Canada's Nuclear Regulator

Guidance for the Design of New Nuclear Power Plants

GD-337

September 2012

DRAFT

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Canada

Guidance for the Design of New Nuclear Power Plants
Guidance Document GD-337

© Minister of Public Works and Government Services Canada 2012
Catalogue number XXXXX
ISBN XXXXX

Published by the Canadian Nuclear Safety Commission

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

Également publié en français sous le titre de : Le document d'orientation sur la conception des nouvelles 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:

[month, year] Version 1.0

Preface

This document provides expectations and guidance on how to meet the requirements set out in regulatory document RD-337 version 2, *Design of New Nuclear Power Plants*.

This document and RD-337 version 2 represent the CNSC's adoption of the principles set forth by the International Atomic Energy Agency (IAEA) SSR 2/1, *Safety of Nuclear Power Plants: Design* (which is the revision to NS-R-1). Further guidance can be obtained from relevant Canadian codes and standards, as well as appropriate international standards, such as IAEA publications.

This document is structured in such a way that the section numbers coincide with those of RD-337 version 2. It deals with a wide variety of topics related to the design of new nuclear power plants, such as safety objectives and concepts, safety management during design, general safety expectations, system-specific expectations and safety analysis.

In this document, "shall" is used to express a requirement, i.e., a provision that a licensee or licence applicant is obliged to satisfy in order to comply with the requirements of this regulatory document. "Should" is used to express guidance, or that which is advised. "May" is used to express an option, or that which is permissible within the limits of this regulatory document. "Can" is used to express possibility or capability.

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

Table of Contents

Guidance for the Design of New Nuclear Power Plants

1.0 Purpose

This document provides expectations and guidance on how to meet the requirements set out in regulatory document RD-337 version 2, *Design of New Nuclear Power Plants*.

2.0 Scope

This document provides information on the methods and approaches considered in the design of new nuclear power plants (NPPs or plants). It deals with a wide variety of topics related to the design of new NPPs, such as safety objectives and concepts, safety management during design, general safety expectations, system-specific expectations and safety analysis.

This document and RD-337 version 2 represent the CNSC's adoption of the principles set forth by the International Atomic Energy Agency (IAEA) SSR 2/1, *Safety of Nuclear Power Plants: Design* (which is the revision to NS-R-1). Further guidance can be obtained from relevant Canadian codes and standards, as well as appropriate international standards, such as IAEA publications.

3.0 Relevant Legislation

The provisions of the *Nuclear Safety and Control Act* (NSCA) and regulations that are relevant to this guidance document include:

1. Subsection 24(4) of the NSCA prohibits the Commission from issuing, renewing, amending or replacing a licence, unless "in the opinion of the Commission, the applicant (a) is qualified to carry on the activity that the licence will authorize the licensee to carry on; and (b) will, in carrying on 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"
2. Subsection 24(5) of the NSCA authorizes the Commission to include in a licence any term or condition that the Commission considers necessary for the purposes of the NSCA
3. Paragraph 3(1)(*i*) of the *General Nuclear Safety and Control Regulations* stipulates that an application for a licence shall contain, in addition to other information, "…a description and the results of any test, analysis or calculation performed to substantiate the information included in the application"
4. Paragraph 12(1)(*f*) of the *General Nuclear Safety and Control Regulations* stipulates that every licensee shall, "…take all reasonable precautions to control the release of radioactive nuclear substances or hazardous substances within the site of the licensed activity and into the environment as a result of the licensed activity"
5. Paragraphs 3(*b*), 5(*a*), (*d*), (*e*), (*f*), (*i*) and 6(*a*), (*b*), (*h*) and 7(*f*) of the *Class I Nuclear Facilities Regulations* stipulates that an application for a licence in respect of a Class I nuclear facility, other than a licence to abandon, shall contain, in addition to other information:
   3(*b*) "plans showing the location, perimeter, areas, structures and systems of the nuclear facility"

5(*a*) "a description of the proposed design of the nuclear facility, including the manner in which the physical and environmental characteristics of the site are taken into account in the design"
5(*d*) "a description of the structures proposed to be built as part of the nuclear facility, including their design and their design characteristics"
5(*e*) "a description of the systems and equipment proposed to be installed at the nuclear facility, including their design and their design operating conditions"
5(*f*) "a preliminary safety analysis report demonstrating the adequacy of the design of the nuclear facility"
5(*i*) "the effects on the environment and the health and safety of persons that may result from the construction, operation and decommissioning of the nuclear facility"
6(*a*) "a description of the structures at the nuclear facility, including their design and their design operating conditions"
6(*b*) "a description of the systems and equipment at the nuclear facility, including their design and their design operating conditions"
6(*h*) "the effects on the environment and the health and safety of persons that may result from the operation and decommissioning of the nuclear facility"
7(*f*) "the effects on the environment and the health and safety of persons that may result from the decommissioning and the measures that will be taken to prevent or mitigate those effects"

6. Other sections of the *Class I Nuclear Facilities Regulations*, as well as sections of the *Radiation Protection Regulations* and the *Nuclear Security Regulations* that pertain to the design of a new nuclear power plant.

4.0 Safety Objectives and Concepts

4.1 General nuclear safety objective

The general nuclear safety objective adopted in RD-337 version 2 is compatible with the purpose of the NSCA, which "provides for the limitation, to a reasonable level and in a manner that is consistent with Canada's international obligations, of the risks to national security, the health and safety of persons and the environment that are associated with the development, production and use of nuclear energy and the production, possession and use of nuclear substances, prescribed equipment and prescribed information".

The general nuclear safety objective of RD-337 version 2 is derived from the IAEA Safety Series No. 110, *The Safety of Nuclear Installations,* which states that the general nuclear safety objective is "to protect individuals, society and the environment from harm by establishing and maintaining in nuclear installations effective defences against radiological hazards".

4.1.1 Radiation protection objective

The radiation protection objective of RD-337 version 2 is also derived from the IAEA document *The Safety of Nuclear Installations*, which states that the radiation protection objective is "to ensure that in all operational states radiation exposure within the installation or due to any planned release of radioactive material from the installation is kept below prescribed limits and as low as reasonable achievable, and to ensure mitigation of the radiological consequences of any accidents".

As stated in *The Safety of Nuclear Installations*, the radiation protection objective "does not preclude limited exposure of people or the release of legally authorized quantities of radioactive materials to the environment from installations in operational states. Such exposures and releases

must be strictly controlled and must be in compliance with operational limits and radiation protection standards".

4.1.2 Technical safety objectives

The technical safety objectives of RD-337 version 2 are also derived from *The Safety of Nuclear Installations,* which states that the technical safety objectives are "to take all reasonably practicable measures to prevent accidents in nuclear installations and to mitigate their consequences should they occur; to ensure with a high level of confidence that, for all possible accidents taken into account in the design of the installation, including those of very low probability, any radiological consequences would be minor and below prescribed limits; and to ensure that the likelihood of accidents with serious radiological consequences is extremely low".

4.1.3 Environmental protection objective

The environmental protection objective provides completeness in the Canadian context, to ensure the design includes adequate environmental protection provisions.

4.2 Application of the technical safety objectives

The technical safety objectives defined above establish general objectives to be met to ensure a high level of safety; however, they do not state how the achievement of such objectives should be quantitatively measured. To this end, RD-337 version 2 provides quantitative criteria and goals for nuclear power plant designs, in the form of dose acceptance criteria and safety goals.

4.2.1 Dose acceptance criteria

Deterministic safety analysis is performed to demonstrate that the dose acceptance criteria for accidents within the design basis are met with a high degree of confidence. The analysis demonstrates that the fundamental safety functions are fulfilled by the safety systems using conservative assumptions. The fundamental safety functions are described in section 6.2 of RD-337 version 2.

The values adopted in RD-337 version 2 for the dose acceptance criteria for anticipated operational occurrences (AOOs) and design basis accidents (DBAs) are consistent with accepted international practices, and take into account the recommendations of the IAEA and the International Commission on Radiological Protection.

4.2.2 Safety goals

Safety goals have been established to assist in judging the acceptability of a nuclear power plant design, using a risk-informed approach. The IAEA publication *Basic Safety Principles for Nuclear Power Plants* (75-INSAG-3 Rev. 1, INSAG-12) notes that: "The comparison of risks due to nuclear plants with other industrial risks to which people and the environment are exposed makes it necessary to use calculational models in risk analysis. To make full use of these techniques and to support implementation of the general nuclear safety objective, it is important that quantitative targets, 'safety goals', be formulated".

Qualitative safety goals

The qualitative safety goals have been established in RD-337 version 2, to ensure that members of the public are not exposed to any significant risk from the operation of a nuclear power plant, in addition to the other risks to which they are normally exposed. The achievement of these goals

is met through the application of the quantitative safety goals.

Quantitative application of the safety goals

The demonstration that the design meets the quantitative safety goals of RD-337 version 2 for core damage frequency, small release frequency, and large release frequency, is performed using probabilistic techniques.

As stated in RD-337 version 2, "*core damage frequency is a measure of the plant's accident preventative capabilities*. *Small release frequency and large release frequency are measures of the plant's accident mitigative capabilities.They also represent measures of risk to society and to the environment due to the operation of a nuclear power plant*".

The values adopted in RD-337 version 2 for the quantitative safety goals are consistent with accepted international practice for new nuclear power plants.

A comprehensive probabilistic safety assessment (PSA) considers the probability, progression and consequences of equipment failures or transient conditions, to derive numerical estimates for the safety of the plant. Core damage frequency is determined by a Level 1 PSA, which identifies and quantifies the sequence of events that may lead to significant core degradation. The small release frequency and large release frequency are determined by a Level 2 PSA, which starts from the results of a Level 1 PSA, analyses the containment behaviour, evaluates the radionuclides released from the failed fuel, and quantifies the releases to the environment.

Further details on PSAs are contained in section 9.5 of this document and CNSC S-294, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*.

4.2.3 Safety analyses

Guidance on safety analysis is contained in section 9.0 and further information is provided in CNSC RD-310, *Safety Analysis for Nuclear Power Plants* and GD-310, *Guidance on Safety Analysis for Nuclear Power Plants*.

4.2.4 Accident mitigation and management

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

4.3 Safety concepts

4.3.1 Defence in depth

Guidance can be found in IAEA INSAG-10, *Defence in Depth in Nuclear Safety*. In addition, refer to section 6.1 for additional guidance.

4.3.2 Physical barriers

Refer to section 6.1.1 for guidance.

4.3.3 Operational limits and conditions

The approaches and terminologies used for operational limits and conditions (OLCs) may vary, as a result of the practices and regulatory systems that have been established in the country of origin for the plant's design. Regardless of the approaches and terminologies used, the design authority

should provide clear definitions of the OLC terminologies used. The design should also include clear objectives and goals for the OLCs.

The information related to OLCs should list the relevant standards (national or international) used, and document how the requirements from these standards have been met.

OLCs may vary depending on nuclear reactor design, general safety philosophy, and the plant's operating configuration.

OLCs should be defined for a suitable set of bounding plant operating configurations, and be based on the approved design of the plant.

Additional information

Further information is available in:

- CSA-N290.15-2010, *Requirements for the safe operating envelope of nuclear power plants*, Canadian Standards Association, 2010
- IAEA safety guide NS-G-2.2, *Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants*, 2000

4.3.4 Interface of safety with security and safeguards

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants.* No additional guidance is provided.

5.0 Safety Management in Design

5.1 Design authority

Additional information

Further information is available in:

- IAEA safety standards series GS-G-3.5, *The Management System for Nuclear Installations Safety Guide*, 2009
- IAEA, INSAG-19, *Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life*, 2003

5.2 Design management

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

5.3 Design control measures

Design control measures, in the form of processes, procedures and practices, include:

- design initiation, specification of scope and planning
- specification of design requirements
- selection of suitably qualified and experienced staff
- work control and planning of design activities
- specification and control of design inputs
- review of design concepts and selection
- selection of design tools and computer software

- conducting conceptual analysis
- conducting detailed design and production of design documentation and records
- conducting detailed safety analysis
- defining any limiting conditions for safe operation
- carrying out design verification and validation
- independence of individuals or groups performing verifications, validations and approvals
- configuration management
- management of the design and control of design changes
- identification and control of design interfaces

CSA N286-05, *Management System Requirements for Nuclear Power Plants,* is the Canadian standard identifying management system requirements for the design, purchasing, construction, installation, commissioning, operating, and decommissioning of nuclear power plants. CSA N286.7-99, *Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants,* provides complementary requirements for analytical, scientific and design computer programs.

