Canada's Nuclear Regulator

CNSC CCSN

Guidance on Safety Analysis for Nuclear Power Plants

GD-310

Canadian Nuclear Safety Commission

Commission canadienne de sûreté nucléaire

Canada

Guidance on Safety Analysis for Nuclear Power Plants
Guidance Document GD-310

© Minister of Public Works and Government Services Canada 2012
Catalogue number: CC172-85/2012E-PDF
ISBN 978-1-100-20451-2

Published by the Canadian Nuclear Safety Commission

Également publié en français sous le titre de **:** *Document d'orientation sur les analyses de la sûreté pour les centrales nucléaires*

Document availability

This document can be viewed on the Canadian Nuclear Safety Commission Web site at nuclearsafety.gc.ca

To order a printed 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
Web site: nuclearsafety.gc.ca

Publishing history:

March 2012	Version 1.0
June 2011	Draft for Public Consultation

Preface

Guidance document GD-310, *Guidance on Safety Analysis for Nuclear Power Plants*, provides information on how the requirements in regulatory document RD-310, *Safety Analysis for Nuclear Power Plants*, may be met. The CNSC expects proponents and applicants for new reactor licences to apply the provisions of regulatory document RD-310 in their submissions for building a new nuclear power plant. In the context of existing reactors, CNSC expects the licensees to apply the provisions of RD-310, in a graduated manner, to all relevant programs in future submissions.

To the extent practicable, the guidance provided in this document is technology-neutral with respect to water-cooled reactors. It includes criteria to ensure that deterministic safety analysis reports clearly demonstrate the safety of the nuclear power plant. This guidance document provides information on preparing and presenting deterministic safety analysis reports, including the selection of events to be analyzed, acceptance criteria, safety analysis methods, safety analysis documentation, and the review and update of safety analysis.

This document provides guidance on a risk-informed approach to the categorization of accidents. This approach considers a full spectrum of possible events, including the events of greatest potential consequence to the public.

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

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

Table of Contents

Guidance on Safety Analysis for Nuclear Power Plants

1. Purpose

This guidance document clarifies the regulatory requirements of RD-310, *Safety Analysis for Nuclear Power Plants*. It provides information to ensure that adequate deterministic safety analyses are completed in order to demonstrate the safety of the nuclear facility. This information facilitates the conduct, review and approval of deterministic safety analyses.

2. Scope

This document provides information on the preparation and presentation of deterministic safety analysis reports, including the selection of events to be analyzed, acceptance criteria, safety analysis methods, safety analysis documentation, and the review and update of safety analysis.

GD-310 focuses on deterministic safety analysis. Probabilistic safety assessment is addressed in the regulatory standard document S-294, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*.

Regulatory requirements and guidance related to the safe handling of fissionable materials outside the reactor core are provided in the regulatory document RD-327, *Nuclear Criticality Safety*, and its associated guidance document GD-327, *Guidance for Nuclear Criticality Safety*.

3. Relevant Legislation

Relevant sections of the *Nuclear Safety and Control Act* (NSCA) and sections of its associated regulations to this guidance document include:

- subsection 24(4) of the NSCA, which provides that "the Commission may only issue, renew or amend licences if the licensee or the applicant: (*a*) is qualified to carry on the activity that the licence authorizes the licensee to carry on; and (*b*) in carrying out that activity, makes 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, which authorizes the Commission to "include in a licence any term or condition that the Commission considers necessary for the purposes of the Act"
- paragraph 3(1)(*i*) of the *General Nuclear Safety and Control Regulations*, which 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"
- paragraph 5(*f*) of the *Class I Nuclear Facilities Regulations*, which 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"
- paragraph 5(*i*) of the *Class I Nuclear Facilities Regulations*, which 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…"

- paragraph 6(*c*) of the *Class I Nuclear Facilities Regulations*, which 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"
- paragraph 6(*h*) of the *Class I Nuclear Facilities Regulations*, which 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…"
- paragraph 7(*f*) of the *Class I Nuclear Facilities Regulations*, which 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. Safety Analysis Objectives

Safety assessments are systematic processes to verify that applicable safety requirements are met in all the lifecycle phases of a nuclear power plant (NPP). These assessments are performed for various aspects of safety, security and safeguards (such as management practices, quality assurance, human performance, safety culture, training, design adequacy, safety analysis, equipment fitness for service, emergency preparedness, environmental protection, and radiation protection).

A safety assessment includes the performance of a safety analysis, which is an analytical quantitative study performed mainly to demonstrate the safety of a nuclear power plant and the adequacy of its design and performance. Deterministic safety analysis, probabilistic safety assessment (PSA) and hazards analysis are three types of safety analyses.

PSA considers the likelihood and consequences of various plant transients and accidents. The primary objectives of the PSA are to help with:

- identifying the sequences of events and their probabilities, which lead to challenges to fundamental safety functions, loss of integrity of key structures, release of radionuclides into the environment and public health effects
- developing a well balanced NPP design
- assessing the impact of changes to procedures and/or components on the likelihood of core damage

For new NPPs, PSAs support deterministic safety analysis in identifying complementary design features for severe accidents, or actions that operators can take during severe accidents to reduce risk. Requirements for probabilistic safety assessment for NPPs are provided in regulatory standard S-294, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*. Probabilistic safety assessments complement the deterministic safety assessments.

A hazards analysis (such as fire hazard assessment, or seismic margin assessment) will demonstrate the ability of the design to effectively respond to credible common-cause events. This analysis is meant to confirm that the NPP design incorporates sufficient diversity and physical separation to cope with credible common-cause events. It also confirms that credited structures, systems and components (SSCs) are qualified to survive and function during credible common-cause events, as applicable.

This document focuses on deterministic safety analysis. PSA and hazard analysis are outside the scope of this document.

4.1 Roles of deterministic safety analysis

The deterministic safety analysis confirms that the design is capable of meeting the safety analysis requirements listed in RD-310, as well as dose acceptance criteria. It also helps demonstrate that safety goals are met, that the design reflects effective defence in depth, and that the plant design and operation are acceptable and robust.

Deterministic safety analysis is used to analyze the behaviour of a plant following a postulated failure of equipment, internal or external event, or operator error. For the analyzed event, the deterministic safety analysis allows prediction and quantification of challenges to the plant's physical barriers, and the performance of plant systems (particularly safety systems), in order to predict failures of barriers to radioactivity releases.

Deterministic safety analysis methods can be applied to a wide range of plant operating modes and events, including normal operation and abnormal operation resulting from equipment failure, operator errors and challenges arising from events like fires, floods or earthquakes.

4.2 Objectives of deterministic safety analysis

1. **Confirm that the design of a nuclear power plant meets design and safety analysis requirements**

   This can be achieved by:

   - demonstrating that the plant as built can operate safely, taking the effect of aging into consideration
   - demonstrating that the design can withstand and effectively respond to identified postulated initiating events (PIEs)
   - demonstrating that the applicable expectations for defence in depth established in RD 337, *Design of New Nuclear Power Plants*, are met
   - predicting expected harsh environmental conditions due to anticipated operational occurrences (AOOs), design basis accidents (DBAs) and beyond design basis accidents (BDBAs), including severe accidents
   - demonstrating that the provisions for protection against severe accidents are adequate (e.g., performance expectations for containment, biological shielding and re-criticality)

2. **Derive or confirm operational limits and conditions that are consistent with the design and safety requirements for the NPP**

   Guidance for this section can be found in CSA N290.15-10, *Requirements for the Safe Operating Envelope of Nuclear Power Plants*, including:

   - safety limits for reactor protection and control
   - safety limits for engineered safety systems
   - operational limits and reference settings for the control systems
   - procedural constraints for operational control of processes
   - identification of the allowable operating configurations

3. **Assist in establishing and validating accident management procedures and guidelines**

   Severe accident management guidelines (SAMG) is an example.

4. **Assist in demonstrating that safety goals - which may be established to limit the risks posed by the nuclear power plant - are met**

   For details see section 5.3.3.

Deterministic safety analyses are also performed to:

- assist in confirming or validating the strategies that have been selected to recover the plant from an AOO or DBA
- assist in developing a strategy for the operator to follow, should the automatic actions and emergency operating procedures fail to prevent a severe accident
- confirm that modifications to the design and operation of the NPP have no significant adverse effects on safety
- understand operational transients and plant system response
- predict source term and doses during severe accidents
- support emergency programs

4.3 Deterministic safety analysis in confirmation of defence in depth

The application of the concept of defence in depth to the design of an NPP should be confirmed, so the design will provide layers of overlapping provisions, such that any failure would be compensated for - or corrected - without causing harm to individuals or the public. Deterministic safety analysis is an important part of this confirmation.

Five levels of defence in depth are defined in RD-337, *Design of New Nuclear Power Plants*. The applicability of deterministic 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).

Good design and proven engineering practices are used to support first-level of defence in depth.

Level 2: The aim of the second-level of defence is to detect and intercept deviations from normal operation in order to prevent AOOs from escalating to accident conditions, and to return the plant to a state of normal operation.

To support second-level defence in depth, AOOs are analyzed to demonstrate the robustness of the control systems in arresting most AOOs and in preventing damage to all SSCs that are not involved in the initiation of an AOO, to the extent that these SSCs will remain operable following the AOO.

Level 3: The aim of the third-level of defence is to minimize the consequences of accidents by providing inherent safety features, fail-safe design, additional equipment, and mitigating procedures.

To support third-level defence in depth, DBAs (including AOOs with failed second-level defences) are analyzed to demonstrate the capabilities of the safety systems to mitigate any resulting radiological consequences, i.e., to demonstrate meeting the prescribed dose limits for DBAs (and AOOs with failed second-level defences) and related derived acceptance criteria for protecting fission product release barriers. AOOs and DBAs are also analyzed to assist in developing emergency operating procedures that define actions that should be taken during these events.

Note that the event combination of AOO plus independent failure of level-2 defence in depth should be considered a DBA, and the dose limit applicable to DBAs should apply.

Level 4: The aim of the fourth-level of defence is to ensure that radioactive releases caused by severe accidents are kept as low as practicable.

Level 5: The aim of the fifth-level of defence is to mitigate the radiological consequences of potential releases of radioactive materials that may result from accident conditions.

In support of fourth and fifth-level defence in depth, BDBAs are analyzed. This analysis is to provide information in support of design and safety of NPPs related to severe accidents, such as performance of complementary design features for severe accidents, or actions that operators should take during severe accidents, in order to mitigate the consequences. The analysis also assists in the development of severe accident management guidelines.

