refer to appendix C.

4.3.1 Identification of postulated initiating events

Requirements

The licensee shall identify PIEs (both internally and externally initiated) that could lead to:

- radiation exposure to workers or to the public
- a release of significant amounts of nuclear substances
- a release of hazardous substances (such as hazardous chemicals) associated with the nuclear substances

The licensee shall describe the methods used to identify the PIEs.

The licensee shall document and maintain the resulting list of PIEs. With input from technical specialists and experts in safety analysis, the licensee shall conduct a review of the list of PIEs:

- initially, to determine that the list is comprehensive and that the events include:
  - all credible failures of the facility's SSCs
  - all credible human errors that could occur in any of the operating conditions of the facility
- regularly, to confirm the relevance of the current list and revise it as necessary, given that relevant PIEs may change as the facility goes through different phases of its lifecycle (for example, as a result of aging effects)

Guidance

The list of PIEs should be developed through a comprehensive assessment of credible failures of the facility's SSCs and documentation of credible human errors that could occur in any of the operating conditions of the facility.

The list of PIEs may take many forms, depending on the complexity of the activity or facility. The licensee should develop a list that is specific to their situation, and that takes into account the nuclear and associated hazardous substances of the specific activity or facility.

On their initial list, the licensee should include as many PIEs as have been identified. If additional PIEs are subsequently identified, the licensee should revise their safety analysis to include those PIEs.

4.3.2 Classification of postulated initiating events

Requirements

During the safety assessment as described in section 4.4, the licensee shall classify PIEs and event sequences upon identification, for the purpose of demonstrating that the acceptance criteria and the safety goals are met.

Guidance

The licensee should group PIEs with similar characteristics (in particular, those that make similar demands on the mitigating measures) into event groups. For the safety assessment, the licensee should identify bounding events from each event group.

4.4 Safety assessment

Safety assessment includes an evaluation of the risk associated with the hazards of a nuclear facility. The assessment can be quantitative, qualitative, or a mix of both (semi-quantitative).

4.4.1 Assessment of consequences

Requirements

The licensee shall perform a deterministic safety analysis (that is, an assessment of the consequences) to identify the physical process occurring in the nuclear facility during an event and to assess the consequences. The licensee shall justify the assumptions and the actions of qualified mitigating measures (such as safety systems and operator actions) used in the deterministic analysis.

When the deterministic analysis is quantitative, the licensee shall develop models of the physical processes to calculate the consequences of the event. The licensee shall validate the computational tools used to calculate the consequences.

Guidance

The licensee should ensure that the level and rigour of validation of the computational tools is commensurate with the level of risk for the activity or facility (that is, apply a graded approach).

Applicants or licensees may use commercially available modelling software and data analysis software; to demonstrate validation of these tools, the licensee may submit the software vendor's validation of the software for this application.

For more information on demonstrating validation of software tools, see:

- section 6 of this regulatory document
- CSA N286.7-16, *Quality Assurance of Analytical, Scientific and Design Computer Programs* [9]

4.4.2 Assessment of likelihood

Requirements

The licensee shall perform an assessment of likelihood to establish the likelihood of PIEs or event sequences to occur.

Guidance

Typically for Class IB nuclear facilities, the licensee performs a qualitative or semi-quantitative assessment of the likelihood of PIEs or event sequences using one of the following methods:

- deterministic safety analysis methods, as published in IAEA Safety Guide No. SSG-5, *Safety of Conversion Facilities and Uranium Enrichment Facilities* [10], and IAEA Safety Guide No. SSG-6, *Safety of Uranium Fuel Fabrication Facilities* [11]

- methods for assessment of likelihood, as published in IAEA TECDOC No. 1267, *Procedures for Conducting Probabilistic Safety Assessment for Non-Reactor Nuclear Facilities* [12]; numerous methods may be used, either in a quantitative or qualitative manner, such as:
  - hazard and operability studies (HAZOPs)
  - failure mode and effects analysis
  - fault tree / event tree analysis
  - operational feedback; for example, through the fuel incident notification and analysis system (FINAS) database and locally recorded events for each facility
  - what-if technique
  - checklists (for example, ergonomics checklists)
  - master logic diagram

4.5 Identification of structures, systems and components important to safety

Requirements

The licensee shall use a safety assessment, or an equivalent methodology, to identify event sequences that may lead to an AOO, DBA, DEC or BDBA. For additional information, see IAEA Specific Safety Requirements No. SSR-4, *Safety of Nuclear Fuel Cycle Facilities* [3].