Organizations from nations not using the above documents should identify the codes, standards, and specifications on which their design and safety analysis control measures are based, whether national or international – such as IAEA GS-G-3.5, *The Management System for Nuclear Installations Safety Guide* and referenced publications, and ISO 9001:2008 *Quality management systems – Requirements*. Such control measures should be mapped to the requisite CSA N286-05 clauses to demonstrate that they satisfy Canadian requirements. Where gaps are identified, the measures to address them should be described.

Organizational processes and procedures can be specific to design and safety analysis, or be part of an overall management system (or quality assurance program) for other NPP lifecycle activities. In the latter case, the organization should identify those processes and procedures applicable to design and safety analysis.

There are no specific platforms, styles or format requirements for documenting design control measures; however, design organizations should identify the types of documents, the style, the format and the media (paper, electronic or Web-based) they intend to use to control their design activities.

Additional information

Further information is available in:

- CSA N286.7.1-09, *Guideline for the application of N286.7-99, Quality assurance of analytical, scientific, and design computer programs for nuclear power plants*, 2009
- IAEA GS-R-3, *The Management System for Facilities and Activities*, 2006
- Nuclear Information and Records Management Association/American National Standards Institute (NIRMA/ANSI), *Standard Configuration Management (CM),* 1.0, 2007

5.4 Proven engineering practices

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

5.5 Operational experience and safety research

As stated in RD-337 version 2, "*the NPP design shall draw on operational experience that has been gained in the nuclear industry and on the results of relevant research programs*".

The design authority should describe the major design features, changes and improvements that have been incorporated as a result of operational experience and safety research including:

- resolution of safety issues from existing reactor designs
- improvements in design due to advances in materials and their properties
- improved methods of design and safety assessment
- improved methods of construction and fabrication
- improvements in reliability, operability and maintainability
- improved methods to mitigate the occurrence and consequences of human error
- improved methods in support of the "as low as reasonably achievable" (ALARA) principle

Operational experience can be found in documents such as the IAEA yearly publication: *Operating Experience with Nuclear Power Stations in Member States*.

Additional information

Further information is available in:

- IAEA Safety Guide Series NS-G-2.11, *A System for the Feedback of Experience from Events in Nuclear Installations*, 2006

5.6 Safety assessment

A formal process should be used in conducting the safety assessment. Aspects considered in the safety assessment include:

- defence in depth provisions
- adequacy of safety margins
- multiple barriers
- safety analysis, including both deterministic and probabilistic approaches, as well as overall scope, approach, safety criteria, uncertainty and sensitivity analysis, use of computer codes, and use of operating experience
- radiation risks
- safety functions
- site characteristics
- radiation protection
- engineering aspects
- human factors
- long-term safety

As stated in RD-337 version 2*, "before the design is submitted, an independent peer review of the safety assessment shall be conducted".* The independent peer review is performed by suitably qualified and experienced individuals, different from those who carried out the safety assessment.

Additional information

Further information is available in:

- IAEA GSR Part 4, *Safety Assessment for Facilities and Activities*, 2009

5.7 Design documentation

A suite of design documentation should be developed, following the establishment of an overall baseline, listing all key design documents. Design documents should be contained in a logical and manageable framework.

Additional information

Further information is available in:

- CNSC RD/GD-369, *Licence Application Guide: Licence to Construct a Nuclear Power Plant*, 2011

6.0 Guidance on Safety Requirements

6.1 Application of defence in depth

RD-337 version 2 requires that "*defence in depth shall be achieved at the design phase through the application of design provisions specific to the five levels of defence*".

IAEA INSAG-10, *Defence in Depth in Nuclear Safety*, a report by the International Nuclear Safety Advisory Group, provides information leading to the concept and application of defence in depth.

Guidance on performing a systematic assessment of the defence in depth can be obtained from the IAEA safety reports series No. 46, *Assessment of Defence in Depth for Nuclear Power Plants*.

The application of defence in depth in the design should ensure the following:

- The approach to defence in depth used in the design should ensure that all aspects of design at the SSCs level have been covered, with emphasis on SSCs that are important to safety.
- The defence in depth should not be significantly degraded if the SSC has multiple functions (e.g., for CANDU reactors, the moderator and end-shield cooling systems may serve the functions of a process system and include the functions of mitigating design extension conditions (DECs)).
- The principle of multiple physical barriers to the release of radioactive material should be incorporated in the design; there should be a limited number of cases where there is a reduction in the number of physical barriers (as may be the case where some components carrying radioactive material serve the function of primary coolant barrier and containment), and adequate justification should exist for such design choices.
- The design (e.g., in safety design guides, management system programs) should provide:
    - levels of defence in depth that are addressed by individual SSCs
    - supporting analysis and calculation
    - evaluation of operating procedures
- The safety analysis should demonstrate that the challenges to the physical barriers do not exceed their physical capacity.

- The structure for defence in depth provisions at each level of defence should be established for a given plant design, and the evaluation of the design from the point of view of maintaining each safety function should be carried out. This evaluation should consider each and every one of the provisions for mitigation of a given challenge mechanism, and confirm that it is well founded, sufficient, feasible, and correctly engineered within the design.
- Special attention should be given to the feasibility of a given provision and the existence of supporting safety analyses. Deficiencies in the completeness of the supporting safety analyses should be documented and flagged as issues to be queried.

6.1.1 Physical barriers

The independence between all levels of defence should be achieved, in particular, through diverse provisions. The strengthening of each of these levels separately would provide, as far as reasonably achievable, an overall reinforcement of defence in depth. For example, the use of dedicated systems to deal with DECs ensures the independence of the 4th defence level.

For independent effectiveness of the different levels of defence, any design features that aim at preventing an accident should not belong to the same level of defence as the design features that aim at mitigating the consequences of the accident.

6.2 Safety functions

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

6.3 Accident prevention and plant safety characteristics

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

6.4 Radiation protection and acceptance criteria

A detailed radiation dose assessment should include estimated annual collective and individual effective and equivalent radiation doses to site personnel and members of the public for normal operation, potential radiation doses to the public for AOOs and DBAs, and potential releases into the environment for DECs.

The assessment process should be clearly documented and should include the process for consideration and evaluation of dose-reduction changes in the NPP design. This is done to ensure that doses to site personnel and members of the public are ALARA and will not exceed the applicable dose limits of the *Radiation Protection Regulations* and relevant dose acceptance criteria and safety goals in RD-337 version 2. Radiation doses resulting from the operation of the NPP should be reduced by means of engineered controls and radiation protection measures to levels such that any further expenditure on design, construction and operational measures would not be warranted by the expected reduction in radiation doses.

The radiation dose assessment process should include the expected occupancy of the NPP's radiation areas, along with estimated annual person-Sv doses associated with major functions, including radioactive waste handling, normal maintenance, special maintenance, refuelling and in-service inspection. Such assessments should include information as to how ALARA and operating experience are used in the design to deal with dose-significant contributors.

Additional information

Further information is available in:

- CNSC G-129 rev. 1, *Keeping Radiation Exposures and Doses "As Low as Reasonably Achievable (ALARA)",* 2004
- CAN/CSA-N288.2-M91 (R2008), *Guidelines for Calculating Radiation Doses to the Public from a Release of Airborne Radioactive Material under Hypothetical Accident Conditions in Nuclear Reactors*, 2008

6.5 Exclusion zone

As defined in the *Class I Nuclear Facilities Regulations*, an exclusion zone is defined as "*a parcel of land within or surrounding a nuclear facility on which there is no permanent dwelling and over which a licensee has the legal authority to exercise control*".

Historically, the exclusion zone for nuclear power plants in Canada has been defined as 914 metres from the reactor building. Rather than prescribe a particular size for the exclusion zone, RD-337 version 2 defines the factors that must be considered in establishing an appropriate size including evacuation needs, land usage needs, security requirements and environmental factors.

Evacuation needs

The design should take into account emergency response requirements based on the size of the exclusion zone and the facilities and infrastructures that are within the zone. Generally, a larger exclusion zone would require more emergency response time and capability.

The exclusion zone boundary should be defined with consideration for the capabilities of onsite and offsite emergency response. The design also considers projected changes over time in land use and population density, which could adversely affect response times, or the ability to shelter or evacuate persons from both the site itself and associated emergency planning regions.

Evacuation needs are generally based on existing provincial nuclear emergency response plans.

Land usage needs

The design should ensure that the exclusion zone is large enough to accommodate the site for the nuclear plant (accounting for the full number of units postulated to be built at the site, whether or not they would be built immediately).

The design activities should seek to optimize land usage by the plant as part of determining the exclusion zone.

Security requirements

The design should provide security requirements based on the size of the exclusion zone, the facilities and infrastructures that are within the zone, and the design of the facility. Generally, a larger exclusion zone would require more security capabilities, in order to avoid a longer response time. Physical characteristics of the site itself (which include geographical characteristics, such as proximity to elevated land) also play a role in determining these requirements.

The design authority may decide to mitigate these risks while maintaining a smaller exclusion zone, by choosing highly robust facility designs, applying engineered security measures to the site, and having a well-designed security program. These engineered measures should be described.

In establishing the radius of the exclusion zone boundary, the design should take into account:

- the site selection and threat assessment report
- facility robustness against natural and human induced external events (including malevolent acts)
- the capability of the onsite security program, along with any offsite security resources that will supplement the onsite security program

In each of the above parameters, the design should take into account projected changes over time in land use and population density, which could adversely affect that parameter. The design should be such that the exclusion zone, as established at the design stage, will be sustainable for the full lifecycle of the facility.

The acceptability of the information to be provided in support of the above is discussed in section 7.22 of this document.

Environmental factors

Environmental factors which may have an impact on the size of the exclusion zone include local meteorological conditions which could affect the radiological dose received from members of the public. The design authority may use generic site data using conservative assumptions regarding meteorological conditions in the absence of a specific site.

The *Radiation Protection Regulations* establish an effective dose limit of 1 mSv per year for members of the public. This limit implies that a hypothetical member of the public who lives at the exclusion zone boundary for 1 year (since no permanent dwelling is permitted within the exclusion zone) would not accumulate a dose of more than 1 mSv from the operation of the nuclear power plant.

The dose acceptance criteria in section 4.2.1 of RD-337 version 2 must be met at the site boundary.

Additional information

Further information is available in:

- CNSC RD-346, *Site Evaluation for New Nuclear Power Plants*, 2008

6.6 Facility layout

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

6.6.1 Multi-unit requirements

As stated in RD-337 version 2, "*the design shall take due account of challenges to a multi-unit site. Specifically, the risk associated with common-cause events affecting more than one unit at a time shall be considered*". Such events could exacerbate challenges that the plant personnel would face during an accident. The events and consequences of an accident at one unit may affect the accident progression or hamper accident management activities at the neighbouring unit; available resources (personnel, equipment and consumable resources) would need to be shared among several units.

7.0 Guidance on General Design Requirements

7.1 Classification of SSCs

The method for classifying the safety significance of SSCs important to safety should be based primarily on deterministic methodologies, complemented (where appropriate) by probabilistic methods. The safety classification of SSCs should be an iterative process that continues throughout the design process.

The SSC classification process should include the following activities:

- review and definition of postulated initiating events (PIEs)
- identification of plant-specific preventive safety features and mitigatory safety functions, based on the associated system or subsystem
- safety categorization of the preventive safety features and mitigatory safety functions, in accordance with their safety significance and role in achieving fundamental safety functions
- identification of SSCs that provide the preventive safety features and mitigatory safety functions
- assignment of SSCs to a safety class corresponding to the safety category
- SSC classification verification
- identification of engineering design rules for classified SSCs

This approach should be used for all SSCs including pressure retaining components, electrical, instrumentation and control (I&C) and civil structures.