5. Guidance on Safety Analysis Requirements

5.1 Responsibilities

As per RD-310, the licensee must maintain adequate capability to perform or procure safety analysis in order to:

- resolve technical issues that arise over the life of the plant
- ensure the safety analysis requirements are met for the safety analysis developed by the operating organization or procured from a third party

A formal process should be established to assess and update the safety analysis to ensure that the safety analysis reflects:

- current plant configuration (for existing plants)
- current operating limits and conditions (for existing plants)
- operating experience, including the experience from similar facilities
- results available from experimental research, improved theoretical understanding or new modelling capabilities to assess potential impacts on the conclusions of safety analyses
- human factors considerations, to ensure that credible estimates of human performance are used in the analysis

5.2 Events to be analyzed

5.2.1 Identifying events

The safety analysis is performed for a set of events that could lead to challenges related to the NPP’s safety or control functions. These include events caused by SSC failures or human error, as well as human-induced or natural common-cause events.

The events considered in safety analysis could be single PIEs, sequences of several consequential events, or combinations of independent events.

The set of events to be considered in safety analysis is identified using a systematic process and by taking into account:

- reviews of the plant design using such methods as hazard and operability analysis, failure mode and effects analysis, and master logic diagrams
- lists of events developed for safety analysis of other NPPs, as applicable
- analysis of operating experience data for similar plants
- any events prescribed for inclusion in safety analysis by regulatory requirements (e.g., RD-337, *Design of New Nuclear Power Plants*)
- equipment failures, human errors and common-cause events identified iteratively with PSA
- the cut-off frequency for common-cause events is consistent across all events

The list of identified events should be iteratively reviewed for accuracy and completeness as the plant design and safety analyses proceed. Reviews should also be periodically conducted throughout the NPP lifecycle, to account for new information and requirements.

RD-310 requires that, when identifying events, all permissible plant operating modes be considered. All operating modes used for extended periods of time should be analyzed. Modes that occur transiently or briefly can be addressed without a specific analysis, as long as it can be shown that existing safety analyses bound the behaviour and consequences of those states.

NPP operating modes include, but are not limited to:

- initial approach to reactor criticality
- reactor start-up from shutdown through criticality to power
- steady-state power operation, including both full and low power
- changes in the reactor power level, including load follow modes (if employed)
- reactor shutting down from power operation
- shutdown in a hot standby mode
- shutdown in a cold shutdown mode
- shutdown in a refuelling mode or maintenance mode that opens major closures in the reactor coolant pressure boundary
- shutdown in other modes or plant configurations with unique temperature, pressure or coolant inventory conditions
- operation of limited duration, with some systems important to safety being unavailable

For events identified by the systematic process used for this purpose, a full range of configurations and operating modes of equipment should be considered in the deterministic safety analysis.

Special plant configurations may occur during major plant modifications such as plant refurbishment, lay up, or decommissioning. These configurations should be considered, and potential events should be identified and included in the deterministic safety analysis.

5.2.2 Scope of events

As stated in RD-310, the list of events developed for the deterministic safety analysis includes normal operation and all credible events initiated by failures or malfunctions of plant SSCs, operator errors, and common-cause events initiated internally or externally.

5.2.2.1 Normal operation

During the design phase, the normal plant operation is analyzed as a separate class of event. This allows sources of radiation or releases of radioactive materials to be assessed in various modes of operation or transition between modes.

For an existing plant, a safety analysis for normal operation may be required if a new operational mode is considered, or if significant design changes (any changes that may alter system characteristics) are implemented.

5.2.2.2 Failures or malfunctions of structures, systems and components

SSC failures may include failure to operate when required, erroneous operation and partial failures. Events to be considered include:

- failures or malfunctions of active systems, such as pumps, valves, control systems or power supply
- failures of passive systems, such as breaks in the reactor's pressure-retaining boundaries, including pipes and rupture discs

5.2.2.3 Operator errors

As initiating events, operator errors normally produce the same results as events caused by equipment failure. Therefore, they do not need to be considered separately in the models and computer codes for deterministic safety analysis. However, the generic implications of human errors as initiating events should be considered to identify any further potential system failures. As such, if a specific operator error could result in a unique initiating event, it should be included in the list of PIEs for the deterministic safety analysis.

5.2.2.4 Internally and externally initiated common-cause events

Common-cause events are multiple component failures that can be initiated by internal and external events (these events could be human-induced or naturally occurring).

Internal common-cause events include fires, floods of internal origin, explosions, and equipment failures (such as turbine breakup) that may generate missiles.

External, naturally occurring events (triggers for plant equipment failures) that are considered in deterministic safety analysis include:

- earthquakes
- external fires
- floods/tsunamis occurring outside the site
- biological hazards (for instance, mussels or seaweed affecting cooling water flow and/or temperature)
- extreme weather conditions (temperature, precipitation, high winds, tornadoes etc.)

External initiating events may cause internal and/or external events. For example, an earthquake could lead to plant equipment failures, loss of offsite power, flood, tsunami or fire. External events may cause accidents in one or more of the units of a multi-unit station.

Human-induced external events that are considered in deterministic safety analysis include:

- aircraft or missile impacts
- explosions at nearby industrial facilities or transportation systems
- release of toxic or corrosive chemicals from nearby industrial facilities or transportation systems
- electromagnetic interference

5.2.2.5 Combinations of events

Combinations of events (which may occur either simultaneously or sequentially while restoring the plant to a stable state) should be considered.

Types of combinations include:

- multiple independent failures in equipment important to safety
- failure of a process system and system important to safety
- multiple process system failures
- equipment failures and operator errors
- common-cause events and operator errors

Examples of event combinations include:

- loss of coolant with subsequent loss of station electrical power, including station blackout
- loss of coolant with loss of containment cooling
- small loss of coolant accidents (LOCA) with failure of primary or secondary depressurization
- main steam line break with failure of the operator to initiate a backup cooling system

5.2.2.6 Grouping of events

Many events will be identified by following the aforementioned guidance, although it may not be practical or necessary to analyze all of these events. The identified events could be grouped into categories based on similarity of the initiating failures, key phenomena, or system and operator responses. Examples of event categories include decrease of the reactor coolant inventory, reactivity and power anomalies, and increase/decrease of heat removal. Since plant responses to an event depend on the design and availability of plant systems, the most suitable classification of events may vary.

In the safety analysis of AOOs and DBAs for level-3 defence in depth, bounding events should be identified for each applicable acceptance criterion within each category of events. In some cases, one accident scenario in the same category of events may be more severe in terms of one acceptance criterion (for example, containment pressure limit) and another may be more severe in terms of a different acceptance criterion (for example, public doses). All these scenarios should be considered in the safety analysis process as bounding events for different acceptance criteria.

5.2.2.7 Subdivision of events

An event may be divided into sub-events for consideration in safety analysis, when there are substantial differences between the subdivided events, such as:

- phenomena occurring at the plant in response to the events
- challenges to safety and systems important to safety
- frequencies

For example, LOCAs are commonly sub-divided into small break LOCAs and large break LOCAs due to significant differences in phenomena and challenges to the safety system.

An event should not be sub-divided without sufficient justification, for the purpose of reclassifying one of the resulting sub-events from an AOO to a DBA, or from a DBA to a BDBA, or for the purpose of attaining a frequency below the cut-off frequency limits used in PSA.

5.2.2.8 Cut-off frequency

When beginning to identify events, both those of low frequency (including earthquakes with consequential tsunamis) and those of minor consequences should be included. In defining the scope of events to be analyzed, the deterministic safety analysis should select the same cut-off frequency as that used in the probabilistic analysis for the same facility. This frequency is chosen so the deterministic analysis can be integrated with the probabilistic analysis.

Some events may be excluded from the detailed consideration (for example, because of their negligible contribution to exceeding the safety goals, or because they are bounded by an analyzed event). Such exclusion should be fully justified and the reasons well documented.

5.2.3 Classification of events

Events are classified because each plant state has different safety analysis requirements and acceptance criteria. Safety analysis requirements reflect the level of protection in accordance with the principle of defence in depth. The normal plant states and accident conditions are considered in the safety analysis. As stated in RD-310, events are classified as follows:

- **anticipated operational occurrences (AOOs) – all events with frequencies of occurrence equal to or greater than 10^{-2} per reactor year**
    - events that are more complex than the normal operation manoeuvres, with the potential to challenge the safety of the reactor, and which might be reasonably expected to happen during the lifetime of a plant

- **design basis accidents (DBAs) – events with frequencies of occurrence equal to or greater than 10^{-5} per reactor year, but less than 10^{-2} per reactor year**
    - events that are not expected to occur during the lifetime of a plant but, in accordance with the principle of defence in depth, are considered in the design of the nuclear power plant; however, certain groups of events with lower frequency may also be included in the plant design basis

- **beyond design basis accidents (BDBAs) – events with frequencies of occurrence less than 10^{-5} per reactor year**
    - events with low probabilities of expected occurrence, which may be more severe than DBAs, and — due to multiple failures and/or operator errors — may result in safety systems that fail to perform their safety functions, leading to significant core damage,

challenges to the integrity of the containment barrier, and, eventually, to the release of radioactive material from the plant

While the assessed frequency of occurrence is the basis for event classification, it is recognized that such assessments may be characterized by significant uncertainty. Therefore, an event with a predicted frequency that is on the threshold between two classes of events, or with substantial uncertainty in the predicted event frequency, is classified into the higher frequency class.

Other factors may affect the selection of certain events for inclusion. In order to establish an understanding of margins of safety or the robustness of the design, the regulatory authority may request that certain events be analyzed as design basis accidents, or as representative severe accidents. Past practices and experience may indicate that certain scenarios are more critical and should be analyzed as DBAs.

Some plant operating modes may be used only for short periods of time. Normally, events are classified without regard to the frequency of these operating modes. However, in classifying events, frequency of operating modes may be considered on a case-by-case basis.

Examples of events of different classes based on CANDU experience are provided in Appendix A. These illustrate possible outputs of the event identification and classification process described in subsection 5.2. This list is for illustration only, and is not meant to be comprehensive. It should be noted that, in practice, such a list would normally be generated by probabilistic methods. The list will be subject to grouping of events (see subsection 5.2.2.6). It is expected that only representative or bounding events for each group of events would be analyzed.

5.2.3.1 Anticipated operational occurrences

Plant design is expected to be sufficiently robust, such that most AOOs would not require the initiation of safety systems to prevent consequential damage to the plant's SSCs. This is part of level 2 defence in depth, and helps to ensure that events requiring use of safety systems are minimized. The plant control systems are expected to compensate for the event's effects and to maintain the plant in a stable state long enough for an operator to intervene. The operator intervention may include, if deemed necessary, activation of safety systems and plant shutdown according to established procedures. After addressing the initiating event, it should be possible to resume plant operations.

For level-3 defence in depth, in addition to meeting the above expectations for level-2 defence in depth, the design is also expected to demonstrate with high confidence that safety systems can mitigate all AOOs without the assistance of plant control systems.

Examples of AOOs include those in Table 1, which provides examples for a CANDU reactor and a light water reactor (LWR). The following list in Table 1 is not exhaustive; a complete list would depend on the type of reactor and the design of the plant systems.