For each event sequence, the licensee shall identify the safety functions, the corresponding SSCs important to safety [4], and the administrative safety requirements that are used to implement the defence-in-depth concept.

To be consistent with the safety analysis results, the licensee shall ensure that [3]:

- SSCs important to safety are designed to withstand the effects of extreme loadings and environmental conditions (such as extremes of temperature, humidity, pressure and radiation levels) that may be encountered in operational states and in accident conditions
- the required intervals for periodic testing and inspection of SSCs important to safety are defined
- the codes and standards applicable to SSCs important to safety are identified, and their use is justified
- the necessary levels of availability and reliability of SSCs important to safety, as established in the safety analysis, are attained

In protecting against potential hazards, the licensee shall ensure that the following hierarchy of design and administrative measures is used to the extent practicable [3]:

1. selection of the process (to eliminate the hazard)
2. passive design features
3. active design features
4. administrative controls

4.6 Operational limits and conditions

Requirements

The licensee shall derive the OLCs from the safety analysis. The licensee shall document the OLCs before starting operation of the facility.

Guidance

OLCs include limiting conditions for safe operation (values, conditions), monitoring systems and associated alarm settings, and surveillance and administrative requirements.

Staff availability and competency are an important component of the operational conditions. The OLCs should set minimum requirements for the availability of staff and equipment. For more information on the availability of staff, see REGDOC-2.2.5, *Minimum Staff Complement* [13].

Where it is not practicable to define precisely the safe limits of all relevant parameters, OLCs should be set to define the limits of the assessment in order to prevent operation in the unanalyzed or unanalyzable conditions.

Appendix B provides examples of parameters that may be managed through OLCs across the broad range of facilities.

4.7 Acceptance criteria

Requirements

The licensee shall establish explicit criteria for the level of safety to be achieved to demonstrate that the licensee is making adequate provision for the protection of the environment and the health and safety of persons [3].

The licensee shall set limits on the radiological consequences and associated chemical consequences for workers and the public of direct exposures to radiation or discharges of radionuclides to the environment. These limits shall:

- be set equal to, or below:
  - the provisions of the *Radiation Protection Regulations*, when applicable and as far as practicable; otherwise
  - criteria established by national or international standards as triggers for protective measures during radiological or chemical emergencies (for example, for sheltering or for distribution of iodine pills)
- apply to the consequences of operational states and the possible consequences of AOO and DBA at the facility
- apply at the site boundaries of the licensed facility when offsite consequences to the public are considered

For new designs, the licensee shall consider targets that are below these limits.

The licensee shall establish derived acceptance criteria to demonstrate that the barriers to prevent the release of nuclear or associated hazardous substances are effective; that is, the barriers:

- avoid the potential for consequential failures resulting from an initiating event
- maintain SSCs important to safety in a configuration that prevents releases of nuclear or associated hazardous substances to the environment or in the facility
- prevent consequences that extend beyond the site boundaries of the licensed facility
- are consistent with the design requirements for the facility's SSCs

For acceptance criteria for nuclear criticality safety, see REGDOC-2.4.3, *Nuclear Criticality Safety* [14].

4.8 Safety goals

Requirements

The licensee shall demonstrate that the offsite consequences, as calculated at the site boundaries of the licensed facility, of a BDBA included in the DEC do not exceed criteria established as a trigger for temporary evacuation, for long-term relocation of the local population, or for both temporary evacuation and long-term relocation in:

- Health Canada's *Canadian Guidelines for Intervention During a Nuclear Emergency* [15]
- IAEA General Safety Requirements No. GSR Part 7, *Preparedness and Response for a Nuclear or Radiological Emergency* [16]

In addressing the concept of defence in depth, the licensee shall include events from BDBAs in the DEC. As a minimum, the licensee shall include the following events in the DEC [7]:

- an extended loss of AC power (ELAP)
- PIEs and event sequences, including those that are specific or unique to the facility, that belong to a category of credible abnormal events [7]

For naturally occurring PIEs (for example, seismic events, flooding and severe weather), when selection of credible abnormal events is not practical, the licensee shall include in the DEC events that are more severe than considered in analyses of DBAs consistent with the guidance of national or international standards (see appendix C).

The classification shall be based on likelihood, as specified in section 4.4.2.