The identified PIEs should be grouped into limiting cases, which are referred to as bounding or enveloping PIEs. Once these bounding PIEs are known and understood, the required safety functions can be identified. Each safety function can be assigned to either a preventive safety feature, or mitigatory safety function. The number of category and class may be chosen to allow for graded design rules.

As stated in RD-337 version 2, "*all SSCs shall be identified as either important or not important to safety. The criteria for determining safety importance are based on*:

1. *safety function(s) to be performed*
2. *consequence(s) of failure*
3. *probability that the SSC will be called upon to perform the safety function*
4. *the time following a PIE at which the SSC will be called upon to operate, and the expected duration of that operation"*

Redundancy and diversity could be considered to apply to factors 3 and 4 above.

The time following the PIE, as identified in factor 4, captures the need for automatic action for short timescales, or manual actions being acceptable for longer-term actions. The expected duration of the operation is also important since some systems may need to operate for months. Others (such as shutdown means) can complete their mission within seconds.

The potential severity of the consequences of a function failure should be evaluated. During the evaluation, it may be assumed that the feature or safety function to be categorized fails, and that other safety features and safety functions remain functional.

Some specific SSCs classification guidelines are given below:

- if there are SSCs whose failure cannot be accepted because the failure will result in unacceptable consequences with certainty, then these SSCs should be allocated to the highest safety class
- as a general rule, supporting SSCs should be assigned to the same class as that of the frontline SSCs to be supported
- if a particular SSC contributes to the performance of several safety functions of different categories, it should be assigned to the class corresponding to the highest safety category, requiring the most conservative design rules
- the classification of SSCs should remain the same, regardless of the operation of the SSC (whether it is active or passive, or a combination of the two)
- any SSC that is not part of a safety function group, but whose failure could adversely affect this safety function group in accomplishing its safety function (if this cannot be precluded by design) should be classified in accordance with the safety category of that safety function group
- where the safety class of connecting or interacting SSCs is not the same (including cases where one SSC belonging to a safety class is connected to another SSC not important to safety), the interference between the SSCs should be separated by a device (e.g., a physical or optical isolator) classified in the higher safety class, to ensure that the failure of a lower safety class SSC will not propagate to a higher safety class SSC

Although the probability of SSCs being called upon during DECs is very low, the failure of safety functions for the mitigation of DECs may lead to high severity consequences. Therefore, these safety functions should be considered a high safety category.

The adequacy of the safety classification should be verified using deterministic safety analysis, which should cover all PIEs and all the credited safety functions. This verification should be complemented, as appropriate, by insight from probabilistic safety assessment and by engineering judgment.

The appropriate design rules and limits as indicated in section 7.5 are specified in accordance with the safety class of SSCs.

7.2 Plant design envelope

As stated in RD-337 version 2, *"the design authority shall establish the plant design envelope, which comprises all plant states considered in the design: normal operation, AOOs, DBAs and DECs"*.

The design basis for each SSC important to safety should be systematically defined and justified. The design should also provide the necessary information for the operating organization to run the plant safely.

The conditions for deviating from conservative deterministic design principles should be clearly stated, including the basis by which such deviation would be justified on a case-by-case basis; such basis may include a more sophisticated calculation methodology, which has been well established, or a multiplicity of the ways in which a particular function can be fulfilled.

The design should adopt deterministic design principles of appropriate conservatism. For example, SSCs should be robust, tolerant of a large spectrum of faults with a gradual degradation

in their effectiveness, and should not fail catastrophically under operational states and accident conditions.

A complementary design feature is a design feature added to the design as a standalone SSC, or added capability to an existing SSC to cope with DECs.

The design principles for complementary design features to deal with DECs do not necessarily need to incorporate the same degree of conservatism as those applied to the design up to and including DBAs. However, there should be reasonable assurance that the complementary design features will function as designed when called upon.

7.3 Plant states

As shown in Figure 1 of RD-337 version 2, plant states are divided into operational states and accident conditions. The design requirements of SSCs should then be developed to ensure that the plant is capable of meeting applicable deterministic and probabilistic requirements for each plant state.

The design should include the following:

- criteria for transition to normal operation following an AOO or DBA (e.g., the safety functions are provided, and the OLC limits for the operating configurations are met)
- key parameters and characteristics for operational states, including nominal values and deviations due to uncertainties and settings of instruments, controls, trips, equipment action time, or due to process fluctuations
- permissible conditions for different operating configurations (e.g., cold and pressurized) including transient time (e.g., power level of reactor or turbine, normal planned power transient rate, heat-up and cool-down rates) for the NPP's operating life
- methods of transferring the plant between different operating configurations
- final safe configurations after AOOs, DBAs, and DECs

7.3.1 Normal operation

The design ensures that normal operations are carried out safely, thereby confirming that radiation doses to workers and members of the public, as well as any planned discharges and releases of radioactive material from the plant, will be within the authorized limits specified in the *Radiation Protection Regulations,* and will meet the requirements of section 4.1.1 of RD-337 version 2.

Operating configurations for normal operation are addressed by the OLCs which are described in section 4.3.3. These typically include:

- normal reactor startup (from shutdown, through criticality, to full-power)
- power operation, including full-power and low-power operation
- changes in reactor power, including load-follow modes (if applicable) and return to full-power after an extended period at low-power
- operation during transition between configurations such as reactor shutdown from power operation (hot shutdown, cool-down)
- refuelling during normal operation, where applicable
- shutdown in a refuelling mode or other maintenance condition that opens the reactor coolant or containment boundary

- handling of fresh and irradiated fuel

The key parameters and unique characteristics of each operational configuration, including the specific design provision for maintaining the configuration, should be identified. The permissible periods of operation at different configurations (e.g., power level) in the event of a deviation from normal operating configurations, should also be identified.

7.3.2 Anticipated operational occurrences

In accordance with the requirements of section 4.3.1 of RD-337 version 2 for Level 2 and Level 3 defence in depth, the design should include the results of the analyses of AOOs and DBAs in order to provide a demonstration of the robustness of the fault tolerance in the engineering design and the effectiveness of the safety systems. The analysis should cover the full range of events over the full range of reactor power. The analysis should also cover all normal operating configurations, including low-power and shutdown states.

For a wide range of AOOs, the design should be such that any deviations from normal operation can be detected, and that the control systems can be expected to return the plant to a safe state, normally without the activation of safety systems. For both AOOs and DBAs, there should be high confidence that qualified systems (as identified in section 5.4.4 of RD-310) can mitigate the event even when acting alone.

For each group of PIE it may be sufficient to analyze only a limited number of bounding initiating events, which can represent a bounding response for a group of events. The rationale for the choice of these selected bounding events should be provided. The plant parameters that are important to the outcome of the safety analysis should also be identified. These parameters would typically include:

- reactor power and its distribution
- core temperature
- fuel cladding oxidation, and deformation
- pressures in the primary and secondary systems
- containment parameters
- temperatures and flows
- reactivity coefficients
- reactor kinetics parameters
- reactivity worth of reactivity devices

Those characteristics of the safety systems, including the operating conditions in which the systems are actuated, the time delays, and the systems' capacity after the actuation claimed in the design, should be specified and demonstrated to be consistent with the overall functional and performance requirements of the systems.

Refer to examples of AOOs in CNSC GD-310, *Guidance on Safety Analysis for Nuclear Power Plants*.

7.3.3 Design basis accidents

The design identifies the set of DBAs and associated conditions for which the NPP is designed. This includes such responses as manual initiation of systems, or other operator actions.

Refer to examples of DBAs in CNSC GD-310, *Guidance on Safety Analysis for Nuclear Power Plants*.

7.3.4 Design extension conditions

For identifying DECs, consideration should be given to:

- factors of the accident progression (i.e., physical conditions, processes and phenomena)
- beyond design basis accident/severe accident scenarios resulting from initiating events, human actions, and SSC's operability (success or failure)
- selection of bounding events that are considered in design and determination of limiting values/ranges of the parameters of these events

The design should identify the features that are designed for use in, or that are capable of preventing or mitigating events considered in DECs. These features include complementary design features and other SSCs that may be credited for DECs. These features should:

- be independent, to the extent practicable, of those used in more frequent accidents
- have a reliability commensurate with the function that they are required to fulfill

The choice of the DECs to be analyzed should be explained and justified, indicating whether it has been made on the basis of a PSA or other analysis that identifies potential vulnerabilities of the plant.

RD-337 version 2 states *"the design shall identify a radiological and combustible gas accident source term for use in the specification of the complementary design features for DECs"*. This reference source term should be calculated for a set of representative accident scenarios based on the best-estimate models. This should take into account the uncertainties of key parameters and the possible changes in governing physical processes.

Accidents in this category are, typically, sequences involving more than one failure (unless these are taken into account in the DBAs at the design stage). Such sequences may include DBAs with degraded performance of a safety system, and sequences that could lead to containment bypass. The analysis of those accidents may:

- use best estimate models and assumptions
- take credit for realistic system action and performance beyond original intended functions, including systems not important to safety
- take credit for realistic operator actions

Where this is not possible, reasonably conservative assumptions should be made in which the uncertainties in the understanding of the physical processes being modelled are considered. The analysis should justify the approach taken.

Refer to examples of BDBAs in CNSC GD-310, *Guidance on Safety Analysis for Nuclear Power Plants*.

7.3.4.1 Severe accidents

Severe accidents represent accident conditions that involve significant fuel degradation, either in-core or in-fuel storage.

Detailed analysis should be performed and documented to identify and characterize accidents that can lead to significant core damage or offsite releases of radioactive material (severe accidents). In addition, evaluations should be carried out on the capability of complementary design features to cope with DECs. The challenges to the plant presented by such events, and the extent to which the design may be reasonably expected to mitigate their consequences should be considered in establishing the initial severe accident management guidelines which will facilitate meeting the expectations of CNSC G-306, *Severe Accident Management Programs for Nuclear Reactors*.

The design should include the analysis performed for severe accident progression and consequence evaluation including assessments on topical issues, as applicable, such as corium stratification, corium-steel-vessel thermal-chemical interaction, corium-vessel/end-shield heat transfer, hydrogen burn, steam explosion due to molten fuel-coolant interaction, and corium-concrete interaction. The results of the severe accident analysis should be taken into account when developing initial severe accident management guidelines and for emergency preparedness.

RD-337 version 2 states "*the design shall include redundant connection points (paths) to provide for water and electrical power which may be needed to support severe accident management actions"*. The redundant connection points should use standard connections and be readily accessible. They should also be physically separated, to minimize risks from common-cause events. The design should facilitate the use of equipment and supplies from onsite and offsite locations, such as fuel supply, batteries, onsite and offsite temporary pumps, generators and battery chargers.

Additional information

Further information is available in:

- CNSC G-225, *Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills*, 2001
- CNSC RD-327, *Nuclear Criticality Safety,* section 16 - Nuclear Criticality Accident Emergency Planning and Response, 2010

7.4 Postulated initiating events

The postulated initiating events (PIEs) are identified using engineering judgment and deterministic and probabilistic assessment. A justification of the extent of usage of deterministic safety analyses and probabilistic safety analyses should be provided, in order to show that all foreseeable events have been considered.

Sufficient information should be provided regarding the methods used to identify PIEs, their scope and classification. In cases where the identification methods have made use of analytical tools (e.g., master logic diagrams, hazard and operability analysis, failure modes and effect analysis), detailed information is expected to be presented.

A systematic approach to event classification should consider all internal and external events, all normal operating configurations, various plant and site conditions, and failure in other plant systems (e.g., storage for irradiated fuel, and tanks for radioactive substances).

The design should take into account failure of equipment that is not part of the NPP, if the failure has a significant impact on nuclear safety.

The scope of PIEs should be established to meet the requirements of CNSC RD-310, *Safety Analysis for Nuclear Power Plants*, and events should be classified in accordance with their anticipated frequencies, and other factors, as appropriate, in accordance with the requirements of RD-310.