Table 1: Examples of anticipated operational occurrences

Event category	Anticipated operational occurrences
increase in reactor heat removal	• inadvertent opening of steam relief valves • secondary pressure control malfunctions leading to an increase in steam flow rate • feedwater system malfunctions leading to an increase in the heat removal rate
decrease in reactor heat removal	• feedwater pump trips • reduction in the steam flow rate for various reasons (e.g., control malfunctions, main steam valve closure, turbine trip, loss of external load, loss of power, loss of condenser vacuum)
changes in reactor coolant system flow rate	• trip of one main coolant pump • inadvertent isolation of one main coolant system loop (if applicable)
reactivity and power distribution anomalies	• inadvertent single control rod withdrawal • neutron poison concentration dilution due to a malfunction in the volume control system • wrong placement of a fuel assembly (LWR), or refuelling incorrect channel (CANDU)
increase in reactor coolant inventory	• malfunctions of the chemical and inventory control system
decrease in reactor coolant inventory	• very small LOCA, due to the failure of an instrument line
release of radioactive material from a subsystem or component	• minor leakage from a radioactive waste system

5.2.3.2 Design basis accidents

The events leading to design basis accidents (DBAs) are classified based on the estimated frequencies of equipment failures, operator errors or common-cause events. All the events identified as initiators of AOOs should also be considered as potential initiators for DBAs, given the relatively high likelihood of AOOs and the possibility of additional equipment failures or operator errors.

Examples of DBAs include those in Table 2, which provides examples for CANDU reactors, pressurized water reactors (PWRs) and other light water reactors (LWRs). The following list in Table 2 is not exhaustive. A complete list of DBAs would depend on the type of reactor and actual design.

Table 2: Examples of design basis accidents

Event category	Design basis accidents
increase in reactor heat removal	• steam line breaks
decrease in reactor heat removal	• feedwater line breaks
changes in reactor coolant system flow rate	• trip of more than one main coolant pump • main coolant pump seizure or shaft break • fuel channel flow blockage (CANDU)
reactivity and power distribution anomalies	• uncontrolled control rod withdrawal • control rod ejection (LWR) • boron dilution due to the start-up of an inactive loop (PWR)
increase in reactor coolant inventory	• inadvertent operaton of emergency core cooling
decrease in reactor coolant inventory	• a spectrum of possible LOCAs • inadvertent opening of the primary system relief valves • leaks of primary coolant into the secondary system
release of radioactive material from a subsystem or component	• overheating of, or damage to, used fuel in transit or storage • break in a gaseous or liquid waste treatment system

5.2.3.3 Beyond design basis accidents

Probabilistic safety assessment (PSA) allows systematic identification of event sequences leading to challenges to the fundamental safety functions. Representative event sequences are then analyzed using deterministic safety analysis techniques to assess the extent of fuel failures, damage to the reactor core, primary heat transport system and containment, and releases of radionuclides. The use of any cut-off limit for the frequency of occurrence of analyzed BDBAs should consider the safety goals established for the plant and be consistent with the safety analysis objectives.

Examples of BDBAs include:

- complete loss of the residual heat removal from the reactor core
- complete loss of electrical power for an extended period

This class of events also includes massive failures of pressure vessels. Some massive failures of pressure vessels can be exempted from the deterministic safety analysis, if it can be demonstrated that these failures are sufficiently unlikely, and if all the following conditions are satisfied:

- the vessel is designed, fabricated, installed, and operated in compliance with the nuclear requirements of the applicable engineering codes and other requirements
- an in-service inspection program is implemented

- operating experience, with vessels of similar design and operating condition, support a low likelihood of failure
- the vessel has adequate restraints to limit propagation of damage to the plant

Note: Although the CANDU heat transport system header is considered as a vessel, its failure has to be postulated in the safety analysis.

Events that have been excluded from the DBA analysis based on leak-before-break (LBB) methodology are to be considered in the BDBA sequences. For example, any large LOCA or main steam line break that may have been excluded from the design basis accident set should be considered for the BDBA analysis.

5.3 Acceptance criteria

Acceptance criteria are established to serve as thresholds of safe operation in normal operation, AOO, DBA and, to the extent practicable, for BDBA. The limits and conditions used by plant designers and operators should be supported by adequate experimental evidence, and be consistent with the safety analysis acceptance criteria as described in subsections 5.3.1 to 5.3.4.

5.3.1 Normal operation

The deterministic safety analysis for normal operation should:

- verify the set points of the safety systems, to demonstrate that their initiation would occur only when needed
- verify that process controls and alarms are effective in reducing (or avoiding) the need for safety system actions
- address all NPP conditions under which systems and equipment are operated as expected, with no internal or external challenges, including all the operational configurations for which the NPP was designed to operate in the course of normal operations over its life, both at power and at shutdown

5.3.2 Anticipated operational occurrences and design basis accidents

The aim of safety analysis for AOOs and DBAs is to demonstrate the effectiveness of the following key safety functions:

- controlling the reactor power, including shutting down the reactor and maintaining it in a shutdown state
- removing heat from the core
- preserving the integrity of fission product barriers
- preserving component fitness for service for AOOs
- ensuring that the consequences of radioactive releases are below the acceptable limits
- monitoring critical safety parameters

Acceptance criteria for AOOs and DBAs should include:

- acceptance criteria which relate to doses to the public
- derived acceptance criteria which relate to the protection of the defence in depth physical barriers (see subsection 5.3.4 and Appendix B for examples)

The committed whole-body dose for average members of the critical groups who are most at risk, at or beyond the site boundary, is calculated in the deterministic safety analysis for a period of 30 days after the analyzed event.

This dose is less than or equal to one of the following dose acceptance criteria:

- 0.5 millisievert for any AOO
- 20 millisieverts for any DBA

These dose limits apply to new NPPs (effectively those licensed after RD-337, *Design of New Nuclear Power Plants*, was issued in 2008). For existing reactors, the dose limits specified in the operating licences must be met.

To demonstrate that the radiological consequences of an analyzed event do not exceed the limits, the doses should be calculated according to the guidance in subsection 5.4.4.7.

Acceptance criteria for the class of events with higher frequencies of occurrence should be more stringent than those for the class of events with lower frequencies of occurrence.

To demonstrate compliance with the public dose acceptance criteria for an AOO, the automatic isolation and pressure suppression functions of the containment system should not be credited, since these functions are normally considered part of level-3 defence in depth. However, the containment passive barrier capability and normally operating containment subsystems could be credited, if they are qualified for the AOO conditions.

Derived acceptance criteria have two components: qualitative and quantitative. Quantitative acceptance criteria should be developed, based on direct physical evidence and well-understood phenomena, and should account for uncertainties.

Regarding the qualitative acceptance criteria (such as the examples provided in Appendix B), the following guides are applied only to AOOs:

- the qualitative acceptance criteria should be satisfied without reliance on the automatic function of the safety systems, for a wide range of AOOs. The plant control systems should normally be able to correct transients and prevent damage to the plant's SSCs
- the control systems should be able to maintain the plant in a stable operating state for a sufficiently long time, to allow the operator to diagnose the event, initiate required actions and, if necessary, shut the reactor down while following the applicable procedures
- even though control systems may be shown to maintain the plant in a safe state following an AOO without the initiation of safety systems (level-2 defence in depth), it should also be shown with high confidence, for all AOOs, that the safety systems can also mitigate the event without beneficial actions by the control systems (level-3 defence in depth)

Certain accidents with predicted frequency of occurrence less than 10^{-5} per reactor year could be used as the design basis event for a safety system. In this case, DBA dose limits shall still be met, and the analysis should also consider meeting qualitative acceptance criteria relevant to this particular safety system. The safety system performance margins should be sufficient to ensure that the DBA dose limits are met.

5.3.3 Beyond design basis accidents

RD-310 states that analysis for BDBAs shall be performed as part of the safety assessment to demonstrate that:

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

The deterministic and probabilistic safety assessment should demonstrate that the level-4 defence in depth prevents or mitigates the consequences of BDBAs (including severe accidents,) as described in RD-337. The BDBA deterministic analysis addresses a set of representative sequences, in which the safety systems have malfunctioned and some of the barriers to the release of radioactive material may have failed, or have been bypassed. The accident sequences for analysis should be relevant and representative with respect to the objective of the analysis. In other words, representative BDBAs can be selected among the dominant accident sequences from the probabilistic safety assessment, or by adding safety system failures or incorrect operator responses to the DBA sequences. In general, the results of the PSA studies can be used for this purpose, if they are applicable.

The aim of safety analysis for BDBAs is to:

- evaluate the ability of the design to withstand challenges posed by BDBA and to identify plant vulnerabilities
- assess the effectiveness of those design features which were incorporated in the plant design for the specific purpose to reduce the likelihood and/or mitigate the consequences of BDBAs, (including the assessment of equipment for accident management and instrumentation to monitor the accident)
- evaluate the ability to restore and maintain the safety functions using alternative or diverse systems, procedures and methods, including the use of non-safety-grade equipment
- assist in the development of an accident management program for BDBAs and severe accident conditions
- provide consequence data for accident sequences to use in the PSA
- provide input for offsite emergency planning

For multi-unit events, as well as for single-unit events, the capacity of essential cooling and power supplies should be evaluated.

The design for BDBAs is aimed to meet risk criteria such as safety goals related to frequency of severe core damage and significant releases of radioactivity, as assessed by PSA.

Deterministic calculations of the source terms for BDBAs can also be performed in accordance with the aim of the BDBA analysis. These calculations should demonstrate, for example, that:

- containment failure will not occur in the short term following a severe accident (see RD-337)
- the public is provided a level of protection from the consequences of nuclear power plant operation, such that there is no significant additional risk to the life and health of individuals

5.3.4 Acceptance criteria for anticipated operational occurrences and design basis accidents

In addition to the dose limits in subsection 5.3.2, the acceptance criteria for AOOs and DBAs also include a set of derived acceptance criteria, such as those examples of qualitative acceptance criteria identified in Appendix B.

These acceptance criteria are established by the designer to limit the damage to different defence barriers. Compliance with these requirements ensures that there are physical barriers preserved to limit the release of radioactive material and prevent unacceptable radiological releases following an AOO or DBA. The failure to meet a derived acceptance criterion does not necessarily mean that dose limits will be exceeded. However, if the derived acceptance criteria are met with significant margin, then the dose calculation can be simplified, because fission product releases are expected to be limited.

The derived acceptance criteria are generally more stringent for events with a higher frequency of occurrence. For example, for most AOOs, the actions of the control systems should be able to prevent consequential degradation of any of the physical barriers to the extent that the related SSCs are no longer fit for continued service (including fuel matrix, fuel sheath/fuel cladding, reactor coolant pressure boundary or containment).