5. Safety Analysis Documents and Records

The safety analysis documents describe the methods used in performing analyses and record the results of each analysis. They support the siting, design, commissioning, operation and decommissioning of a nuclear facility. They demonstrate that any risks to the health and safety of persons are managed and mitigated, and also help to demonstrate that defence in depth has been achieved.

5.1 Purpose and scope of safety analysis documents and records

Guidance

The safety analysis documents and records provide information on the safety analysis, as follows:

- demonstrate that the safety goals, objectives and acceptance criteria are met
- assist in deriving or confirming operational limits and conditions that are consistent with the design and safety requirements of the facility
- assist in establishing and validating operating and emergency procedures and guidelines

The scope of safety analysis documents and records covers internal and external events that could lead to a release of nuclear or associated hazardous substances, to a criticality accident, or to an accidental exposure to high radiation fields.

5.2 Content of safety analysis documents and records

Requirements

The licensee shall report the safety analysis results in sufficient detail to permit review by CNSC staff.

The licensee shall ensure that the content of the safety analysis documents and records for a facility includes, as a minimum, the SAR and the OLCs (or equivalent) [3].

The SAR shall contain a representative summary of the safety analysis documents and records. The SAR shall:

- describe the site characteristics
- identify nuclear and associated hazardous substances and their locations
- identify applicable acceptance criteria for offsite consequences to the public of pertinent accidents (some examples of pertinent accidents are radiological, nuclear criticality, fire and chemical accidents, including explosions)
- identify SSCs that prevent or mitigate release of nuclear or associated hazardous substances, or prevent accidental exposure to high radiation fields (to the extent appropriate for the facility, in accordance with a graded approach)
- classify SSCs in accordance with their importance to safety
- identify operating and emergency procedures and actions that prevent or mitigate release of nuclear or associated hazardous substances
- identify the safety analysis assumptions (some examples are boundary conditions, facility configuration, and time for operator actions); many of these assumptions may be documented in the operational limits and conditions
- identify credible initiating events that may affect the licensee's control of nuclear or associated hazardous substances, including:
  - internal events (for example, component failures, human error, fire or flood)
  - external events (for example, earthquake, fire, flood or extreme weather)
- group together all initiating events that have similar characteristics and identify bounding events for analysis
- provide the results of the analysis of the consequences of the analyzed events
- include uncertainty and sensitivity analysis results, when applicable
- compare the results to acceptance criteria
- provide results and conclusions
- be independently reviewed as per the management system of the licensee
- provide references to detailed analyses that support the safety analysis results

Guidance

The licensee may incorporate information by reference. For example, many of the safety analysis assumptions may be documented in the licensee's operational limits and conditions and may be incorporated into the SAR by reference.

The licensee should ensure that staff with a variety of perspectives (for example, employee representatives) have an opportunity to review the SAR and to provide independent comments.

Risks to the environment as a result of routine releases (which are considered part of normal operation) are considered in the licensee's environmental risk assessment (ERA) for the facility, and therefore are not considered in the SAR.

For more information on:

- validation and verification of safety analysis tools, see section 6
- a sample structure and content for a SAR, see appendix A

5.3 Documenting and recording postulated initiating events and design-basis accidents

Requirements

The licensee shall describe the facility's behaviour following a PIE and compare it to the analysis acceptance criteria.

Guidance

For DBAs, the licensee should describe each event in the SAR as follows:

- the timing of the main events, including:
  - the initial event and any subsequent failures
  - times at which mitigating equipment is actuated
  - times of operator actions
  - time at which a safe long-term stable state is achieved
- graphical presentation of key parameters as functions of time during the event (the parameters should be selected so that a full understanding of the event's progression can be obtained within the context of the acceptance criterion being considered)
- comparison with acceptance criteria
- the conclusion of the event

5.4 Maintaining safety analysis documents and records

The SAR and other safety analysis documents and records are updated periodically throughout the lifecycle of the facility. The period for SAR updates is stated in each facility's licence conditions handbook (LCH). Five years is the recommended period, but different periods may be set; for example, based on the overall safety impact of the facility or on significant changes to the facility.

Requirements

The licensee shall perform an ongoing site evaluation. If the ongoing site evaluation identifies new information about the site characteristics (that is, changing the results of the identification and classification of PIEs), then safety precautions (such as engineering controls and emergency arrangements) may need to be reviewed and revised.