The safety analysis for the identified PIEs should be performed based on guidance in section 9.0.

7.4.1 Internal hazards

The design takes into account specific loads and environmental conditions (temperature, pressure, humidity, radiation) imposed on structures or components by internal hazards.

The design takes into account the effects of pipe failures such as jet impingement forces, pipe whip, reaction forces, pressure wave forces, pressure buildup, humidity, temperature and radiation on components, building structures, electrical and I&C equipment.

The following potential initiators of flooding should be considered: leaks and breaks in pressure-retaining components, flooding by water from neighbouring buildings, spurious actuation of the fire fighting system, overfilling of tanks, and failures of isolating devices.

The design considers internal missiles which can be generated by failure of rotating components (such as turbines), or by failure of pressurized components. For those potential missiles considered to be credible, the design should include the following:

- a realistic assessment is made of the postulated missile size and energy, and its potential trajectories
- potentially impacted components associated with systems required to achieve and maintain safe shutdown are identified
- a loss of these potentially impacted components is evaluated to determine if sufficient redundancy remains to achieve and maintain a safe shutdown condition

The design takes into account loads generated by internal hazards in the environmental loading category consistent with section 7.15.

7.4.2 External hazards

The design should take into account all site characteristics that may affect the safety of the plant, and should identify the following:

- site-specific hazard evaluation for external events (of human or natural origin)
- design assumptions or values, in terms of recurrence probability of external events
- definition of the design basis for external events
- collection of site reference data for the plant design (geotechnical, seismological, hydrological, hydrogeological and meteorological)
- evaluation of the impact of the site-related issues to be considered in the application, concerning emergency preparedness and accident management
- arrangements for the monitoring of site-related parameters throughout the life of the plant

Natural external hazards other than earthquakes may be categorized as:

- hazards that have potential to damage SSCs important to safety
- hazards that are evaluated and screened out

Natural external hazards that are evaluated and screened out may be based on the following criteria:

- a phenomenon which occurs slowly or with adequate warning with respect to the time required to take appropriate protective action
- a phenomenon which in itself has no significant impact on the operation of a NPP and its design basis
- an individual phenomenon which has an extremely low probability of occurrence
- the NPP is located sufficiently distant from or above the postulated phenomenon (e.g. fire, flooding)
- a phenomenon that is already included or enveloped by design in another phenomenon. For example: storm-surge and seiche included in flooding or accidental small aircraft crash enveloped by tornado loads

Natural external hazards considered in the design include:

- earthquakes
- extreme meteorological conditions of temperature, snow, freezing rain, hail, frost, subsurface freezing and drought
- floods due to tides, tsunamis, seiches, storm surges, precipitation, waterspouts, dam forming and dam failures, snow melt, land slides into water bodies, channel changes and work in the channel
- cyclones (e.g., hurricanes, tornadoes and tropical typhoons) and straight winds
- abrasive dust and sand storms
- lightning
- volcanoes (site is sufficiently remote from volcanoes)
- biological phenomena
- collision of floating debris (e.g., ice, logs) with accessible safety-related structures, such as water intakes and ultimate heat sink (UHS) components
- geomagnetic storm (solar flare and electromagnetic pulses)
- combinations of extreme weather conditions that could reasonably be assumed to occur at the same time

Human induced hazards considered in the design include:

- aircraft crashes (general aviation)
- explosions (deflagrations and detonations) with or without fire, with or without secondary missiles, originating from offsite and onsite sources (but external to safety-related buildings), such as hazardous or pressurized materials in storage, transformers, pressure vessels or high energy rotating equipment
- release of hazardous gases (asphyxiant, toxic) from offsite and onsite storage
- release of corrosive gases and liquids from offsite and onsite storage
- release of radioactive material from offsite sources

- fire generated from offsite sources (mainly for its potential for generating smoke and toxic gases)
- collision of ships or floating debris with accessible safety-related structures, such as water intakes and UHS components
- collision of vehicles at the site with SSCs
- electromagnetic interference from off the site (e.g., from communication centres and portable phone antennas) and on the site (e.g., from the activation of high voltage electrical switchgear and from unshielded cables)
- any combination of the above, as a result of a common initiating event (such as an explosion with fire and release of hazardous gases and smoke)

Malevolent acts including aircraft crashes are considered separately, in section 7.22.

Human induced hazards which are classified as DBAs are taken into account as loads in the abnormal/extreme environmental load category, consistent with section 7.15. Less frequent human induced hazards are considered part of DECs.

Additional information

Further information is available in:

- CNSC RD-346, *Site Evaluation for New Nuclear Power Plants*, 2008
- *National Building Code of Canada* (NBCC), 2010
- American Nuclear Society (ANS) 2.3- 2011, *Estimating Tornado, Hurricane, and Extreme Straight Line Wind Characteristics at Nuclear Facility Sites*, 2011
- IAEA NS-G-3.1, *External Human Induced Events in Site Evaluation for Nuclear Power Plants*, 2002 (formerly 50-SG-S5)

7.4.3 Combination of events

Where the results of engineering judgement, deterministic safety assessments and probabilistic safety assessments indicate that combinations of events could lead to AOOs or to accident conditions, such combinations of events should be considered to be DBAs or should be included as part of DECs, depending on their likelihood of occurrence.

7.5 Design rules and limits

As stated in RD-337 version 2, "*the design authority shall specify the engineering design rules for all SSCs. These rules shall comply with appropriate accepted engineering practices*". Such SSCs should include pressure-retaining components, electrical and I&C equipment, and civil structures.

Methods to ensure a robust design must be applied, and proven engineering practices must be adhered to in the design, as a way to ensure that the fundamental safety functions would be achieved in all operational states and accident conditions.

The engineering design rules for all SSCs should be determined based on their importance to safety, as determined using the criteria in section 7.1. The design rules should include, as applicable:

- identified codes and standards
- conservative safety margins
- reliability and availability
    - material selection
    - single failure criterion
    - redundancy
    - diversity
    - independence
    - fail-safe design
- equipment qualification
    - environmental qualification
    - seismic qualification
    - electromagnetic interference (EMI)
- operational considerations
    - testability
    - inspectability
    - maintainability
    - aging
- management system

The design of complementary design features should be such that they are effective for fulfilling the actions credited in the safety analysis, with a reasonable degree of confidence. Other SSCs that are credited for DECs should also meet this expectation.

Design rules should include all relevant national and international codes and standards. In cases of SSCs for which there are no appropriate established codes or standards, an approach derived from existing codes or standards for similar SSCs may be applied; in the absence of such codes and standards, the results of experience, tests, analysis or a combination of these may be applied, and this approach should be justified.

A set of design limits consistent with the key physical parameters for each SSC important to safety for the nuclear power plant is specified for all operational states and for accident conditions. The design limits specified are consistent with relevant national and international codes and standards.

7.6 Design for reliability

The design for reliability is based on meeting applicable regulatory requirements and industry standards. The design should provide assurance that the requirements of CNSC S-98 revision 1, *Reliability Programs for Nuclear Power Plants*, will be met during operation.

The following principles are applied for SSCs important to safety:

- the plant is designed, constructed, and operated in a manner that is consistent with the assumptions and risk importance of these SSCs
- these SSCs do not degrade to an unacceptable level during plant operations
- the frequency of transients posing challenges to SSCs is minimized

- these SSCs function reliably when challenged

The SSC reliabilities assumed in the design stage need to be realistic and achievable.

Deterministic analysis or other methods may be used if the PSA lacks effective models or data.

7.6.1 Common-cause failures

7.6.1.1 Separation

Physical separation may be achieved by barriers, distance (both horizontal and vertical) or a combination of the two. For example, the design may provide elevation differences of redundant equipment to protect against flooding and to ensure water-tightness.

7.6.1.2 Diversity

The design should implement adequate diversity in safety systems, such as:

- design diversity
- equipment diversity
- functional diversity
- human diversity

The design for instrumentation and control systems (I&Cs) should also consider:

- signal diversity
- software diversity

For I&C systems important to safety, it is recommended to use an automated diverse backup system. A manual diverse backup system could be used; its justification should include a human factor engineering analysis.

The following diversity strategies should be considered:

- different technologies
- different approaches within the same technology
- different architectures within the same technology

A diversity and defence in depth analysis should be conducted, to assess design vulnerabilities to common-cause failure (CCF). If the defence in depth analysis reveals that certain safety functions could be affected by CCF, the design should provide for a diverse backup system to perform the safety functions affected by the CCF.

7.6.1.3 Independence

Means for providing independence include physical separation, functional independence and independence from the effects of data communication errors. Generally a combination of these methods should be applied, to achieve an acceptable level of independence.

Functional independence (such as electrical isolation) should be used, in order to reduce the likelihood of adverse interaction between equipment and components of redundant or connected systems, resulting from normal operation or failure of any component in the systems.

SSCs important to safety should be independent of the effects of an event to which they are required to respond. For example, an event should not cause the failure or loss of a safety system or safety function that is necessary to mitigate the consequences of that event.

Redundant portions of a safety group should be independent from each other, to ensure that the safety group can perform its safety function during (and following) any event that requires that function.

The functional failure of the support features of a safety system should not compromise the independence between redundant portions of a safety system, or between a safety system and a system of lower safety classification.

The potential for harmful interactions between those SSCs important to safety that might be required to operate simultaneously should be evaluated, and the effects of any harmful interactions should be prevented.

In the analysis of the potential for harmful interactions of SSCs important to safety, due account should be taken of physical interconnections, and of the possible effects of one system's operation, maloperation or malfunction on the local environmental conditions for other essential systems. This would ensure that changes in environmental conditions do not affect the reliability of systems or components while functioning as intended.

Additional information

Further information is available in:

- U.S. NRC NUREG/CR-6303, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*, 1994
- U.S. NRC NUREG/CR-7007, *Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems*, 2010
- U.S. NRC Branch Technical Position (BTP) 7-19, *Guidance for Evaluation of Diversity and Defense-in-Depth and in Digital Computer-Based Instrumentation and Control Systems*, 2007

7.6.2 Single failure criterion

The application of the single failure criterion (SFC) in design should follow a systematic approach applied to all safety groups. The approach should be adequately verified, such as by using failure modes and effects analysis.

As stated in RD-337 version 2*, "all safety groups shall function in the presence of a single failure".* The SSCs inside the safety group should include both the primary SSCs and the supporting SSCs.

Justification in support of an exception to the SFC should consider the consequences of failure, practicality of alternatives, added complexity and operational considerations. The integrated effect of all exceptions should not significantly degrade safety; in particular, defence in depth should be preserved.

For passive components that are exempt from the SFC, the following should be considered in order to demonstrate a high degree of performance assurance:

- adequate testing during the manufacturing stage
- sample testing from those components received from the manufacturer
- adequate testing during construction and commissioning stages
- necessary testing to verify their reliability after the components have been removed from service during the operation stage

Any consideration for an exception to the SFC during testing and maintenance should fall into one of the following permissible categories:

- the safety function is provided by two redundant, independent systems (e.g., two redundant, fully effective, independent cooling means)
- the expected duration of testing and maintenance is shorter than the time available before the function is required following an initiating event (e.g., spent fuel storage pool cooling)
- the loss of safety function is partial and unlikely to lead to significant increase in consequences even in the event of failure (e.g., small area containment isolation)
- the loss of system redundancy has minor safety significance (e.g., control room air filtering)
- the loss of system redundancy may slightly increase PIE frequency, but does not impact accident progression (e.g., leak detection)

A request for an exception during testing and maintenance should also be supported by a satisfactory reliability argument, covering the allowable outage time.

The OLCs should clearly state the allowable testing and maintenance time, along with any additional operational restrictions, such as suspension of additional testing or maintenance on a backup system for the duration of the exception.

Additional information

Further information is available in:

- IAEA Safety Series No. 50-P-1, *Application of the Single Failure Criterion*, 1990
- IEEE Standard 379-1988, *Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*, 1988

7.6.3 Fail-safe design

Knowing the failure modes of SSCs is important in applying the fail-safe concept to SSCs important to safety. An analysis, such as a failure modes and effects analysis, should be performed so as to identify the potential failure modes of SSCs important to safety.