More demanding requirements may be set to demonstrate the availability of a margin between the predicted value and the quantitative acceptance criteria, or to simplify an analysis (for example, to avoid having to perform complex modelling). The conditions of applicability for each additional criterion should be clearly identified.

For each of the qualitative acceptance criteria, as illustrated in Appendix B, quantitative acceptance criteria (or limits) should be established. These quantitative limits should:

- be applicable to the particular NPP system and accident scenario
- provide a clear boundary between safe states (when failure of an SSC is prevented with high confidence,) and unsafe states (when a failure of an SSC may occur)
- be supported by experimental data
- incorporate margins or safety factors to account for uncertainty in experimental data and relevant models

When there is insufficient data to identify the transition from a safe state to an unsafe state, or to develop accurate models, then the quantitative limit for the corresponding safety requirement should be set at the boundary of the available data, provided that the established limit is conservative.

5.4 Safety analysis methods and assumptions

5.4.1 General

Subsection 5.4 mainly addresses analysis methods and assumptions for the deterministic safety analysis of AOOs and DBAs for level-3 defence in depth. Similar analysis methods and assumptions can be applied for levels-2 and 4 defence in depth (with appropriate levels of conservatism). Certain conservative rules, such as the single failure criterion, are not applied in level-2 and level-4 analyses.

The safety analyst has the option of selecting safety analysis methods and assumptions, as long as the regulatory requirements and expectations are satisfied.

The selection of the safety analysis methods and assumptions should be such that the appropriate level of confidence can be achieved in the analysis results.

5.4.2 Analysis method

The basic elements included in the safety analysis method are described in subsections 5.4.2.1 to 5.4.2.9. There are three main analysis methods used in the deterministic safety analysis:

- conservative analysis method, such as the method used for level-3 defence in depth
- best estimate plus evaluation of uncertainties method, such as the method used for level-3 defence in depth
- best estimate analysis method, such as the method used for levels-2 and 4 defence in depth

The first and second methods above are considered as part of the application of conservatism in safety analysis, and are addressed in subsection 5.4.6. Evaluation of uncertainties is elaborated in section 5.4.2.7.

5.4.2.1 Identifying the scenarios to be analyzed

The scenario to be analyzed, or the analyzed event, should be defined by including descriptions of the following:

- initial conditions
- the initiating event and any additional events
- expected actions of the plant systems and of the operator, in response to the initiating event
- general description of the anticipated transient
- associated safety concerns
- long term stable state (including cold and depressurized shutdown) at the end of an event

5.4.2.2 Identifying the applicable acceptance criteria

A set of applicable criteria should be identified, including any regulatory requirements. These criteria should address all safety challenges while also demonstrating compliance with the dose acceptance criteria given in subsection 5.3.2, as well as the derived acceptance criteria adopted by the designer. In addition to these criteria, others may be defined — in order, for example, to simplify the analysis by imposing more restrictive criteria, or to allow intermediate assessments in search of bounding cases.

5.4.2.3 Identifying the important phenomena

Key phenomena, key parameters, and the range of parameter values associated with the analyzed event should be identified. The supporting experimental data should also be provided or referenced, and theoretical understanding should be demonstrated.

If an event is characterized by sufficiently different stages, then key phenomena should be identified for each stage.

The importance of the involved phenomena should be judged against each acceptance criterion, separately. Key parameters are identified for each important phenomenon. These parameters are then ranked for their importance in influencing the applicable acceptance criteria.

Sensitivity analyses can be used, in conjunction with expert judgment, to help identify and rank the parameters by assessing their influence on analysis results for each acceptance criterion. Particular importance should be given to the identification of "cliff-edge" effects, such as any abrupt changes in phenomena during any stage of the analysis.

The results of experiments should also be used to help identify important parameters, assist in ranking the importance, and to identify if and where abrupt changes occur.

5.4.2.4 Models and computer codes

Safety analysis is performed using models of the plant systems and physical phenomena.

All the important phenomena, as identified in subsection 5.4.2.3, should be represented in the models embedded in the computer code used for the calculations.

The models and computer code applicability to the analyzed event should be demonstrated. Models of plant systems shall be verified to reflect as-built plant condition, taking into account plant states and aging effects (such as pump degradation, steam generator fouling, increased roughness). Severe accidents may have a particular impact on multi-unit NPPs, which emphasizes the need for a multi-unit model for severe accidents, at such stations. Further guidance is provided in subsection 5.4.5.

5.4.2.5 Defining boundary and initial conditions

The analysis should define the data characterizing the plant condition preceding the analyzed event and plant performance during the event — such as, but not limited to:

- plant operating mode
- reactor power
- fuel burnup and burnup distribution
- fuel temperatures
- coolant temperatures and pressures
- trip set-points and action set-points for mitigating systems
- instrumentation delays and uncertainties
- safety system performance characteristics
- performance of other plant equipment (such as pumps, valves, coolers, boilers, and turbine)
- weather conditions

In the application of such data, the plant operating limits and conditions (OLCs) should be taken into account. The plant condition used as the initial conditions for the analysis may reflect the actual plant condition or (in many cases) reflect the limits selected for enforcement of the OLCs. This would be done so that the analysis can confirm that the selection of an OLC value is effective. Alternatively, the analysis results may be employed to derive a suitable value for use as an operating limit. Care and good judgment are required to ensure that the set of OLCs derived from such safety analyses are consistent with each other.

5.4.2.6 Conducting calculations

Comprehensive calculations are conducted to assess the plant performance against each applicable acceptance criterion. Sensitivity studies are undertaken to assess the impact on analysis results of key assumptions — for example, in identifying the worst single failures in various systems, or to assess the impact of using simplified models instead of more accurate and sophisticated approaches (requiring significant effort in the calculations). Sensitivity analysis, with systematic variations in computer code input variables or modelling parameters, should confirm that there are no “cliff-edge” effects — such as abrupt changes in plant response, or accident consequences resulting from a change in parameter values.

The duration of the transients considered in the analysis should be sufficient to determine the event consequences. Therefore, the calculations for plant transients are extended beyond the point where the NPP has been brought to shutdown and stable core cooling, as established by some identified means (i.e., to the point where a long-term, stable state has been reached and is expected to remain as long as required). The analysis should take into account the capacity and limitations of long-term make-up water and electrical power supplies.

In cases where the various stages of the transient are governed by different phenomena and/or different time scales, different methods and tools can be applied to model the consecutive stages.

5.4.2.7 Accounting for uncertainties

In the deterministic safety analysis for level-3 defence in depth, all key uncertainties should be identified and accounted for. The safety analysis for level-3 should incorporate appropriate uncertainty allowances for the parameters relevant to the analyzed accident scenario. Such uncertainties include modelling and input plant parameters uncertainties.

The modelling relevant parameters include those used to start the action of a mitigating system and/or those which can have a significant impact in challenging the integrity of a barrier preventing the release of fission products. The modelling uncertainties are associated with the models and correlations, the solution scheme, data libraries and deficiencies of the computer programs.

The code accuracy obtained as the result of validation work should be used as a source for uncertainties of relevant modelling parameters. The code accuracy is defined by the bias and the variability in bias, and should be obtained from the comparison of code predictions with experimental data, station data or other applicable data.

Input plant parameters (also referred to as operational parameters) are those parameters that characterize the state of plant’s SSCs or are used to actuate a mitigating system. These are measured using in-reactor instrumentation.

The measurement uncertainties are available from the plant instrumentation and control system documentation or the OLCs. The systematic (“bias”) and random uncertainty components (“standard deviation”) should be accounted for.

The measurement bias represents an element of measurement uncertainty arising from a systematic error known to cause deviation in a fixed direction. The standard deviation represents an element of measurement uncertainty which cannot be defined exactly, or which can cause deviation in either direction, but can be estimated on the basis of a probability distribution.

The above-presented uncertainties should be accounted for accordingly, either in the conservative analysis, or in the best estimate plus evaluation of uncertainties methodologies.

In the safety analyses for level-2 and level-4 defence in depth (where a realistic, best-estimate analysis method may be used) it is not necessary to account for uncertainties to the same extent.

5.4.2.8 Verification of results

Verification is performed to ensure that the deterministic safety analysis results are:

- correctly extracted from the analysis codes' output
- physically and logically sound
- consistent with experimental data from suitable integral tests, plant recorded data, previous similar safety analyses or simulations with more advanced models
- bounding predictions for each of the safety analysis acceptance criteria

5.4.2.9 Documentation of results

Results of deterministic safety analysis calculations are documented in such a way as to facilitate their review and understanding. The documentation of safety analysis results should include:

- objective of the analysis
- analysis assumptions and their justification
- plant models and modelling assumptions
- any computer code user options that differ from the options used in code validation
- analysis results in comparison with acceptance criteria
- findings and conclusions from sensitivity and uncertainty analyses

Further guidance is provided in subsection 5.5.

5.4.3 Analysis data

RD-310 requires the safety analysis be based on plant design and complete and accurate as-built information.

Operational historical recorded data (such as thermal power, flow rates, temperature and pressure) should also be included, where applicable. This information should cover plant SSCs, site specific characteristics and offsite interfaces.

For an NPP in the design phase, the operational data, if needed, should be derived from generic data from operating plants of similar design, or from research or test results. For an operating NPP, the safety analysis should use plant specific operational data.

The safety analysis values for each plant input parameter should be determined based on:

- design specifications
- tolerances
- permissible ranges of variability in operation
- uncertainties in measurement or evaluation for that parameter

The operational data should include:

- information on component and system performance, as measured during operation or tests
- delays in control systems
- biases and drift of instrumentation
- system unavailability due to maintenance or testing

Applicable limits for NPP parameters that are used as initial and boundary conditions should be identified. The NPP parameters assumed in the safety analysis should bound the ranges of parameters allowed by the operating procedures or, in a statistical approach, cover a predetermined high percentile of each range at a predetermined high confidence level.

The following NPP parameters may be used in analysis as input data, and should be specified in the OLCs, as measured or evaluated during plant operation:

- neutronic and thermal powers, including power distribution
- pressures
- temperatures
- flows
- levels
- leakage or bypass of valves, seals, boiler tubes, and containment
- inventory of radioactive materials
- fuel sheath defects
- flux shapes
- isotopic purity of coolant and moderator (where relevant)
- neutron poison concentration
- core burnup and burnup distribution
- instrument tolerances
- instrument time constants and delays
- parameters related to SSC aging (besides accounting for aging effects on other parameters)
- position of rods, valves, dampers, doors, gates
- number of operational components, such as pumps and valves

Note: In the preparation of the data in the above list, there are some parameters (such as core burnup and burnup distribution) that are not measured directly. Core characteristics for all fuel loads should be accounted for. In this example, they are evaluated and extracted from computer simulation for which the accuracy of these tools is supported by station and experimental data. There are generally some inputs to the safety analysis that are derived or inferred from data obtained experimentally.