Guidance

The process for updates should meet the requirements of the safety analysis program and should include:

- identification of sections to be revised due to:
  - changes to initiating events
  - changes to the facility equipment or procedures
  - extension of the facility operating life

    - changes to regulatory requirements
    - new knowledge from research or operating experience
    - aging of SSCs
- performance of analysis
- independent review
- documents and records in the SAR

Items of safety analysis may be performed at various times, for a variety of reasons. Normal practice is that any updated safety analysis performed in mid-cycle is included with the next scheduled update of the SAR.

6. Validation and Verification of Safety Analysis Tools

Guidance

The safety analysis tools should be validated and verified. For more information, see:

- REGDOC-3.5.3, *Regulatory Fundamentals* [2]
- CSA N286-12, *Management System Requirements for Nuclear Facilities* [5]
- CSA N292.0, *General Principles for the Management of Radioactive Waste and Irradiated Fuel* [17]
- CSA N292.1, *Wet Storage of Irradiated Fuel and Other Radioactive Materials* [7]
- CSA N292.2, *Interim Dry Storage of Irradiated Fuel* [18]

7. Graded Approach

Guidance

For information on the CNSC's risk-informed graded approach, see REGDOC-3.5.3, *Regulatory Fundamentals* [2].

Class IB nuclear facilities have risk profiles that vary significantly, depending on the particular characteristics of the activity or facility. The licensee may propose, with adequate justification, specific design measures, analyses or other measures that are commensurate with the level of risks.

Some examples of elements of the safety analysis that may be considered using the graded approach include:

- frequency boundaries for facility states (AOO, DBA and DEC)
- rigour of validation and verification of safety analysis tools
- rigour of uncertainty evaluation
- extent of sensitivity studies
- quantity and quality of supporting evidence for analysis

Appendix A: Sample Structure and Content for a Safety Analysis Report

This appendix provides a sample structure for an SAR. The licensee is under no obligation to follow this format; however, as described in sections 2 through 5 of this regulatory document, the report shall include all information as applicable.

Table of contents

Chapter 1: Introduction

Chapter 2: General facility description

- applicable regulations, codes and standards
- basic technical characteristics
- facility layout
- operating modes
- additional referenced analyses
- a summary of significant modifications or changes to the site or facility since the previous safety analysis report, including modifications to any facility buildings, processes, equipment, procedures, programs or organizational structure

Chapter 3: Management of safety

- organizational structure
- operational management philosophy
- safety culture
- quality assurance
- monitoring and review of safety performance

Chapter 4: Site evaluation

- site reference data (area under the control of the licensee and the surrounding area)
- hydrology
- hydrogeological characteristics
- meteorology
- seismology
- present and projected surrounding population distribution
- present and projected surrounding land use
- evaluation of site-specific hazards
- proximity of industrial, transport and military facilities
- activities at the facility site that may influence the facility's safety
- radiological conditions due to external sources
- site-related issues in emergency planning and accident management
- monitoring of site-related parameters

Chapter 5: General design aspects

- safety objectives, design principles and criteria
- conformance with design principles and criteria
- classification of SSCs
- civil engineering aspects of facility design
- equipment qualification and environmental factors
- human performance program
- protection against internal and external hazards

Chapter 6: Description of facility systems and components

- nuclear systems and components
- non-nuclear systems and components
- instrumentation and control
- electrical systems
- auxiliary systems
- fire protection systems
- radioactive waste treatment system
- other SSCs important to safety

Chapter 7: Safety analyses

- safety objectives and acceptance criteria
- identification and classification of PIEs
- human actions
- deterministic approach
- probabilistic approach
- summary of results of the safety analyses

Chapter 8: Commissioning (for new facilities)

Chapter 9: Operational aspects

- organization
- administrative procedures
- operating procedures
- emergency operating procedures
- guidelines for accident management
- maintenance, surveillance, inspection and testing
- management of aging
- control of modifications
- qualification and training of personnel
- human factors
- feedback of operational experience
- documents and records

Chapter 10: Operational limits and conditions

Chapter 11: Radiation protection

- application of the ALARA principle
- sources of radiation
- design features for radiation protection
- radiation monitoring
- radiation protection program

Chapter 12: Emergency preparedness

- emergency management
- emergency response facilities
- fire protection program

Chapter 13: Environmental aspects associated with credible abnormal events (such as spills)

- radiological effects
- non-radiological effects

Chapter 14: Radioactive waste management

- control of waste
- handling of radioactive waste
- minimizing the accumulation of waste
- conditioning of waste
- storage of waste
- disposal of waste