Failures of SSCs important to safety should be detectable by periodic testing, or revealed by alarms or another reliable indication.

7.6.4 Allowance for equipment outages

If the design does not allow online maintenance or online testing for certain equipment, the design should adequately demonstrate that the equipment can maintain its reliability target between outages.

The time allowed for each equipment outage and the respective response actions should be specified in the OLCs.

7.6.5 Shared systems

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

7.7 Pressure-retaining SSCs

For the design of pressure-retaining systems and components, the design authority should ensure that the selection of codes and standards is adequate to provide confidence that plant failures are minimized. This is achieved by using industry standards – such as CSA N285.0-08, *General requirements for pressure-retaining systems and components in CANDU nuclear power plants* and *ASME Boiler and Pressure Vessel Code* – to meet the requirements of different classes of pressure-retaining systems, components, piping and their supports. Alternative codes and standards may be used, if this would result in an equivalent or superior level of safety; justifications should be provided in such cases.

The design should make provisions to limit stresses and deformation of SSCs important to safety during and after PIEs. The list of PIEs should be comprehensive, and the loads generated by them should be included in the design analysis. The loads generated by these PIEs should be included in the stress analyses required by the design.

As stated in RD-337 version 2*,* "*the design shall minimize the likelihood of flaws in pressure boundaries"*. For example, the reactor coolant pressure boundary should be designed with sufficient margin to ensure that, under all operating configurations, the material selected will behave in a non-brittle manner and minimize the probability of rapidly propagating fractures.

The pressure boundary components in a NPP almost invariably contain process fluids at very high temperature and pressure. The design should take into account the location of high-energy lines in relation to SSCs important to safety, in order to limit or reduce pipe whip concerns. This includes consideration of:

- components in the means of shutdown
- main coolant pumps
- headers
- emergency core cooling system (ECCS) piping
- steam generators
- steam lines
- turbine

Leak-before-break

A qualified leak-before-break (LBB) system design will permit the design authority to optimize protective hardware – such as pipe whip restraints and jet impingement barriers – and to redesign pipe-connected components, their supports and their internals.

A qualified LBB methodology should include the following:

- LBB should be only applied to high energy, ASME Code Class 1 or 2 piping or the equivalent. Applications to other high energy piping may be performed based on an evaluation of the proposed design and in-service inspection requirements.
- No active degradation mechanism should exist in the piping system to be qualified for LBB.
- An evaluation of phenomena such as the water hammer, creep damage, flow accelerated corrosion and fatigue should be performed to cover the entire life of the high energy piping systems. To demonstrate that water hammer is not a significant contributor to pipe rupture,

reliance on historical frequencies of water hammer events in specific piping systems coupled with reviews of operating procedures and conditions may be used for this evaluation.
- Leak detection methods for the reactor coolant should ensure that adequate detection margins exist for the postulated through-wall flaw used in the deterministic fracture mechanics evaluation. The margins should cover uncertainties in the determination of leakage from a piping system.
- Stress analyses of the piping that is considered for LBB should be in accordance with the requirements of Section III of the ASME code.
- The LBB evaluation should use design basis loads and, after construction, be updated to use the as-built piping configuration, as opposed to the design configuration.
- The methodology should take account of potential for degradation by erosion, corrosion, and erosion/cavitation due to unfavourable flow conditions and water chemistry.
- The methodology should take account of material susceptibility to corrosion, the potential for high residual stresses, and environmental conditions that could lead to degradation by stress corrosion cracking.

In addition, leak detection methods for the reactor coolant should be examined, so as to ensure that adequate detection margins exist for the postulated through-wall flaw used in the deterministic fracture mechanics evaluation.

Finite element methods

The design authority customarily uses finite element methods to show that all of the pressure boundary components (both vessels and piping) meet the structural integrity requirements imposed by applicable design codes and standards. When finite element methods are used for design analyses covering all ASME class components, the following parameters should be provided:

- finite element modelling and analysis assumptions are checked, to make sure they are judicious and conservative
- finite element mesh is properly refined, to account for geometric structural discontinuities with proper element shapes and aspect ratios
- loads and boundary conditions are correct, and properly applied in the finite element models
- load combinations and scale factors applied to unit load cases conform to design/load specifications
- linearized stress results, obtained from load combinations, are compared with ASME code allowable limits

7.8 Equipment environmental qualification

The designer should provide detailed guidance for an equipment environmental qualification (EQ) program, for qualifying safety-related equipment associated with systems that are essential to perform the credited safety functions defined in RD-337 version 2. The EQ program should address qualification criteria and methods used, and all anticipated environmental conditions upon which the qualification of the equipment (mechanical, electrical, I&C and certain post accident monitoring) is based.

The designer identifies the EQ-related standards and codes (e.g., CSA, IEEE, ASME). The latest editions of the applicable standards for use in the equipment qualification will be preferred; any deviations should be justified.

As a minimum, the basic EQ program elements should be provided as described below.

7.8.1 Identification of equipment requiring harsh environmental qualification

The design should identify:

- systems and equipment required to perform safety functions in a harsh environment, including their safety functions and applicable DBAs
- non-safety-related equipment whose failure due to harsh post-accident environment could prevent safety-related equipment from accomplishing its safety function
- accident monitoring equipment

7.8.2 Identification of equipment service conditions

Service conditions should be identified, to determine required qualification methods as they apply to various types of qualification (e.g., harsh environments, mild environments, radiation-only harsh environments).

The design should provide for:

- a distinction between mild and harsh environments (e.g., specific criteria to define plant environments as either mild or harsh)
- a list of bounding harsh DBAs for qualification of equipment
- the environmental conditions (e.g., temperature, pressure, radiation, humidity, steam, chemicals, submergence) for each applicable DBA to which equipment is exposed in various plant locations
- temperature, pressure and radiation profiles for harsh environment qualification
- typical equipment mission time during DBAs
- mild environmental conditions (e.g., temperature, pressure, humidity, radiation) for operational states, including the assumed duration of the AOOs to which equipment is exposed in various plant locations

7.8.3 Qualification methods

The design should describe methods used to demonstrate the performance of safety-related equipment when subjected to a range of environmental conditions during operational states or DBAs. The methods should determine whether equipment should be qualified for mild or harsh environments.

For harsh environment qualification, the design should include the following:

- for equipment and components located in a DBA harsh environment, type tests are the preferred method (particularly for electrical equipment) over other methods of qualification; where type tests are not feasible, justification by analysis or operating experience (or a combination of both) may be used
- equipment should be reviewed in terms of design, function, materials and environment, to identify significant aging mechanisms caused by operational and environmental conditions occurring during normal operation; where a significant aging mechanism is identified, that aging should be taken into account in the equipment qualification
- the qualification should systematically address the sequence of age conditioning, including sequential, simultaneous, synergistic effects, and the method for accelerating radiation degradation effects
- appropriate margins, as given in EQ-related standards, should be applied to the specified environmental conditions

- for certain equipment (e.g., digital I&C equipment, and new advanced analog electronics) additional environmental conditions – such as electromagnetic interference (EMI), radio frequency interference (RFI), and power surges – should be addressed

For mild environment qualification, the design should include the following:

- equipment located in a mild environment may be considered qualified, provided that the environmental conditions are specified in a design specification, and that the manufacturer provides certification that the equipment meets the specification

7.8.4 Equipment and instrumentation assessment under DECs

A demonstration of equipment and instrumentation operability should include the following:

- the functions credited in the accident timeframes that need to be performed to achieve a safe shutdown state for DECs
- the accident timeframes for each function
- the equipment type and location used to perform necessary functions in each timeframe
- the bounding harsh environment of DECs within each timeframe
- a reasonable assurance that the equipment will survive to perform its function in the accident timeframes, in the DEC environment

7.8.5 Protective barriers

The design should address protective barriers, if applicable. When protective barriers are designed to isolate equipment from possible harsh environmental conditions, the barriers themselves should be addressed in a qualification program. Examples of protective barriers include:

- steam protected rooms and enclosures
- steam doors
- water protected rooms (for flooding)

Additional information

Further information is available in:

- CSA N290.13-05, *Environmental Qualification of Equipment for CANDU Nuclear Power Plants*, 2009
- IEEE-627-2010, *IEEE Standard for Qualification of Equipment Used in Nuclear Facilities*, 2010
- IEEE-323-2003, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations*, 2003
- ASME QME-1-2002, *Qualification of Active Mechanical Equipment Used in Nuclear Power Plants*, 2002
- International Electrotechnical Commission (IEC) IEC-60780 edition 2.0, *Nuclear power plants - electrical equipment of the safety system – qualification*, 1998
- IAEA Safety Reports Series No. 3, *Equipment qualification in operational nuclear power plants: upgrading, preserving and reviewing*, 1998
- Electric Power Research Institute (EPRI) technical report, *Nuclear Power Plant Equipment Qualification Reference Manual*, Revision 1, 2010

7.9 Instrumentation and control

7.9.1 General

As indicated in RD-337 version 2, "*instrumentation for measuring variables that can affect the fission process, the integrity of the reactor core, the reactor cooling systems, and containment, as well as instrumentation for obtaining any plant information that is necessary for its reliable and safe operation"*.

Particular attention should be paid to the provision of startup instrumentation.

The monitoring should not be limited to process variables of safety and safety-related systems. It should extend to the monitoring of radiation, hydrogen, seismic, loose parts, vibration, and fatigue.

The measurements should include continuous and discrete plant variables. Detection and testing should also consider failure, degradation, unsafe conditions, deviation from specified limits, operator errors, and self-diagnosis. Correction of invalid, inauthentic and corrupted functions or data should be applied, to maintain the reliability of systems.

As stated in RD-337 version 2, "*the design shall be such that the safety systems and any necessary support systems can be reliably and independently operated, either automatically or manually, when necessary"*. There should be a bumpless transfer between automatic and manual modes.

Once safety systems are initiated, the reset of safety system functions should require separate operator actions for each system-level function. Deliberate operator action should be required to return the safety systems to normal. However, this should not prevent the use of essential equipment protective devices (such as the protection for electrical or mechanical components) or the provision for deliberate operator interventions (such as trip and isolation of the switchgear). Seal-in of safety system actuation is generally required at system or subsystem level, but not required at individual channel level.

The design should provide for the capability to record, store and display historical information, if such displays will help plant staff to identify patterns and trends, understand the past or current state of the system, perform post-accident analysis, or predict future progressions.

The design should take into account redundancy, independence, common-cause failure, interaction with other systems, and signal validation, so as to meet the reliability target.

When a safety system has been taken out of service for testing or maintenance, clear indication should be provided for the duration of testing or maintenance activities. For any safety systems being bypassed, the bypassed condition should also be clearly annunciated.

If the use of a system for testing or maintenance can impair an instrumentation and control (I&C) function, the interfaces should be subject to hardware interlocking, in order to ensure that interaction with the test or maintenance system is impossible without deliberate manual intervention.

If testing equipment is part of the safety system and stays connected when not in use for testing, the safety class of such equipment should be same as for the safety system.

The interlock systems important to safety should either reduce the probability of occurrence for specific events, or maintain safety systems in an available state, during an accident. The interlock systems should be stated and justified.

Means should be provided to automatically initiate and control all safety actions, except those for which manual action alone has been justified. Examples of situations in which manual action alone might be justified include:

- initiation of safety tasks after completion of automatic sequences
- initiation of safety actions that are not required until a considerable time after the PIE
- control actions to bring the plant to a safe state in the long-term, after an accident

The value of each input parameter used in safety system functions, the status of each trip and actuation function in each division, and the status of each system initiation, should be available to plant operators.