It should also be noted that the effects of aging include both long-term mechanisms causing gradual degradation, as well as mechanisms causing rapid degradation. Degradation mechanisms include thermal cycles, deformation, strain, creep, scoring, fatigue, cracking, corrosion and erosion. The allowed aging limits are part of the safety analysis input data.

Uncertainties in plant data should be determined and recorded. These uncertainties should be considered in the uncertainty and sensitivity analyses.

5.4.4 Analysis assumptions

Assumptions are made in the input data, such as those related to the design and operating parameters, as well as in the physical and numerical models implemented in the computer codes.

Assumptions may be intended to be realistic, or deliberately biased in a conservative direction.

The assumptions that are generally used for the level-3 defence in depth analysis of AOOs and DBAs are described in subsections 5.4.4.1 to 5.4.4.7. It should be noted that some of these assumptions are not necessary in the analysis of AOOs for assessing control system capability (level-2 defence in depth,) if such an approach can be justified.

For BDBA safety analysis, one objective is to demonstrate the capabilities of SSCs to meet the design requirements specified for BDBA conditions. The analysis should account for the full design capabilities of the plant, including the use of some safety and non-safety systems beyond their originally intended function (to return the potential severe accident to a controlled state, or to mitigate its consequences). The BDBA analysis assumptions on crediting and modelling plant systems and their capability during a BDBA should be consistent with the objectives of the analysis. If credit is taken for use of systems beyond their originally intended function, there should be a reasonable basis to assume they can and will be used as assumed in analysis. This basis can be obtained from the evaluation of effectiveness of these systems to operate in severe accident conditions, if they are still available.

5.4.4.1 Single failure criterion in safety group

The single failure criterion stipulates that the safety group consisting of a safety system and its support systems should be able to perform its specified functions even if a failure of single component occurs within this group.

Expectations related to the application of the single failure criterion in design can be found in the CNSC's regulatory document RD-337, *Design of New Nuclear Power Plants*.

The analysis should assume a single failure to occur for each element of a safety group in turn, and identify the worst single failure for each acceptance criterion. In addition to a single failure of a component, the analysis should account for the impact of possible maintenance, testing, inspection or repair on safety group performance.

Safety analysis of AOOs and DBAs for level-3 defence in depth should apply the single failure criterion to each safety group.

The single-failure criterion does not need to be applied in the analysis of AOO for level-2 defence in depth and BDBA.

5.4.4.2 Consequential failures

The analysis should take into account consequential failures that may occur as a result of an initiating event.

Any failures that occur as a consequence of the initiating event are part of that event and are not considered to be a single failure for the purpose of safety analysis. For example, equipment that is not qualified for specific accident conditions should be assumed to fail unless its normal operation leads to more conservative results.

5.4.4.3 Credit for actions of systems – performance of structures, systems and components

5.4.4.3.1 Availability of systems

The operation of systems should be credited only when they are designed or shown to be capable of performing the intended function, and are qualified to withstand all challenges and cross-link effects arising from the accident.

In the safety analysis of an AOO for level-2 defence in depth, credit may be taken for the operation of process and control systems whose actions could help mitigate the event, as long as the credited systems are not impaired as a consequence of the initiating event. The status of these systems and the values assigned to their parameters need to be justified.

In the safety analysis of AOOs and DBAs for level-3 defence in depth, no credit should be taken for the operation of the control systems in mitigating the effects of the initiating event. The effects of control system actions should be considered, if these actions would aggravate the transient or delay the actuation of the protection features.

If the operation of non-qualified equipment results in worse event consequences, this will lead to the general assumption that such equipment is operated in a manner that makes the event worse.

Any process equipment that is operating prior to the event is assumed to continue operating, if it is not affected by the initiating event. For example, boiler feed can be assumed to continue until loss of electrical power, for those events which do not produce a harsh environment.

5.4.4.3.2 Partial and total failures

Partial and total failures of equipment should be considered in the analysis of each failure sequence, to identify the worst failure for each acceptance criterion.

5.4.4.3.3 Worst piping failure

Various modes of piping failures should be considered in loss of coolant analyses. They include circumferential, guillotine, and longitudinal failures at any location in a system.

For circumferential and guillotine failures, analysis should consider a discharge area up to, and including, twice the cross-sectional area of the piping.

For longitudinal breaks, the analysis should justify the upper limit of the range of postulated break size.

The worst break location, size, and orientation, in the context of posing the most challenges to a safety analysis requirement, should be identified through analysis, including sensitivity analysis, using a conservative break model.

For CANDU reactors, failures of reactor inlet and outlet headers are considered in the same way as piping failures.

5.4.4.3.4 Loss of offsite power

In addition to a single failure and any consequential failures, a loss of offsite power should be assumed, unless a justification is provided.

The loss of offsite power may be assumed to occur either at the initiation of the event or as a consequence of reactor and turbine trip. For example, when loss of Class IV power (CANDU type reactor) is assumed, the event should be analyzed both with and without the loss of offsite power, and the most limiting results should be used.

5.4.4.4 Credit for actions of systems – safety system performance

Safety systems should be credited at their minimum allowable performance, in accordance with the OLCs.

5.4.4.4.1 Shutdown means

The deterministic safety analysis shall demonstrate the effectiveness of all credited shutdown means, by demonstrating that the design meets applicable acceptance criteria (see subsection 5.3

This subsection contains different expectations, depending on the reactor's design and inherent characteristics, as described in RD-337. Two broad categories of reactors are considered, as follows:

- reactors with inherent safety - designs that demonstrate that an AOO or DBA with failure of the fast-acting shutdown means (anticipated transient without reactor trip type analysis) does not lead to severe core damage and a significant early challenge to containment
- reactors with engineered safety - designs that cannot demonstrate that an AOO or DBA with failure of the fast-acting shutdown means does not lead to severe core damage and a significant early challenge to containment

The following are the applicable acceptance criteria for the two categories of reactors:

Reactors with inherent safety

For the first shutdown means, which is fast-acting, the analysis should demonstrate that the criteria applicable to the initiating event class (AOO or DBA, as applicable) are met. Operator actions to supplement the fast-acting shutdown means may be credited, provided that the conditions for manual reactor trip are satisfied (see the end of this subsection).

For the second shutdown means (which may be manually initiated), the frequency of occurrence of an AOO and the failure frequency of the fast-acting shutdown means may result in a combined frequency that falls in the DBA range, in which case the applicable limits are the DBA dose limits. If the designer can demonstrate a very high reliability for the fast-acting shutdown means, it may be acceptable to use BDBA limits (i.e., the safety goals).

The frequency of a DBA and the failure frequency for the fast-acting shutdown means may result in a combined frequency that falls in the BDBA range, in which case the applicable limits are the safety goals.

Reactors with engineered safety

The design includes two redundant, fast-acting means of shutdown, both of which should be demonstrated to be equally effective (see RD-337, *Design of New Nuclear Power Plants*). The criteria for both shutdown means will be the same, and will be AOO or DBA criteria, as applicable to the event class.

To assist with better understanding of trip parameter expectations, Table 3 can be used to determine the minimum expectations for the specific event under consideration. Reactor designs with inherent safety are shown as "reactor design scenario 1". Reactor designs with engineered safety are shown as "reactor design scenario 2".

Table 3: Minimum expectations for the number of trip parameters

Reactor design scenario	**Failure to shutdown challenges containment**	**Means of shutdown (SD)**	**Ideal trip parameter (TP) expectation**	**Is a direct trip parameter available?**	**Minimum expectation**	**Trip parameter total**
1	no	one fast-acting SD means	one direct TP per event	yes	one direct TP per event	one TP
				no	two diverse indirect TPs per event	two TPs
		second SD means	one direct TP per event	yes	one direct TP per event	one TPs
				no	two diverse indirect TPs per event	two TPs
2	yes	one fast-acting SD means	two TPs per event (at least one direct)	yes	two TPs (at least one direct)	two TPs
				no	two indirect TPs	two TPs
		second fast-acting SD means	two TPs per event (at least one direct)	yes	two TPs (at least one direct)	two TPs
				no	two indirect TPs	two TPs

The following major points from Table 3 should be noted:

- two shutdown means are always required for each reactor design scenario
- if the consequences of a failure to shutdown may challenge the containment, then two fast-acting shutdown means are required (reactor design scenario 2)
- if the consequences of a failure to shutdown may challenge the containment, then there are two trip parameters per event per shutdown means
- multiple trip parameters on a shutdown means must be diverse, if practicable
- trip parameters between shutdown means must be diverse, if practicable

A manual reactor trip can be considered to be equivalent to a trip parameter if the requirements for crediting operator action from the main control room are met (see subsection 5.4.4.5) and the reliability of manual shutdown meets the reliability requirements for an automatic trip.

5.4.4.4.2 Emergency core cooling system

If the emergency core cooling system (ECCS) logic has an injection logic conditioned by the presence of other indicators (i.e., conditioning signal), then the safety analysis should identify and evaluate the consequences of situations where those conditioning signals may be blinded.

If the ECCS activation logic is complex (i.e., several different actions are required for the system to be considered fully activated), then the safety analysis should consider the consequences if some of these actions do not occur — for example, a failure to re-align the ECCS pump suction to the containment sump.

For certain designs, the following considerations should be taken into account:

- the potential for gas entrainment that could result in damage due to the occurrence of water hammer
- the impact on recirculation flows in the presence of filter plugging, debris blockage, heat exchanger blockage, or pump cavitations
- the effect of non-condensable gases on flow and heat transfer

The safety analysis should consider the impact on the effectiveness of the ECCS of the inaction, partial action, and normal functioning of any other systems that supplement or degrade the cooling capability of the ECCS.

5.4.4.4.3 Containment

The deterministic safety analysis should identify and evaluate consequences of situations when the containment isolation instrumentation is blinded. For containment, "blinded" refers to conditions for which a containment isolation actuation setpoint is approached, but not reached. For example, the containment may be blinded by the inaction, partial action, or normal functioning of other systems that supplement or degrade the containment performance. Containment blinding scenarios are important, because an accident with a potential for radioactivity release may not trigger the activation of containment isolation.

The containment leakage rate assumed in the analysis should be based on containment design leak-tightness requirements, and confirmed by the leakage rate tests.

5.4.4.4.4 Equipment under maintenance

The analysis should account, where applicable, for the possibility of the equipment being taken out of service for maintenance.