Chapter 15: Decommissioning and end-of-life aspects

- decommissioning plan
- financial guarantee

Chapter 16: Public information program

Appendix B: Sample Parameters for Operational Limits and Conditions

This appendix provides some examples of limiting conditions for safe operation of the facility, applying requirements for:

- nuclear substances (type, chemical and physical form, maximum capacity in the facility, isotopic composition)
- associated hazardous substances (such as chemicals) inside the facility and its equipment
- minimum availability requirements for:
  - SSCs important to safety
  - requirements on testing values of the SSCs

  Note: In some cases, OLCs relating to the availability of SSCs may include requirements for their testing, including:
    - initial and periodic tests
    - type of tests
    - verification
    - calibration or inspection
    - required intervals for inspections
    - time between 2 successive tests

- means of confinement:
  - air flows (and where appropriate, temperatures and humidity) within the facility and its processes
  - target pressure drops across filters
  - pressures within the facility buildings (rooms, cells or boxes as appropriate) relative to the atmosphere (under normal and emergency conditions)
  - isolation of means of confinement and starting of emergency ventilation
  - operations that require confinement
  - configuration and minimum equipment for ventilation system
  - leak rate from the means of confinement
  - efficiency of filters

- radiation protection and management of radioactive waste:
  - alarm setting for criticality alarm systems and for radiation detection and monitoring instrumentation and equipment
  - limits on the airborne concentration of nuclear substances
  - radiation exposure control levels for operation, including radiation dose action levels
  - limits for controlling surface contamination
  - storage capacity for liquid and solid nuclear waste
- material handling, including requirements for:
  - movements of nuclear and associated hazardous substances, including onsite transfer and offsite transportation
  - material handling tools and equipment, including cranes (maximum allowable loads and testing requirements)

    - storage containers
- electrical systems, including requirements for:
    - emergency power supply
    - testing frequency
    - availability and reliability of uninterruptable power supply and diesel generators
- other systems; some examples are:
    - fire protection systems
    - process auxiliaries
    - communications systems
    - emergency lighting systems
- monitoring system and associated alarm settings:
    - values of the settings for instrumentation in the facility
    - values of the settings for process equipment necessary for safety
- administrative requirements:
    - staffing (for example, minimum staffing and hours of work)
    - prerequisites for activities important to safety (such as transport of radioactive or fissile material, both onsite and offsite)

Appendix C: Postulated Initiating Events

This appendix describes the types of PIEs and the ranges of conditions to be considered for applicability at Class IB nuclear facilities.

C.1 Selected postulated initiating events

Some examples of PIEs are:

1. incorrect specification of incoming and transferred material
2. loss of services
   - loss of electrical power
   - loss of compressed air
   - loss of inert atmosphere
   - loss of coolant
   - loss of ultimate heat sink
3. loss of criticality safety controls
   - drop of fuel during handling
   - loss of geometry
   - flooding
   - loss of neutron poison
   - excess reflection or moderation
   - unintentional change of phase
   - failure or collapse of structural components
   - maintenance error
   - control system error
   - over (double) batching
4. processing errors
   - incorrect facility configuration
   - insufficient reagent or coolant, added too fast or too early
   - incorrect pressure or gas flow, rupture
   - incorrect or extreme temperature
   - unexpected phase changes leading to criticality or loss of confinement
   - function required for safety not applied
   - safety function applied too late
5. facility and equipment failures
   - failure of confinement or leak
   - inadequate isolation of process fluids
   - blockage or bypass of filter or column
   - spurious actuation of an SSC important to safety
   - structural failures
6. handling errors
   - hazardous load dropped
   - heavy load dropped on SSC(s) important to safety
   - safety interlocks failure on demand
   - brakes, overspeed or overload protection inadequate

- obstructed pathway leading to collision
- failure of lifting component (for example, hook, beam or cable)
- load fixed to floor