Additional information

Further information is available in:

- IEC 61513, *Nuclear power plants – Instrumentation and control important to safety, General requirements for systems*, 2011
- IEC 60880, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*, 2006
- IEC 60987, *Nuclear power plants – Instrumentation and control important to safety –* Hardware design requirements for computer-based systems, 2007
- IEC 60671, *Nuclear power plants – Instrumentation and control systems important safety – Surveillance testing*, 2007
- IEC 62385, *Nuclear power plants – Instrumentation and control important to safety – Methods for assessing the performance of safety system instrument channels*, 2007
- IEEE 603, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*, 2009
- IEEE 7-4.3.2, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*, 2010
- CSA N290.6-09, *Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of an Accident*, 2009
- CSA N290.14-07, *Qualification of pre-developed software for use in safety related instrumentation and control applications in nuclear power plants*, 2007

7.9.2 Use of computer-based systems or equipment

The standards and codes used for computer-based systems or equipment are identified prior to the design. The instrumentation and control development lifecycle, which implements the requirements in the standards and codes, should be coordinated with the human factors engineering (HFE) lifecycle and the cyber security lifecycle, since they have a strong influence on I&C development.

The verification and validation activities should be identified and use a top-down approach. The relationship between design and verification and validation should be indicated and the outcome of verification and validation activities should be documented. The relationship between lifecycle and verification and validation activities should be stated.

The software provided by a third-party should have the same level of qualification as for software that is written specifically for the application. The qualification of software should be verified through the national or international standards relevant to the qualification activities of pre-developed software.

The software development process should include consideration of consistency, modularity, structuredness, traceability, understandability and verifiability:

- consistency should contain uniform notations, terminology, comments, symbology, and implementation techniques
- modularity should consider that any change to one component has minimal impact on the others
- structuredness means that the design should proceed in an orderly and systematic manner (e.g., top-down design) and have minimized coupling between modules and subsystems
- traceability should provide a thread to antecedent and subsequent documents, and refer to the ability to trace the design decision history and reasons for changes
- understandability means that the development processes and outputs should be clear to a third-party
- verifiability should refer to the extent to which the development processes and outputs have been created to facilitate verification using both static methods and testing

The complete software development documentation should provide all information throughout the software development lifecycle.

7.9.3 Accident monitoring instrumentation

Instrumentation is provided to ensure that essential information is available for assessing plant conditions, monitoring safety system performance, making decisions related to plant responses to abnormal events, and predicting radioactive material releases. Instrumentation is also provided for recording vital plant parameters and variables, including:

- temperature at various locations
- pressure of containment, and primary coolant system
- level of radioactivity at various locations
- reactor vessel water level for light water reactor (LWR) or moderator level for CANDU
- containment water level
- hydrogen concentration

The design should provide the design basis, the design criteria, and display criteria for the accident monitoring parameters.

Accident monitoring instrumentation should meet performance criteria, such as measurement range, accuracy, response time, operating time and reliability target. Appropriate design analysis should be performed to confirm that the performance criteria have been met.

Accident monitoring instrumentation meets the single failure criterion (RD-337 version 2, section 7.6.2). The design should address common-cause failure at the variable level.

To the extent practicable, the same variables and displays should be used for both normal operation and accident monitoring.

The design should:

- incorporate testing capability, to verify operability requirements on a periodic basis
- facilitate maintenance, repair and calibration
- permit administrative access control to instrument channel calibration and testing

Accident monitoring instrumentation is demonstrated to be qualified to perform their required functions for the length of time when their function is required under accident conditions.

Additional information:

Further information is available in:

- IEEE 497-2010 - *IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations*, 2010
- CSA N290.6-09, *Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of an Accident*, 2009

7.10 Safety support systems

The design basis for any compressed air system that serves an item important to safety at the nuclear power plant should specify the quality, flow rate and cleanness of the air to be provided.

Systems for air conditioning, air heating, air cooling and ventilation should be provided (as appropriate) in auxiliary rooms or other areas at the nuclear power plant, so as to maintain the required environmental conditions for systems and components important to safety, in all plant states.

As stated in RD-337 version 2*, "the emergency support systems shall support continuity of the fundamental safety functions until long term (normal or backup) service is re-established*

- *without the need for operator action to connect temporary onsite services for at least 8 hours*
- *without the need for offsite services and support for at least 72 hours".*

Pre-installed equipment can be credited after 30 minutes where only control room actions are needed or after 1 hour if field actions are needed. These actions should be limited to operating valves, starting pumps, etc. Guidance is provided in section 8.10.4 for justification of such actions.

If equipment is not pre-installed, but is stored on site, it can normally be credited after 8 hours. However, this must be justified based on an assessment of the actions required and the availability of procedures and training to support those actions. It is possible that longer times may be necessary for complex actions. Equipment or supplies stored offsite or support staff from offsite should not normally be credited for 72 hours. Again, the value used should be justified and may be longer.

Guidance on redundant connection points for temporary services is described in section 7.3.4.

7.11 Guaranteed shutdown state

A guaranteed shutdown state (GSS) is one for which the reactor will remain in a stable, sub-critical state, independent of any perturbation reactivity effect produced by any change in core configuration, core properties, or process system failure.

The design should describe the GSSs that are expected to be used over the life of the facility, including steps for GSS placement, removal and restart, and functional tests to be performed.

7.12 Fire safety

7.12.1 General provisions

Effective fire protection is achieved by:

- fire protection features such as programs and procedures, fire prevention, fire detection, fire warning, emergency communication, fire by-product management, fire suppression and fire containment, non-combustible construction, seismic and environmental qualification of fire protection equipment
- the use of physical barriers to segregate redundant SSCs important to safety

The design should address protection from fire by demonstrating that a defence in depth approach has been implemented. Supporting documents are expected to include a comprehensive design report, code compliance review, a fire hazard assessment, fire safe shutdown analysis, and a fire protection program.

An independent third-party review of the design assessing compliance against the applicable fire codes and standards used in the design for protection from fires and explosions should be performed. The review should provide a definitive statement that the design conforms to the identified codes and standards, meets good engineering practices, and achieves fire protection objectives.

The design should comply with the requirements of the following codes and standards:

- Canadian Commission on Building and Fire Codes, *National Building Code of Canada* (NBCC), 2010
- CSA N293-07, *Fire Protection for CANDU Nuclear Power Plants*, 2007
- National Research Council, *National Fire Code of Canada* (NFCC), 2010

Although CSA N293-07 is considered acceptable to provide technology-neutral design criteria, it does not fully address some fire safety aspects, such as:

- operator-initiated manual actions
- associated fire safe shutdown circuit analysis
- multiple spurious operations

Guidance on the above fire safety aspects is provided in:

- U.S. NRC NUREG-1852, *Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire*, 2007
- Nuclear Energy Institute NEI 00-01, *Guidance for Post-Fire Safe Shutdown Circuit Analysis*, 2005
- U.S. NRC SECY-08-0093, *Resolution of Issues Related to Fire-Induced Circuit Failures*, 2008

Additional information

Further information is available in:

- NEI 04-02, Revision 1, *Guidance for Implementing a Risk-Informed, Performance-Based Fire Protection Program under 10 CFR 50.48(c)*, 2005
- National Fire Protection Association (NFPA) NFPA 804, *Standard for Fire Protection for Advanced Light Water Reactor Electric Generating Plants*, 2010
- NFPA 805, *Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants*, 2010
- NFPA *Fire Protection Handbook*, 2008
- Society of Fire Protection Engineers, *SFPE Handbook of Fire Protection Engineering*, 2008
- IAEA NS-G-1.7, *Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants*, 2004
- IAEA NS-G-2.1, *Fire Safety in Operation of Nuclear Power Plants*, 2000
- IAEA Safety Report Series No. 8, *Preparation of Fire Hazard Analysis for Nuclear Power Plants*, 1998
- U.S. NRC NUREG/CR-6850, EPRI 1011989 *Fire Probabilistic Risk Assessment Methods Enhancements*, 2010
- U.S. NRC NUREG-0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR edition - Fire Protection Program*, section 9.5.1.1, 2009
- U.S. NRC Regulatory Guide 1.189, *Fire Protection for Operating Nuclear Power Plants*, 2001

7.12.2 Safety to life

The National Building Code of Canada (NBCC) is an objective-based national model code. The provisions of the NBCC are considered the minimum acceptable measures for meeting the objectives of safety, health, structural protection, and fire protection of buildings. As such, additional fire protection measures may be required to meet the regulatory requirements detailed in RD-337 version 2. Additional fire safety provisions are usually assessed and documented in the code compliance and fire hazard assessment, as required by CSA N293-07, *Fire Protection for CANDU Nuclear Power Plants*.

7.12.3 Environmental protection and nuclear safety

As indicated in section 7.12.2, the *National Building Code of Canada* and the *National Fire Code of Canada* (NFCC) cover the minimum fire safety and fire protection features that must be incorporated at the time of building design and construction. Additional fire protection measures may be required to meet the regulatory requirements detailed in section 7.12.3 of RD-337 version 2. Additional fire safety provisions are usually assessed and documented in the code compliance, fire hazard assessment and fire safe shutdown analysis, as required by CSA N293-07.

7.13 Seismic qualification

7.13.1 Seismic design and classification

The seismic design of a NPP should account for:

- technical safety objectives and corresponding load categories
- seismic input motion
- seismic classification

- structural layout criteria
- seismic analysis and design of structural systems, subsystems and equipment
- seismic testing and instrumentation

Design and beyond design load categories are defined to demonstrate structural performance in operational states and accident conditions. Earthquake load is not part of the normal load category corresponding to normal operation. Site design earthquake load, according to the CSA N289 series on seismic design and qualification, is defined under the severe load category corresponding to AOO. Design basis earthquake is defined as a part of the abnormal/extreme load category corresponding to DBA. Beyond design basis earthquake load should be considered under DECs.

Seismic input motion, derived from the design basis earthquake, should be based on seismicity and geologic conditions at the site and expressed in such a manner that it can be applied for the qualification of SSCs. Design basis earthquake response spectrum should be defined taking into account a design factor applied to a mean uniform hazard spectrum (with a probability of occurrence of 10^{-4}/yr as defined in the standard ASCE 43-05, *Seismic Design Criteria for Structures, Systems and Components in Nuclear Facilities*). (The probability of occurrence of the loading thus defined is equivalent to the probability of the loading due to DBAs). A minimum seismic input motion, consistent with national or international standards, should be considered in the design phase for the design basis earthquake. The minimum seismic input motion should take into account frequencies of interest for SSCs.

Structural layout criteria, including structural separation, should follow best engineering practices and lessons learned from past earthquakes.

Modelling of soil-structure interaction (SSI) should be based on geotechnical investigation and taking into account the random nature of soil material properties and inherent uncertainties incorporated in soil constitutive models used in the analysis. To account for uncertainties in soil properties a range with at least three values (upper limit, best estimate and lower limit) should be taken into account in the analysis according to CSA N289.3-10, *Design procedures for seismic qualification of nuclear power plants,* clause 5.2.2.

The analysis of SSI should take into account all effects due to kinematic interaction (effect of applied seismic ground motion on massless structure) and inertial interaction (inertial forces developed in the structure due to the seismic ground motion). The detail and sophistication of soil-structure models should be in accordance with the purposes of the analyses. The frequency range of interest determines aspects of the structure model and the SSI model parameters.

The frequency range of interest should be based on the combination of the frequency range of the earthquake input, the soil properties, the frequency range of building response (including response of subsystems modelled in the main building or structure model), and the frequency range of the response parameter of interest. Refined finite element meshes and increased analytical rigor are required to transmit higher frequencies through the analytical models.

Damping ratios for structural systems and sub-systems should be taken into account according to ASCE 43-05. For generating the in-structure response spectra to be used as input to the structure mounted systems and components, Response Level 1 damping of the structure is more appropriate unless the structure response generally exceeds demand over capacity factor given in ASCE 43-05.

The seismic design of structural systems should be according to seismic design category (SDC) 1 to 5 as per ASCE 43-05.

SDC 1 and 2 structural systems should be in accordance with *National Building Code of Canada,* Division B, Part 4. According to the Code, SDC 1 should be as normal and SDC 2 as post-disaster.