5.4.4.5 Operator action

Specific operator actions required in response to an accident should be identified. Operator actions can be credited in the safety analysis for level-3 defence in depth only if:

- there is reliable instrumentation designed to provide clear and unambiguous indication of the need to take action
- the power plant has operating procedures that identify the necessary actions, operator training, support personnel, spare parts, and equipment
- environmental conditions do not prevent safe completion of operator actions

Following the first clear and unambiguous indication of the necessity for operator actions, such actions may normally be credited in the safety analysis (level-3 defence in depth) to be started no sooner than:

- 15 minutes for actions in the main control room
- 30 minutes for actions outside the main control room (see RD-337, *Design of New Nuclear Power Plants*)

It should be shown by assessment that the specified times are sufficient for the operator to detect and completely diagnose the event, and to carry out the required actions. Such assessment should account for the following:

- time starting from the occurrence of the initiating event to the receipt of the event indication by the operator
- time to carry out the diagnosis
- time required to perform the action
- time for the safety related function to be completed

In certain circumstances, which must be justified, a completion time shorter than 15 minutes for a control room action might be assumed, provided that:

- the operator is exclusively focused on the action in question
- the required action is unique, and does not involve a choice from several options
- the required action is simple and does not involve multiple manipulations

The assessment of the credited human action items should be formally documented. It should include a validation process, which can encompass:

- documented procedures that define specific operator action entry points and actions
- training of personnel on those procedures (training outline, materials, records)
- performing station drills, exercises or control room simulator studies, to confirm that human actions can be completed, and to assess response times
- consideration of control room simulator data from training activities
- analysis and assessment of the response times, to provide credible time estimates for safety analysis usage
- validation reports

5.4.4.6 Modelling assumptions

The assumptions incorporated in the computer codes, or made during code applications, should be such that safety analysis results (whether best-estimate or conservative) remain physically sound.

In performing safety analysis, justifications should be provided for all instances where the assumptions used are different than those used in the validation.

5.4.4.7 Dose calculations

As mentioned in subsection 5.3, the committed whole-body dose for average members of the critical groups who are most at risk (at, or beyond the site boundary) is calculated in the deterministic safety analysis for a period of 30 days after the analyzed event.

The effective dose should be used in dose calculations, and should include contributions from:

- external radiation from cloud and ground deposits
- inhaled radioactive materials
- skin absorption of tritium

In dose calculations, the worst weather scenario in terms of predicted dose should be assumed. All weather scenarios with probabilities of occurrences higher than 5% should be accounted for.

No intervention in the form of decontamination or evacuation should be assumed. Intervention against ingestion of radioactive materials and natural removal processes may be assumed.

Dose calculations should also be conducted for several time intervals, and up to one year after the accident.

5.4.5 Computer codes

The use of realistic computer codes in safety analysis is preferable, given that the use of conservative codes may produce misleading or unrealistic results. However, an extensive experimental database should be established to demonstrate the code applicability and to validate the code, thereby providing a basis for confidence in code predictions.

Fully integrated models could give a more accurate representation of the event, and should be used to the extent practicable. These models address all important phenomena within a single code or code package. Sequential application of single-discipline codes is more likely to misrepresent feedback mechanisms than fully integrated models, and should be avoided unless there is a specific advantage.

As indicated in RD-310, CSA standard N286.7-99*, Quality Assurance of Analytical, Scientific, and Design Computer Programs for Nuclear Power Plants*, shall be applied in safety analysis code development and use.

The selection of computer codes should consider the code applicability, the extent of code validation, and the ability to adequately represent the physical system.

5.4.5.1 Computer code applicability

For the safety analysis of an event, the applicability of computer codes used to predict the consequences is established before conducting the analysis. The demonstration of code applicability includes the following steps:

- identification of all phenomena significantly influencing the key output parameters (see subsection 5.4.2.3)
- confirmation that the code implements adequate models for all key phenomena, and demonstrating that these models have been verified and validated against separate effect tests
- assessing the closure equations and constitutive relationships
- assessing scaling effects; the scalability of the integral effects tests should be assessed to confirm that there is no significant distortion in the database. Scaling distortions and their impact on the code assessment should be identified, evaluated and addressed in the safety analysis
- assessing the numerical stability of calculations and temporal and spatial convergence of iterative approximations. The spatial and temporal convergence are achieved when an increase or a reduction in the node or time step sizes (which includes changing the minimum time step, if necessary) does not change simulation results significantly
- addressing any gaps or deficiencies in the code applicability for the analyzed event

The code applicability assessment and relevant knowledge bases are documented in sufficient detail to allow for an independent review.

To model behaviour involving many coupled phenomena, it should be demonstrated that data is transferred through interfaces (i.e., from the calculation of one phenomenon to another) in a manner which adequately captures the physical phenomena and feedback mechanisms.

5.4.5.2 Code validation and quantification of accuracy

RD-310, *Safety Analysis for Nuclear Power Plants*, requires all computer codes to be validated for their application in safety analysis. The purpose of validation is to provide confidence in the ability of a code for a given application, and also to determine the code accuracy.

The validation should:

- demonstrate the capability and credibility of a computer code for use in specific analysis application
- quantify the accuracy of the code calculations (quantified through comparison of code prediction with experimental data or other known solutions)

The codes used in safety analysis are validated by comparing code predictions with:

- experimental data
- commissioning data and operating data, where available
- solutions to standard or benchmark problems
- closed mathematical solutions
- results of another validated computer program

The comparison of code predictions with solutions to standard problems or closed mathematical solutions for the purposes of validation is acceptable, but they should normally be supplemented with other types of comparisons.

The experimental database used for validation may encompass separate effects, as well as component and integrated tests. Chosen test validation should satisfy the following criteria:

- test data are obtained at physical and geometrical conditions and phenomena that are relevant either to normal operation conditions, or to a postulated accident scenario in the reactor
- tests used for validation are free of distortions due to geometry or other properties, to the extent practicable
- measurement uncertainties are quantified
- systematic errors (bias) are minimized, and their sources are understood
- the integrated tests used for validation should be specific to the reactor, and contain components representative of those used in the NPPs
- data used for model development is independent from data used for computer code validation

Accuracy of code predictions should be provided for the key modelling parameters, and for the plant parameters used to control power generation or to initiate a mitigating system (see subsection 5.4.2.7).

The bias and variability of bias in the computer code can be obtained from the comparison of code predictions with experimental data.

The code models used during validation should be identified and recommended for use in safety analysis, so that the safety analysis is consistent with the validation. Otherwise, the impact of using different models on the simulation results (code accuracy) should be assessed.

Clear recommendations should be made on the use of a code beyond the conditions for which validation has been performed, and all the effects of such extrapolations should be assessed and accounted for.

The effect of the modelling assumptions on the validation results should be assessed, including confirmation that a spatial and temporal convergence of the solution is achieved.

Documentation of the computer tools should be clear and easy to follow, so the uncertainties due to user effects would be negligible. The use of different computer hardware or operating systems should also have negligible effects. Means such as user training and compliance with quality assurance procedures should be clearly stated.

Computer code validation should be performed by qualified persons. Validation reports should be reviewed by qualified persons who had not participated in the validation.

The guidance given above is consistent with and complements the requirements in CSA N286.7-99, *Quality Assurance of Analytical, Scientific, and Design Computer Programs for Nuclear Power Plants*.

5.4.5.3 Physical representations

Data is also prepared to provide a mathematical representation of the physical components, and how their arrangements are to be represented by the computer simulation. This input data should be prepared in accordance with the following principles:

- a systematic method for representing components and connections should be developed
- the basis for the methodology should be documented. The methods used are usually based on experience in representing experimental facilities and other plants of similar configurations
- the representation should be verified and validated
- in some cases, plant tests (sometimes as commissioning tests) are required to establish the precision of such representations

In general, representations used for plant simulations should be created using the same principles as the representation used for code validation to minimize the related user effects.

5.4.6 Conservatism in analysis

Safety analysis needs to incorporate a degree of conservatism that is commensurate with the safety analysis objectives and is dependent on the event class. Conservatism in safety analysis is often necessary to cover the potential impact of uncertainties, and may be achieved through judicious application of conservative assumptions and data.

The concept of conservatism is applied to level-3 defence in depth safety analysis, to ensure limiting assumptions are used for the cases where knowledge of the physical phenomena is insufficient.

For level-2 and level-4 defence in depth, the safety analysis should be carried out using best estimate assumptions, data and methods. Where this is not possible, a reasonable degree of conservatism (appropriate for the objectives of these levels) should be used, to compensate for the lack of adequate knowledge concerning the physical processes governing these events.

While it is permissible — and sometimes encouraged — to use conservative codes, it is usually preferable to apply realistic (best estimate) computer codes. Where conservative analysis results are required for level-3 defence in depth (AOO and DBA) analysis, best estimate computer codes should be used along with the assessment of modelling and input plant parameter uncertainties.

The deterministic safety analysis for AOO and DBA (conservative analysis for level-3 defence in depth) should:

- apply the single-failure criterion to all safety groups, and ensure that the safety groups are environmentally and seismically qualified
- use minimum allowable performance (as established in the OLCs) for safety groups
- account for consequential failures that may occur as a result of the initiating event
- credit the actions of process and control systems only where the systems are passive and environmentally and seismically qualified for the accident conditions
- include the actions of process and control systems when their actions may have a detrimental effect on the consequences of the analyzed accident
- credit the normally running process systems that are not affected by the analyzed accident
- if operator actions are credited, demonstrate that credible “worst case” operator performance has been considered in the analysis and assessment

Independent selection of all parameters at their conservative values can lead to plant states that are not physically feasible. When this could be the case, it is recommended to select conservatively those key parameters that have the strongest influence on the results in comparison with the acceptance criterion under consideration. The remaining parameters can be specified more consistently in the ensuing calculations. Each calculation should account for the impact of a particular parameter, so that the effects of all parameters can be assessed.

5.5 Safety analysis documentation

Safety analysis documentation shall be comprehensive and sufficiently detailed to allow for a conclusive review. The review should be an independent review and conducted by suitably qualified experts. In particular, the following elements need to be included in the safety analysis documentation:

- a technical basis that includes
    - the objective(s) of the analysis
    - a description of the analyzed event, which should include description of the NPP operating mode, action of SSCs, operator actions and significant phases of the analyzed event (note that other events bounded by the analyzed event should also be identified)
    - a description of safety concerns, challenges to safety, and applicable safety analysis criteria, requirements and numerical limits
    - identification of key phenomena significantly affected by the key parameters for the analyzed event, along with a description of the systematic process used for identification of key parameters
- a description of the analyzed facility, including important systems and their performance, as well as operators actions
- information on the analysis method and assumptions
- information demonstrating the code applicability, including (when available) evidence that codes have been validated against prototypical experiments and assessment of code accuracy, as well as references to the relevant experimental results. Demonstration that the analysis assumptions are consistent with the plant operating limits (with evidence from NPP operation

and experiments demonstrating the assumed observed variances in operating parameters, and uncertainties in modelling parameters, respectively)

- a description of the results of analysis, including results of sensitivity and uncertainty studies with sufficient detail to show dominant phenomena. Evidence of independent verification of the inputs and the results. Evidence of analysis review, including assessment, of the impact — if any — on the plant operating limits, conditions, manuals etc.