7. special internal events
   - internal fires or explosions
   - internal flooding (for example, from sprinkler systems or other water pipes)
   - malfunction in experiment
   - improper access by persons to restricted areas
   - criticality event
   - fluid jets, pipe whip, internal missiles
   - exothermic chemical reaction
   - ignition of accumulated combustible gases (for example, hydrogen)
   - failure due to corrosion
   - loss of neutron absorption
   - accidents on internal transport routes (including collisions into the facility building)
8. external events
   - external fires or explosions
   - earthquakes (including seismically induced faulting and landslides)
   - flooding (including failure of an upstream/downstream dam, blockage of a river, or damage due to storm surges or high waves)
   - tornados and tornado missiles
   - extreme meteorological phenomena (including precipitation, sandstorms, hurricanes, storms and lightning)
   - aircraft crashes
   - toxic spills
   - effects from adjacent facilities (for example, nuclear facilities, chemical facilities and waste management facilities)
   - biological hazards such as microbial corrosion, structural damage or damage to equipment by rodents or insects
   - power or voltage surges on the external supply line
9. human errors
   - worker error or omission
   - maintenance error or omission

C.2 Range of selected events to be considered for applicability

The following classification and ranges of internal events are to be considered for applicability:

- **anticipated operational occurrence (AOO):** an event with a likelihood of occurrence that is greater than 10^{-2} per year
- **design-basis accident (DBA):** an event with a likelihood of occurrence that is less than 10^{-2} per year and greater than 10^{-5} per year
- **design extension conditions (DEC):** an event with a likelihood of occurrence that is less than 10^{-5} per year and greater than 10^{-6} per year

The following ranges of selected external events are to be considered for applicability.

Wind and tornado loading

For assessment of a design-basis accident (DBA):
The potential for the occurrence of tornadoes in the region of interest shall be assessed on the basis of detailed historical and instrumentally recorded data for the region. For example, wind design for an existing facility if prescribed by an applicable building code would have an annual exceedance probability of greater than or equal to 2×10^{-2}. For more information, see the United States Nuclear Regulatory Commission's *Standard Review Plan for Fuel Cycle Facilities License Applications (NUREG-1520)* [19].

For assessment of design extension conditions (DEC):
Depending on the geographical location of the facility, the effects of a tornado with an annual exceedance probability of 10^{-5} or greater may need to be considered if a potential exists at the facility for offsite consequences of DEC that may lead to offsite emergency mitigation measures.

Flooding hazards

For assessment of DBA:
Existing facilities are generally to be sited above the 100-year flood plain.

For assessment of DEC:
Maximum probable flood plain should be used if a potential exists at the facility for offsite consequences of DEC that may lead to offsite emergency mitigation measures.

Seismic hazards

Near regional studies should include a geographical area typically not less than 25 km in radius. Site vicinity studies should cover a geographical area typically not less than 5 km in radius. Site area studies should include the entire area covered by the facility. For more information, see IAEA Specific Safety Guide SSG-9, *Seismic Hazards in Site Evaluation for Nuclear Installations* [20].

Information on prehistorical, historical and instrumentally recorded earthquakes in the region should be collected and documented. For more information, see IAEA Safety Standard No. NS-R-3 (Rev. 1), *Site Evaluation for Nuclear Installations* [21].

For assessment of DBA:
Structures at existing nuclear fuel cycle facilities are built to a building code. Guidance in CSA N289.5, *Seismic Instrumentation Requirements for Nuclear Power Plants and Nuclear Facilities* [22], should be used if a potential exists at the facility for offsite consequences of DBA that may lead to offsite emergency mitigation measures.

For assessment of DEC:
CSA N289.5, *Seismic Instrumentation Requirements for Nuclear Power Plants and Nuclear Facilities* [22], provides guidance that includes meeting a design-basis earthquake having an exceedance probability of 10^{-3} per year to less than 10^{-4} per year. CSA N289.5 [22] should be used if a potential exists at the facility for offsite consequences of DEC that may lead to offsite emergency mitigation measures.

Aircraft crashes

The potential for aircraft crashes, including impacts, fires and explosions onsite, should be considered with account taken of:

- the foreseeable characteristics of air traffic, the locations and types of airports
- the characteristics of aircraft, including those with special permission to fly over or near the facility, such as firefighting aircraft and helicopters

For more information, see IAEA Safety Standard No. NS-R-3 (Rev. 1), *Site Evaluation for Nuclear Installations* [21].

For assessment of both DBA and DEC:
The potential hazards arising from aircraft crashes are taken into account if:

- airways or airport approaches pass within 4 km of the site
- airports are located within 10 km of the site for all but the biggest airports
- for large airports, the distance (d) in kilometers to the proposed site is less than 16 km and the number of projected yearly flight operations is greater than $500d^2$

Where the distance (d) is greater than 16 km, the hazard is considered if the number of projected yearly flight operations is greater than $1000d^2$.