All structures important to safety are classified as SDC 5. However, the designer may still classify some structures as SDC 3, 4 and 5 provided that they include proper justification. Guidance on SDC 3, 4 and 5 (if SDC 3 and 4 are used) structural systems are provided as follows:

- for concrete containment, the design should be based on the American Society of Civil Engineers, ASCE 43-05 (SDC 5, limit state D) and CSA N287.3-93, *Design Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants*
- for steel containment, the design should be based on ASCE 43-05 (SDC 5), 2010 *ASME Boiler and Pressure Vessel Code*, Section III: Rules for Construction of Nuclear Power Plant Components, Division 1, Subsection NE: Class MC Components and U.S. NRC Regulatory Guide 1.57, *Design Limits and Loading Combinations for Metal Primary Reactor Containment System Components*
- for concrete and steel safety related structures the design should be based on ASCE 43-05 (SDC 5, limit state D) and CSA N291-08, *Requirements for Safety-Related Structures for CANDU Nuclear Power Plants*

For all safety design categories in a NPP, ductility requirements should be in accordance with CSA-A23.3-04 (R2010), *Design of Concrete Structures* for concrete structures and CSA S16-09, *Design of Steel Structures* for steel structures assuming that the structures are ductile or type D. These ductility requirements should provide margins for the beyond design basis earthquake.

Sub-system analysis should follow the guidance presented for structural systems with the following criteria specific to sub-system supports:

- in-structure response spectra
- in-structure time response histories

The methods of defining in-structure response spectra or in-structure time-histories as well as application of this seismic input to sub-systems and components should be in accordance with ASCE 04, *Seismic Analysis for Safety-Related Nuclear Structures*.

Multiple support seismic input of sub-systems and components should take into account their inertial and kinematic components. The analysis should follow ASCE 04 or CSA N289.3-10, *Design procedures for seismic qualification of nuclear power plants.*

Determination of the number of earthquake cycles for sub-system analysis should be in accordance with U.S. NRC NUREG-0800, Standard Review Plan, section 3.7.3, *Seismic Subsystem Analysis* as well as seismic analysis of above-ground tanks.

Seismic design of sub-systems and components should be in accordance with ASCE 43-05 section 8.2.3 which follows ASME Code.

For equipment qualified by testing, multi-axis, multi-frequency testing is acceptable for the design basis earthquake in accordance with the requirement of IEEE 344-2004 – *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations* and that the testing response spectrum should be at least a factor of 1.4 times the required response spectrum throughout the frequency range. Any deviation from this should be conservatively justified on a case by case basis.

Any evaluation for beyond design basis earthquake should utilize the methodology in the Electrical Power Research Institute, (EPRI) TR-103959, *Methodology for Developing Seismic Fragilities* to determine if a high confidence low probability of failure (HCLPF) goal is met.

Seismic instrumentation design should follow CSA-N289.5-M91 (R2008) *Seismic*, *Instrumentation Requirements for CANDU Nuclear Power Plants* which itemizes the requirements for single and multi-unit site seismic instrumentation.

Beyond design basis margin should be such that seismically induced SSC failure probabilities do not contribute to the total core damage frequency and small and large release frequency to the extent that they do not meet the safety goals. The acceptance criteria for beyond design basis earthquake should be:

- a plant level HCLPF being at least 1.67 times the design basis earthquake
- the containment integrity in the case of beyond design basis earthquake

Assessment and validation of margins for beyond design basis earthquake should be considered, including the metric HCLPF.

The seismic isolation of SSCs is an acceptable design approach to limit seismic demand. Seismic isolation devices should be designed, manufactured and installed to withstand a seismic action defined by a design basis earthquake without any failure, preserving its mechanical resistance and full load bearing capacity during and after the earthquake. Moreover, the devices and the whole structural system should be designed to withstand beyond design basis earthquake up to 2 times the spectral accelerations of the design basis earthquake without major damages and preserving its function (without experiencing cliff-edge effect). It includes the provisions to accommodate the structural displacements up to 2 times the displacements under design basis earthquake conditions.

Additional information

Further information is available in:

- CSA N289 series on seismic design and qualification of CANDU nuclear power plants
- *National Building Code of Canada* (NBCC), 2010
- CSA A23.3-04 (2010), *Design of Concrete Structures*, 2010
- CSA S16-09, *Design of Steel Structures,* 2009
- CSA N287 series on requirements for concrete containment structures for CANDU nuclear power plants
- CSA N291-08, *Requirements for Safety-Related Structures for CANDU Nuclear Power Plants*, 2008
- American Society of Civil Engineers (ASCE)/SEI 43-05, *Seismic Design Criteria for Structures, Systems and Components in Nuclear Facilities*, 2005
- American National Standards Institute (ANSI)/American Nuclear Society (ANS) Standard 2.26, *Categorization of Nuclear Facility Structures, Systems, and Components for Seismic Design*, Reaffirmed 2010
- ASCE 04-98, *Seismic Analysis of Safety-Related Nuclear Structures*, 2000
- American Society of Mechanical Engineers (ASME) BPV Code Section III, Division 1-Subsection NE *Rules for Construction of Nuclear Facility Components*, 2010
- U.S. NRC, Regulatory Guide 1.57, *Design Limits and Loading Combinations for Metal Primary Reactor Containment System Components*, 2007
- U.S. NRC Regulatory Guide 1.91, *Evaluations of Explosions Postulated to Occur on Transportation Routes Near Nuclear Power Plants*, 1978

- U.S. NRC, NUREG-0800, section 3.7.3, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*: LWR edition- Seismic Subsystem Analysis, 2007
- Institute of Electrical and Electronics Engineers, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*, IEEE 344-2004
- Electric Power Research Institute, *Methodology for Developing Seismic Fragilities*, TR-103959, 1994
- European Standard EN 1337-3, *Structural Bearings – Elastomeric Bearings*, 2000
- European Standard EN 1337-1, *Structural Bearings – General Design Rules*, 2000
- European Standard EN 15129, *Anti-seismic Devices*, 2009

7.14 In-service testing, maintenance, repair, inspection and monitoring

While in-service testing, maintenance, repair, inspection and monitoring take place primarily during the operating phase of the plant's lifecycle, the NPP is designed to permit the effective implementation of these activities during operation. In particular, the reactor core should be designed to permit the implementation of a material surveillance program to monitor the effects of service conditions on material properties throughout the operating life of the reactor.

The design should establish a technical basis of SSCs that require in-service testing, maintenance, repair, inspection and monitoring.

The development of strategies and programs to address in-service testing, maintenance, repair, inspection and monitoring is a necessary aspect of the plant design phase. The strategies and programs that will be implemented for these in-service activities should be developed so as to ensure that plant SSCs remain capable and available to perform their safety functions. The design should incorporate provisions recognizing the need for in-service testing, maintenance, repair, inspection and monitoring, as well as to permit the repair, replacement and modification of those SSCs likely to require such actions, due to anticipated operating conditions. In addition, activities which need to be carried out during the construction and commissioning phases should be identified, in order to provide a meaningful baseline data of the plant, at the outset of its operating life.

The strategies should include well-planned and effective programs for evaluating and trending SSCs performance, coupled with an optimized preventive maintenance program.

The strategies and programs should demonstrate consideration of the following:

- the intended design life, design loading conditions, operational requirements and safety significance of SSCs
- the requirements of applicable codes, standards and regulations
- the responsibilities of the designer, vendor, constructor, operating organization and contractors
- interdependence of SSCs important to safety and possible effects of failures of SSCs of lower safety significance on SSCs of higher safety significance
- plant design, layout and the accessibility of SSCs during construction, commissioning, and during the intended service life
- monitoring, inspection and testing programs used during the construction, commissioning and service for NPPs of similar or identical design and layout
- technologies and methodologies available for monitoring, inspection and testing, as well as for the repair, replacement and/or modification of SSCs
- research and development activities
- operating experience

- human factors
- training and qualification of personnel
- availability of adequately trained and qualified personnel
- availability of required laboratory or testing facilities and equipment

If risk informed in-service inspection methodologies are used when defining the scope of an inspection program, the methodology should be clearly documented.

SSCs important to safety should be designed and located to make surveillance and maintenance simple, to permit timely access, and in case of failure, to allow diagnosis and repair, and minimize risks to maintenance personnel.

Means provided for the maintenance of SSCs important to safety should be designed such that the effects on the plant safety are acceptable.

Additional information

Further information is available in:

- CSA N285.4-09, *Periodic inspection of CANDU nuclear power plant components*, 2009
- CSA N285.5-08, *Periodic inspection of CANDU nuclear power plant containment components*, 2008
- CSA N287.7-08, *In-service examination and testing requirements for concrete containment structures for CANDU nuclear power plants*, 2008
- CSA N291-08, *Requirements for safety-related structures for CANDU nuclear power plants*, 2008
- CNSC S-210, *Maintenance Programs for Nuclear Power Plants*, 2007
- CNSC RD-334, *Aging Management for Nuclear Power Plants*, 2011
- ASME *Boiler and Pressure Vessel Code-2010*, Section XI, *Rules for Inservice Inspection of Nuclear Power Plants*, 2010
- IAEA Safety Guide NS-G-2.6, *Maintenance, Surveillance and In-Service Inspection in Nuclear Power Plants,* 2002

7.15 Civil structures

This guidance covers the design of all the safety related structures including containment structures in the NPP.

7.15.1 Design

The design authority should provide the design principles, design basis requirements and criteria, and applicable codes and standards, design and analysis procedures, the assumed boundary conditions and the computer codes used in the analysis and design.

All internal and external hazard loads and their criteria are specified in section 7.4. Earthquake design input loads and malevolent act impacts including large aircraft crash can be found in section 7.13 and 7.22, respectively.

The design authority should demonstrate achievement of safety objectives by conducting a comprehensive hazard analysis in operational states and accident conditions.

Load categories corresponding to the plant states are defined in this section so as to demonstrate structural performances as follows:

- normal condition loads which are expected during the assumed design life of the NPP
- AOO loads (or severe environmental loads)
- DBA loads (or abnormal/extreme environmental loads
- DEC loads (or beyond design loads)

The design should identify all DEC loads considered in the structure design and provide the assessment methodology and acceptance criteria.

The structural design should consider the aging impact on the structure and its material.

The design should demonstrate sufficient safety margins for the buildings and structures that are important to safety.

The physical and material description of each civil structure and its base slab should include:

- the type of structure, and its structural and functional characteristics
- the geometry of the structures, including sketches showing plan view at various elevations and sections (at least two orthogonal directions)
- the relationship between adjacent structures, including any separation or structural ties
- the type of base slab and its arrangement with the methods of transferring horizontal shears (such as those seismically induced) to the foundation media

Containment structure

The design should specify the safety requirements for the containment building or system, including, for example, its structural strength, leak tightness, and resistance to steady-state and transient loads (such as those arising from pressure, temperature, radiation, and mechanical impact) that could be caused by postulated internal and external events. In addition, the design should specify the safety requirements and design features for the containment internal structures, (such as the reactor vault structure, the shielding doors, the airlocks, and the access control and facilities).

The design of the containment structure should include:

- base slab and sub-base
- containment wall and dome design
- containment wall openings and penetrations
- pre-stressing system
- containment liner and its attachment method

The design pressure of containment building should be determined by increasing by at least 10% the peak pressure that would be generated by the DBA (refer to clause 4.49 of IAEA NS-G-1.10, *Design of Reactor Containment Systems for Nuclear Power Plants*).

Ultimate internal pressure capacity should be provided for the containment building structures including containment penetrations.

If the containment building foundation is the common mat slab which is not separated with the other buildings foundation, the impact should be evaluated.

Concrete containment structures should be designed and constructed in accordance with CSA N287 series, as applicable:

- N287.1 for general requirements in documentation of design specification and design reports
- N287.2 for material
- N287.3 for design
- N287.4 and N287.5 for containment construction and inspection
- N287.6 for pressure test before operation

Steel containment structures should be designed according to the ASME *Boiler and Pressure Vessel Code*, Section III, Division 1, Subsection NE, Class MC Components or equability. Stability of the containment vessel and appurtenances should be evaluated using ASME Code, Case N-284-1, metal containment shell buckling design methods, Class MC, Section III, Division 1.