Safety analysis documentation should be written in a manner that can be easily understood by the station staff controlling the plant's operating limits and conditions.

5.6 Safety analysis review and update

5.6.1 Review of safety analysis results

Procedures should be developed to determine the extent of the independent review to be applied at each step of the safety analysis.

To review the safety analysis and identify potential deficiencies, reviewers should be familiar with:

- safety standards, analytical methods, and technical and scientific research
- changes in power plant data, design, operating envelope and operating procedures
- information on operating experience from other nuclear power plants

In reviewing the safety analysis, the following review elements should be considered:

- plant design information, supported by layout, system and equipment drawings, and design manuals
- operating limits and permitted operational states
- information about the functional capability of the plant, systems and major items of equipment
- the findings of tests which validate the functional capability
- the results of inspection of components
- site characteristics, such as flood, seismic, meteorological, and hydrological databases
- offsite characteristics, including population densities
- results of similar analyses
- developments in analytical methods and computer codes
- regulatory rules for safety analysis
- safety analysis standards and procedures

The extent and method of the review should be commensurate with:

- the analysis complexity and novelty
- similarity to previously reviewed analyses
- predicted margins to acceptance criteria

For novel and complex analysis, the use of alternative methods should be considered to confirm analysis results. Alternative methods used for confirmation may be simplified, but should be capable of demonstrating that the original analysis results are reasonable.

5.6.2 Update of safety analysis

The safety analysis report is 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*.

The periodic update of the safety analysis report should:

- incorporate new information
- address identified new issues
- use current tools and methods
- address the impact of modifications to the design and operating procedures that might happen over the life of the NPP

Updating the safety analysis ensures that it remains valid, while taking into account:

- the actual status of the NPP
- permitted plant configuration and allowable operating conditions
- predicted plant end-of-life state
- changes to analytical methods, safety standards and knowledge that invalidate existing safety analysis

In order to achieve the above objective, the following guidelines can be used in updating safety analyses:

- review safety analysis methods against the applicable standards, and research findings available in Canada and internationally, to identify the elements that should be taken into account
- review the changes made in the NPP data, design, operating envelope, and operating procedure, to identify the elements that shall be updated
- review information on NPP commissioning and operating experience, both in Canada and worldwide, to identify relevant information that should be accounted for
- review the progress in the resolution of previously identified safety analysis issues, to identify the impact on the safety analysis methods and results

5.7 Quality of safety analysis

All safety analysis activities should be performed in conformance with the established quality assurance (QA) program. All sources of data should be referenced and documented, and the various steps of the process should be recorded and archived, to allow independent checking.

The safety analysis QA program should comply with regulatory requirements, codes and standards, and be consistent with the best international practices.

Appendix A: Outputs of Event Identification and Classification

This table provides grouping of the events into AOOs, DBAs and BDBAs, and illustrates the outputs of the event identification and classification process described in subsection 5.2. This list is for illustration only, and is not meant to be comprehensive.

Initiating Event	Additional Failures	AOO	DBA	BDBA
LOCA inside containment				
very small LOCA (leak) • heat transport system (HTS) leak inside containment (within the D_2O feed pump capacity up to 50 kg/s)	no additional failures	√		
small LOCA • small HTS pipe failure (range of 50-1,000 kg/s) • pipe failure at the top of pressurizer • end-fitting failure • pressure tube failure with calandria tube intact • pressure tube/calandria tube failure (in-core LOCA)	no additional failures		√	
	failure of D_2O recovery/D_2O feed		√	
	failure of Class IV power		√	
	failure of containment isolation			√
	failure of all vault coolers			√
	failure of containment pressure relief valves (PRV)			√
	failure of containment pressure suppression			√
	failure of filtered containment discharge			√
	failure of steam generator (SG) cooldown			√
	failure of emergency core cooling system (ECCS)			√
transition break LOCA • HTS pipe failure (1,000–3,000 kg/s)	no additional failures		√	
	failure of Class IV power		√	
	failure of containment isolation			√
	failure of all vault coolers			√
	failure of containment PRV			√
	failure of containment pressure suppression			√
	failure of filtered containment discharge			√
	failure of SG cooldown			√
	failure of ECCS			√
large-break LOCA • (>3,000 kg/s)	no additional failures		√	
	failure of Class IV power		√	
	failure of containment isolation			√
	failure of all vault coolers			√
	failure of containment PRV			√
	failure of containment pressure suppression			√
	failure of filtered containment discharge			√
	failure of SG cooldown			√
	failure of ECCS			√

Initiating Event	Additional Failures	AOO	DBA	BDBA
LOCA outside containment				
very small LOCA (leak) outside containment • HTS instrument tubing rupture outside containment	no additional failures	√		
	failure of shutdown cooling system (SDCS)		√	
SG tube chronic leak (<50kg/h) with high I-131 concentration	no additional failures	√		
single SG tube rupture	no additional failures	√		
	failure of SDCS		√	
	failure of condenser steam discharge valves (CSDVs)		√	
	failure of affected SG main steam isolation valves (MSIV)		√	
	failure of SDCS and CSDVs			√
multiple (≤10) SG tube rupture	no additional failures		√	
multiple (>10) SG tube rupture	no additional failures			√
HTS gland seal failure	no additional failures	√		
	failure of SDCS		√	
HTS bleed line failure	no additional failures		√	
	bleed valve failed open		√	
HTS feed line failure	no additional failures		√	
	bleed valve failed open		√	
failure to close HTS check valve	no additional failures		√	
Loss of flow				
minor flow blockage in one channel	no additional failures	√		
	ECCS or containment impairment		√	
severe flow blockage in one channel	no additional failures		√	
	ECCS or containment impairment			√
stagnation feeder break	no additional failures		√	
	failure of Class IV power			√
	failure of containment isolation			√
	failure of all vault coolers			√
	failure of containment PRV			√
	failure of containment pressure suppression			√
	failure of filtered containment discharge			√
	failure of SG cooldown			√
	failure of ECCS			√

Initiating Event	Additional Failures	AOO	DBA	BDBA
Fuelling failures				
fuel ejection from fuelling machine into containment	no additional failures		√	
	failure of class IV power			√
	failure of containment isolation			√
	failure of all vault coolers			√
	failure of containment PRV			√
	failure of containment pressure suppression			√
	failure of filtered containment discharge			√
	failure of SG cooldown			√
	failure of ECCS			√
Feedwater system failures				
total loss of feedwater	no additional failures		√	
	failure of SDCS		√	
	failure of steam generator emergency cooling system (SGECS) or emergency secondary water supply system (ESWS)			√
feedwater line failure upstream of the last check valve	no additional failures		√	
	failure of SDCS		√	
	failure of SGECS or ESWS			√
feedwater line failure downstream of the last check valve	no additional failures		√	
	failure of SDCS			√
	failure of SGECS or ESWS			√
Steam supply system failure				
inadvertent closing of one MSIV	no additional failures	√		
turbine/generator load rejection and turbine trip	no additional failures	√		
spurious opening of one or more main steam safety valves (MSSVs)	no additional failures	√		
turbine trip with CSDV unavailable	no additional failures	√		
large steam pipe failure: • main steam line rupture • main steam balance header failure • SG steam nozzle rupture	no additional failures		√	
	failure of SDCS			√
	failure of SGECS or ESWS			√
reheater drain line failure	no additional failures	√		
	failure of SDCS		√	
	failure of SGECS or ESWS			√
loss of deaerator pressure due to rupture of extraction steam line	no additional failures		√	
Heat transport pump events				
HTS pump trip	no additional failures	√		
HTS pump seizure	no additional failures		√	
HTS pump shaft failure	no additional failures		√	

Initiating Event	Additional Failures	AOO	DBA	BDBA
Fuel handling system failures				
loss of fuelling machine (FM) cooling in transit	no additional failures		√	
	failure of containment isolation			√
	failure of containment PRVs			√
loss of FM coolant on reactor	no additional failures	√		
	failure of containment isolation		√	
	failure of containment PRVs		√	
	failure of filtered containment discharge		√	
bundle crushed with FM latched to reactor	no additional failures	√		
	steam generator tube leak	√		
fuel handling incidents at the irradiated fuel port (IFP)	no additional failures	√		
	off-gas system not available		√	
irradiated fuel bay (IFB) incidents	no additional failures	√		
	loss of bay contaminated exhaust system		√	
loss of IFB cooling	no additional failures	√		
	loss of backup cooling		√	
	loss of bay contaminated exhaust system		√	
loss of IFB inventory	no additional failures		√	
	loss of bay contaminated exhaust system			√
Electrical failures				
loss of Class IV power	no additional failures	√		
	failure of Class III power		√	
loss of unit Class I power	no additional failures	√		
loss of unit Class II power	no additional failures	√		
loss of unit emergency power supply (EPS)	no additional failures	√		
loss of common electrical power	no additional failures	√		
Control failures				
controlling computer failures	no additional failures	√		
loss of reactivity control	no additional failures	√		
loss of power reactor regulation	no additional failures	√		
steam generator (SG) pressure low-spurious opening of atmospheric steam discharge valves (ASDVs) and CSDVs	no additional failures	√		
loss of SG level control	no additional failures	√		
loss of dearator level control	no additional failures	√		
loss of heat transport pressure control: over-pressurization	no additional failures	√		
loss of heat transport pressure control: depressurization	no additional failures	√		
SDCS and shield cooling failures				
loss of cooling/temperature control	no additional failures	√		
loss of flow	no additional failures		√	
piping failure	no additional failures		√	
SDCS heat exchanger tube failure	no additional failures		√	

Initiating Event	Additional Failures	AOO	DBA	BDBA
shield cooling system loss of circulation	no additional failures		√	
	failure of SDCS		√	
total loss of low-pressure service water open system (LPSWOS)	no additional failures	√		
loss of end shield inventory	no additional failures	√		
	failure of SDCS		√	
loss of shield temperature control	no additional failures	√		
	failure of SDCS		√	
Moderator system failures				
loss of LPSWOS	no additional failures	√		
	failure of moderator high-level trip		√	
	failure of containment isolation		√	
	failure of PRVs		√	
	failure of containment filtered discharge		√	
loss of moderator circulation	no additional failures	√		
	failure of moderator high level switch		√	
	failure of SDCS		√	
loss of moderator temperature control low	no additional failures	√		
loss of moderator inventory	no additional failures		√	
	failure of SDCS		√	
moderator heat exchange tube failure	no additional failures		√	
loss of cover gas pressure	no additional failures	√		
loss of cover gas circulation	no additional failures	√		
loss of LPSWOS to moderator heat exchangers	no additional failures	√		
	failure of moderator high level trip		√	
	failure of SDCS		√	
Support system failures				
loss of LPSWOS/recirculating cooling water failure	no additional failures	√		
	failure of moderator high level trip		√	
	failure of containment isolation		√	
	failure of PRVs		√	
	failure of containment filtered discharge		√	
	failure of ESWS		√	
ESWS failure	no additional failures	√		
instrument air system failure	no additional failures		√	
loss of condensate flow to deaerators	no additional failures		√	
Common mode triggered events (classification of these events would depend on the assumed parameters)				
internal fires	no additional failures		√	√
tritium release	no additional failures		√	√
hydrogen fire	no additional failures		√	√
hydrogen explosion	no additional failures		√	√
design basis earthquake	no additional failures		√	√

Initiating Event	Additional Failures	AOO	DBA	BDBA
turbine breakup	no additional failures		√	√
Flood	no additional failures		√	√
design basis tornado	no additional failures		√	√
design basis rail line blast	no additional failures		√	√
toxic/corrosive chemical rail line incident	no additional failures		√	√

Appendix B: Examples of Derived Acceptance Criteria

In accordance with RD-310, *Safety Analysis for Nuclear Power Plants*, subsection 5.3.4, the licensee is to establish derived acceptance criteria. Appendix B provides guidance on the application of the derived acceptance criteria specified in this guidance document. The examples below are obtained from current Canadian and international practice.