For military installations or air space usage such as practice bombing or firing ranges, which might pose a hazard to the site, the hazard is considered if there are such installations within 30 km of the proposed site.

For more information, see IAEA Safety Guide NS-G-3.1, *External Human Induced Events in Site Evaluation for Nuclear Power Plants* [23].

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. Canadian Nuclear Safety Commission (CNSC), REGDOC-2.11.1, *Waste Management, Volume III: Safety Case for the Disposal of Radioactive Waste*, Ottawa, Canada.

2. CNSC, REGDOC-3.5.3, *Regulatory Fundamentals*, Ottawa, Canada.

3. International Atomic Energy Agency (IAEA), Specific Safety Requirements No. SSR-4, *Safety of Nuclear Fuel Cycle Facilities*, Vienna, Austria, 2017.

4. CNSC, REGDOC-3.6, *Glossary of CNSC Terminology*, Ottawa, Canada.

5. CSA Group, CSA N286-12, *Management System Requirements for Nuclear Facilities*, reaffirmed in 2017.

6. IAEA, Safety Guide No. GS-G-3.5, *The Management System for Nuclear Installations*, Vienna, Austria, 2009.

7. CSA Group, CSA N292.1, *Wet Storage of Irradiated Fuel and Other Radioactive Materials*, 2016.

8. CNSC, REGDOC-2.5.2, *Design of Reactor Facilities*, Ottawa, Canada.

9. CSA Group, CSA N286.7-16, *Quality Assurance of Analytical, Scientific and Design Computer Programs*, 2016.

10. IAEA, Safety Guide No. SSG-5, *Safety of Conversion Facilities and Uranium Enrichment Facilities*, Vienna, Austria, 2010.

11. IAEA, Safety Guide No. SSG-6, *Safety of Uranium Fuel Fabrication Facilities*, Vienna, Austria, 2010.

12. IAEA, TECDOC No. 1267, *Procedures for Conducting Probabilistic Safety Assessment for Non-Reactor Nuclear Facilities*, Vienna, Austria, 2002.

13. CNSC, REGDOC-2.2.5, *Minimum Staff Complement*, Ottawa, Canada.

14. CNSC, REGDOC-2.4.3, *Nuclear Criticality Safety*, Ottawa, Canada.

15. Health Canada, H46-2/03-326E, *Canadian Guidelines for Intervention During a Nuclear Emergency*, Ottawa, Canada, 2003.

16. IAEA, General Safety Requirements No. GSR Part 7, *Preparedness and Response for a Nuclear or Radiological Emergency*, Vienna, Austria, 2015.

17. CSA Group, CSA N292.0, *General Principles for the Management of Radioactive Waste and Irradiated Fuel*, 2019.

18. CSA Group, CSA N292.2, *Interim Dry Storage of Irradiated Fuel*, 2013 (reaffirmed in 2018).

19. United States Nuclear Regulatory Commission (NUREG), *Standard Review Plan for Fuel Cycle Facilities License Applications (NUREG-1520)*, Revision 2, 2015.

20. IAEA, Specific Safety Guide SSG-9, *Seismic Hazards in Site Evaluation for Nuclear Installations*, Vienna, Austria, 2010.

21. IAEA, Safety Standard No. NS-R-3 (Rev. 1), *Site Evaluation for Nuclear Installations*, Vienna, Austria, 2016.

22. CSA Group, CSA N289.5, *Seismic Instrumentation Requirements for Nuclear Power Plants and Nuclear Facilities*, reaffirmed in 2017.

23. IAEA, Safety Guide NS-G-3.1, *External Human Induced Events in Site Evaluation for Nuclear Power Plants*, Vienna, Austria, 2002.

Additional Information

The CNSC may recommend additional 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".

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

- CSA Group, CSA N291, *Requirements for Nuclear Safety-Related Structures*, 2019.
- International Atomic Energy Agency (IAEA), General Safety Requirements GSR Part 4 (Rev. 1), *Safety Assessment for Facilities and Activities*, Vienna, Austria, 2016.
- IAEA Safety Guide GS-G-4.1, *Format and Content of the Safety Analysis Report for Nuclear Power Plants*, Vienna, Austria, 2004.
- United States Nuclear Regulatory Commission(U.S. NRC), *Integrated Safety Analysis Guidance Document (NUREG-1513)*, 2001.

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.