B.1 Anticipated operational occurrences (AOOs)

The overall criteria for an AOO are as follows (see RD-337, *Design of New Nuclear Power Plants*):

- the dose acceptance criterion for an AOO is met
- SSCs that are not involved in initiating the event are to remain fit for continued operation

RD-337 states expectations that the majority of AOOs will be mitigated by the control systems and will not need the action of the safety systems to prevent damage.

Additionally, all AOOs shall be mitigated by the safety systems, with no assistance from the control systems. Only the criteria that show successful mitigation by the safety systems are shown here, in Table B.1.

Table B.1: Examples of acceptance criteria for anticipated operational occurrences for level-2 defence in depth

Barrier to fission product releases or fundamental safety function	Qualitative acceptance criteria
fuel matrix	• fit for service
fuel sheath (fuel cladding)	• no dryout/no departure of nucleate boiling (DNB)
fuel assembly	• maintain fuel cooling ability • retain rod-bundle geometry with adequate coolant channels to permit removal of residual heat • no impediment to reactor shutdown means due to geometry change (LWR)
fuel channel (CANDU)	• fit for service o ASME service level B not exceeded
primary coolant system (excluding CANDU fuel channel)	• fit for service o ASME service level B not exceeded
secondary coolant system	• fit for service o ASME service level B not exceeded

Barrier to fission product releases or fundamental safety function	Qualitative acceptance criteria
Containment	• fit for service o ASME service level B not exceeded • leakage remains within design limit leakage
control of reactivity	• reactivity controlled by safety system • after shutdown, there is no inadvertent return to criticality
removal of residual heat	• heat removal by safety system effective
monitoring of conditions	• fit for service: o safety system instrumentation environmentally and seismically qualified
offsite dose	• within the dose acceptance criteria of RD-337 for an AOO

B.2 Design basis accidents

The overall criteria for a DBA are as follows:

- the dose acceptance criterion for a DBA is met
- the event does not progress to more severe conditions

Subsection 5.3.4 of RD-310 states the following general principles to be met by derived acceptance criteria:

- avoid the potential for consequential failures resulting from an initiating event
- maintain the SSCs in a configuration that permits the effective removal of residual heat
- prevent development of complex configurations or physical phenomena that cannot be modeled with high confidence
- be consistent with the design requirements for the plant’s SSCs

Table B.2 provides examples of DBA acceptance criteria.

Table B.2: Examples of acceptance criteria for design basis accidents

Barrier to fission product releases or fundamental safety function	Qualitative acceptance criteria
fuel matrix	• no fuel centreline melting • no fuel breakup • no excessive energy deposition

Barrier to fission product releases or fundamental safety function	**Qualitative acceptance criteria**
fuel sheath (fuel cladding)	• fuel elements (fuel rods) that exceed the critical heat flux (CHF) or departure of nucleate boiling (DNB) criteria are assumed to rupture and contribute to offsite dose • no excessive strain of fuel sheath • fuel elements are to meet applicable limits for: o sheath temperature o local sheath oxidation o oxygen embrittlement of fuel sheath
fuel assembly	• maintain fuel coolability • retain rod-bundle geometry or fuel assembly with adequate coolant channels to permit removal of residual heat • no impediment to reactor shutdown means due to geometry change (LWR)
fuel channel (CANDU)	• fuel channel remains intact • local pressure tube strain below failure threshold • moderator subcooling precludes failure • no constrained expansion • no fuel sheath melting • no fuel centreline melting • no fuel breakup • no fuel element bowing and/or sagging into pressure tube (PT) contact
primary coolant system (excluding CANDU fuel channel)	• pressure boundary remains intact: o ASME service level C not exceeded o no consequential boiler tube leaks
secondary coolant system	• pressure boundary remains intact: • ASME service level C not exceeded
calandria and moderator system (not applicable to LWR)	• pressure boundary remains intact: o ASME service level C not exceeded

Barrier to fission product releases or fundamental safety function	**Qualitative acceptance criteria**
containment	• containment conditions remain within design basis: o pressure less than design pressure o containment leakage remains within design leakage limit o environmental qualification (EQ) conditions (temperature, humidity, radioactive doses) on credited SSCs are met o no break local effects (missiles, break jets, pipe whip, hydrogen standing flame) that could fail confinement function o local hydrogen concentrations below flame acceleration (FA) and deflagration to detonation transition (DDT) criteria o combustion loads from slow deflagration less than those that could damage containment SSCs
control of reactivity	• reactivity is controlled: o no prompt criticality o after shutdown, any return to power is limited in extent, and does not lead to exceeding any other derived acceptance criteria
removal of residual heat	• continuous long term core cooling is possible: o core geometry is coolable o residual heat is removed from the core o heat is transported to ultimate heat sink
monitoring of conditions	• fit for service: o safety system instrumentation environmentally and seismically qualified
offsite dose	• within the dose acceptance criteria of RD-337 for a DBA

Abbreviations

ALARA	as low as reasonably achievable
AOO	anticipated operational occurrence
ASME	American Society of Mechanical Engineers
BDBA	beyond design basis accident
CNSC	Canadian Nuclear Safety Commission
DBA	design basis accident
ECCS	emergency core cooling system
EPS	emergency power supply
HTS	heat transport system
IAEA	International Atomic Energy Agency
LBB	leak-before-break
LOCA	loss of coolant accident
LWR	light water reactor
MCR	main control room
NPP	nuclear power plant
NSCA	*Nuclear Safety and Control Act*
OLC	operating limits and conditions
PIE	postulated initiating event
PSA	probabilistic safety assessment
PWR	pressurized water reactors
RCS	reactor coolant system
SSCs	structures, systems and components

Glossary

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

acceptance parameter
A plant parameter that characterizes plant response and has a defined acceptance criterion as a limit for the acceptable range of values.

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 nuclear power plant, 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 beyond design basis accident may or may not involve core degradation.

bias
Uncertainty arising from a systematic error that is known to cause deviation in a fixed direction.

blinding
Conditions for which an actuation or conditioning signal is approached but not reached, either because of the small magnitude of the initiating event or the actions of other process or safety systems.

bounding event
The event with the smallest predicted margin to a specific acceptance criterion.

code accuracy
The degree of closeness of a calculated quantity to its actual value. Comprised of the bias and variability of bias of a computer code that are derived from the comparison of code predictions with experimental data.

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.

conservatism
Use of assumptions, based on experience or indirect information, about a phenomena or behaviour of a system being at or near the limit of expectation, which increases safety margins or makes predictions regarding consequences more severe than if best-estimate assumptions had been made.

design basis accident (DBA)
Accident conditions against which a nuclear power plant 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.

dose acceptance criteria
Bounds for radiation doses that are established to protect workers and the public from harm due to the release of radioactive material in normal operation, anticipated operational occurrences and design basis accidents.

emergency core cooling system (ECCS)
A safety system that transfers heat from the reactor core following a loss of reactor coolant that exceeds makeup capability.

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

human error
Mistakes made in the performance of assigned tasks (i.e., some kind of deviation from the current intention and/or from an appropriate route towards some goal). It usually refers to either the omission of an action, the selection of an incorrect action for the situation or the incorrect implementation of the intended action.

human factors
Factors that influence human performance as they relate to the safety of the reactor facility, including activities during design, construction, commissioning, operation, maintenance and decommissioning phases. Examples of human factors are: organizational and management structures; policies and programs; allocation of functions to humans and machines; the design of user interfaces; staffing provisions; job-design features; work schedules; the design of procedures; training; and the physical work environment.

human performance
The outcomes of human behaviours, functions and actions in a specified environment, reflecting the ability of workers and management to meet the system's defined performance, under the conditions in which the system will be employed.

measurement uncertainty
The amount by which a measured value may not represent the actual physical value of a parameter at the time of measurement.

modelling uncertainties
Uncertainties that are associated with the models and correlations embedded in a computer code, that represent the physics of the problem, the solution scheme, data libraries and inherent deficiencies of the computer program.

normal operation
Operation of a nuclear power plant within specified operational limits and conditions, including start-up, power operation, shutting down, shutdown, maintenance, testing and refuelling.

nuclear power plant (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 (OLCs)
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.

plant parameters
Those parameters that characterize the state of the plant's SSCs, or are used to actuate a mitigating system (also referred to as operational parameters).

postulated initiating event (PIE)
An event identified in the design as leading to either an anticipated operational occurrence or accident conditions. This means that a postulated initiating event is not necessarily an accident itself; but rather it is the event that initiates a sequence that may lead to an AOO, a DBA, or a BDBA, depending on the additional failures that may occur.

probabilistic safety assessment (PSA)
A comprehensive and integrated assessment of the safety of the 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 the 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

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.

safety goal
Objective to protect reactor facility staff, the public and the environment from harm by establishing and maintaining effective defences against the release of the radiological hazards.

safety group
Assembly of structures, systems and components designated to perform all actions required for a particular postulated initiating event to ensure that the specified limits for anticipated operational occurrences and design basis accidents are not exceeded. It may include certain safety and safety support systems, and any interacting process system.

safety system
A system provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents.

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

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

single failure
A failure that results in the loss of capability of a system or component to perform its intended function(s) and any consequential failure(s) that result from it.

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
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.

Additional Information

1. Canadian Nuclear Safety Commission (CNSC), RD-337, *Design of New Nuclear Power Plants*, Ottawa, 2008.

2. CNSC, S-294, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*, Ottawa, 2005.

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

4. CNSC, G-149, *Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors*, Ottawa, 2000.

5. CNSC, RD-327, *Nuclear Criticality Safety*, Ottawa, 2010.

6. CNSC, GD-327, *Guidance for Nuclear Criticality Safety*, Ottawa, 2010.

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