For other requirements on the design of containment structures, refer to section 8.6.2 of RD-337 version 2.

Safety-related structures

The safety-related structures other than the containment should be designed and constructed in accordance with CSA N291-08, *Requirements for safety-related structures for CANDU nuclear power plants*.

The design of other safety-related structures should include:

- internal structures of reactor building
- service (auxiliary) building
- fuel storage building
- control building
- diesel generator structures
- containment shield building, if applicable
- other safety-related structures defined by the design
- turbine building (for boiling water reactor)

Additional information

Further information is available in:

- ACI 349-06, *Code Requirements for Nuclear Safety-Related Concrete Structures & Commentary*, American Concrete Institute, 2007
- IAEA safety guide NS-G-1.10, *Design of Reactor Containment Systems for Nuclear Power Plants*, 2004
- ASME BPVC Section III, Division 2, Section 3, *Code for Concrete Containments*, 2010
- U.S. NRC NUREG-0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Concrete Containment*, Section 3.8.1, 2007
- U.S. NRC Regulatory Guide 1.76, *Design Basis Tornado and Tornado Missiles for Nuclear Power Plants*, 2007
- U.S. NRC Regulatory Guide 1.91, *Evaluations of Explosions Postulated to occur on Transportation Routes near Nuclear Power Plants*, 1978
- U.S. NRC NUREG/CR-6486, *Assessment of Modular Construction for Safety-Related Structures at Advanced Nuclear Power Plants*, 1997

7.15.2 Surveillance

For concrete containments, it is important to accommodate the structural integrity inspection and pressure testing for pre-operational and in-service phases. The inspection and pressure testing programs should be provided and meet the applicable requirements listed in CSA N287.6-11, *Pre-operational proof and leakage rate testing requirements for concrete containment structures for nuclear power plants,* and CSA N287.7-08, *In-service examination and testing requirements for concrete containment structures for CANDU nuclear power plants*.

Special design provisions should be provided to accommodate in-service inspection and pressure testing of concrete containments (e.g., providing sufficient physical access, providing alternative means for identification of conditions in inaccessible areas that can lead to degradation, or providing remote visual monitoring of high-radiation areas). Programs should be implemented for the examination of inaccessible areas, monitoring of ground water chemistry, and monitoring of settlements and differential displacements. The design should also provide for equipment and instrumentations, for example a strain gauge, to monitor stress, strain and any deformation of the structures.

7.15.3 Lifting of large loads

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

7.16 Construction and commissioning

Due account should be taken of relevant experience that has been gained in the construction and commissioning of other similar plants and their associated SSCs. Where best practices from other relevant industries are adopted, such practices should be shown to be appropriate to the specific nuclear application.

The design should include preliminary plant commissioning requirements for both pre-operational and initial startup tests:

- Pre-operational tests consist of those tests conducted following completion of construction and construction-related inspections and tests, but before fuel loading. Such tests demonstrate, to the extent practicable, the capability of SSCs to meet performance requirements and design criteria.
- Initial startup tests include those test activities scheduled to be performed during and following fuel-loading. Testing activities include fuel loading, pre-critical tests, initial criticality, low-power tests, and power ascension tests, which should confirm the design bases and demonstrate, to the extent practicable, that the plant will operate in accordance with its design and is capable of responding as designed to AOOs and accident conditions.

The design authority should provide general guidance to control commissioning activities, including administrative controls that will be used to develop, review and approve individual test procedures, coordination with organizations involved in the test program, participation of plant operational and technical staff, and the review, evaluation and approval of test results.

The design should include general guidance about how (and to what extent) the test program will use and test the plant's operating, surveillance and emergency procedures.

The design should include test abstracts of SSCs and unique design features, which will be tested to verify that SSCs performance is in accordance with the design. These test abstracts should

include the objectives, pre-requisites, test methods, and acceptance criteria that will be included in the test procedures.

The design should include the acceptance criteria of commissioning activities that are necessary and sufficient to provide reasonable assurance that, if these commissioning activities are performed and the acceptance criteria met, the as-built facility will conform to the approved plant design and applicable regulations.

The scope of the acceptance criteria should be consistent with the SSCs that are in the design descriptions. In general, each system should have sufficient acceptance criteria that verify the information in the design descriptions. The level of detail specified in the acceptance criteria should be commensurate with the safety significance of the functions and bases for that SSC.

The acceptance criteria should be objective and unambiguous, match the design commitments, and be able to be verified by adequate inspections, tests, and analyses during the construction and commissioning stages.

Additional information

Further information is available in:

- IAEA SSR 2/2, *Safety of Nuclear Power Plants: Commissioning and Operation*, 2011
- IAEA Safety Standards Series No. NS-G-2.9, *Commissioning for Nuclear Power Plants*, 2003
- U.S. NRC NUREG-0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition – Initial Test Program and ITAAC – Design Certification*, chapter 14, 2007

7.17 Aging and wear

In addition to RD-337 version 2, further requirements for aging and wear are provided in CNSC RD-334, *Aging Management for Nuclear Power Plants*.

The design should also consider the following:

- identification of all SSCs subject to aging management
- use of advanced materials with greater aging resistant properties
- need for materials testing programs to monitor aging degradation
- need to incorporate online monitoring, particularly where this technology would provide forewarning of degradation leading to failure of SSCs, and where the consequences of failure could be significant to safety

7.18 Control of foreign material

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

7.19 Transport and packaging for fuel and radioactive waste

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

7.20 Escape routes and means of communication

Additional information

Further information is available in:

- Canadian Commission on Building and Fire Codes, *National Building Code of Canada* (NBCC), 2010
- CSA N293-07, *Fire Protection for CANDU Nuclear Power Plants*, 2007
- National Research Council, *National Fire Code of Canada* (NFCC), 2010
- IAEA GS-R-2, *Preparedness and Response for a Nuclear or Radiological Emergency*, 2002

7.21 Human factors

This section applies to the design of all plant systems where there are human factors (HF) considerations. Human factors means "factors that influence human performance", as defined in CNSC P-119 *Policy on Human Factors*. In practice, it is expected that most plant systems will require some consideration of HF.

The systematic approaches and processes taken for HF in design should meet international standards and good practices. HF codes and standards that are used by the design authority for the plant design should be identified and evaluated for their suitability, applicability, sufficiency and adequacy.

There should be sufficient authority in the management of HF in design to ensure that HF considerations that influence safety are adequately taken into account. HF design requirements that will supplement the codes (e.g., concerning usability and human performance) should also be identified and specified early in the design stage process.

The following areas should have interfaces with HF in design:

- engineering design of specific SSCs
- procedure development
- training development
- consideration of human actions in safety analyses
- specifications of staffing and minimum shift complement

The design expectations are provided below for use in different design stages.

Planning

A human factors engineering program plan (HFEPP) demonstrates how HF considerations are incorporated into the design activities. Further guidance on how to develop such a plan is provided in the CNSC G-276 *Human Factors Engineering Program Plans* and U.S. NRC NUREG-0711, Revision 2, *Human Factors Engineering Program Review Model*. The technical elements described in the plan should be supported by subsequent verification and validation activities for the resulting design, as described in CNSC G-278 *Human Factors Verification and Validation Plans*.

The HF in design activities is effectively integrated in the overall engineering design process and incorporated early enough to make an effective contribution to safety. There should be a sufficient number of trained, qualified and experienced HF specialists to carry out the HF in design activities.

Analysis

Systematic analytical approaches are used to establish the HF inputs. Such analyses should be conducted from the earliest stages of design, to provide a strong foundation upon which the design solutions are based. The specific HF analyses should be:

- appropriate to the activities in question that they cover, considering the risk of the activities and the novelty of the design
- carried out throughout the development of the design
- use methods, techniques, and good practices that are considered acceptable by trained and experienced human factors specialists
- share the information produced between groups engaged in different parts of the design

The HF analyses could include:

- function analysis
- task analysis
- human reliability analysis
- hazard analysis
- link analysis
- information requirements analysis
- staffing analysis
- usability analysis
- operability and maintainability analysis

The design should also provide research or study reports for any work carried out as part of the process of developing and testing any new human-system interface technologies (i.e., displays and controls) that are new to NPP applications and that may have a bearing on safety.

The design should demonstrate that steps have been taken in developing the design to reduce or eliminate, where practicable, the potential for human error; that there are acceptable means by which to identify error; that methods are provided by which to recover from the error; and that the consequences of error can be mitigated.

Design

There should be evidence that a systematic process exists for the design of work areas, work environments, and human-system interfaces for SSCs throughout the plant. The design should demonstrate consideration of HF issues for all aspects of the plant, not just control areas. HF aspects should be considered where off-the-shelf SSCs are specified and procured. Operating experience concerning HF issues gained from existing or similar systems should be considered in the design.

A significant aspect of this systematic process is the use of modern human factors codes, standards, and good practices in developing the design. Guidance is provided in U.S. NRC NUREG-0700 Revision 2, *Human-System Interface Design Review Guidelines*.

The design should demonstrate that operators (and any other potential users) in the main control room, the secondary control room, the emergency support centre, and in the plant, are provided with the necessary and appropriate information in a format that is compatible with necessary decision and action times. The same kind of considerations should apply to other users of equipment (e.g., maintainers and technicians) elsewhere in the plant.

Operating personnel

Personnel who have operating experience from similar plants should be actively involved in the design process, to ensure that consideration is given, as early as possible to the future operation and maintenance of the SSCs.

Formal interfaces should be defined between the HF in design group(s) and the various design engineering groups involved in the design process; this facilitates the interactions and sharing of information to achieve good integration of HF considerations in the design.

Verification and validation

Evaluations are an essential part of HF in the design process and include both verification and validation activities. Evaluation criteria (i.e., design requirements and standards) should be established prior to conducting these evaluations.

HF verification activities should be carried out (generally by vendor and licensee) to confirm that the design conforms to HF design standards and has been implemented as intended in the plant.

Validations should be carried out iteratively at various stages of the design process, ensuring that the task fidelity is appropriate. Data from the validation activities should be analysed and the results should be used to improve the design. Validation should confirm that the system, including the human components and procedures to support the tasks, meets the specified system and usability requirements. Validations should also demonstrate that operations and maintenance personnel can successfully carry out their tasks in a safe manner.

Guidance on evaluations is provided in CNSC G-278, *Human Factors Verification and Validation Plans*, and U.S. NRC NUREG-6393, *Integrated System Validation: Methodology and Review Criteria.*

Additional information

Further information is available in:

- CNSC P-119, *Policy on Human Factors*, 2000
- CNSC G-276, *Human Factors Engineering Program Plans*, 2003
- CNSC G-278, *Human Factors Verification and Validation Plans*, 2003
- CNSC G-323, *Ensuring the Presence of Sufficient Qualified Staff at Class I Nuclear Facilities – Minimum Staff Complement*, 2007

- CSA N290.6-09, *Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of an Accident*, 2009
- CSA N290.4-11, *Requirements for Reactor Control Systems of Nuclear Power Plants*, 2011
- IEC 61839, *Nuclear Power Plants – Design of Control Rooms – Functional Analysis and Assessment*, 2000
- IEC 60964, *Nuclear Power Plants – Control Rooms – Design*, 2009
- ANSI/ANS-58.8, *Time Response Design Criteria for Safety-Related Operator Actions*, 1994
- IEEE 1023, *IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations*, 2004
- IEEE 1289, *IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations,* 1998
- U.S. NRC NUREG/CR-1278, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications- Final Report*, 2011
- U.S. NRC NUREG-0711, *Human Factors Engineering Program Review Model*, 2002
- U.S. NRC NUREG-0700, *Human System Interface Design Review Guidelines*, 2002
- U.S. NRC NUREG-6393, *Integrated System Validation: Methodology and Review Criteria*, 1997
- U.S. NRC NUREG/CR-6633, *Advanced Information Systems Design: Technical Basis and Human Factors Review Guidelines*, 2000
- U.S. NRC NUREG-6684, *Advanced Alarm Systems: Revision of Guidance and Its Technical Basis*, 2000

7.22 Robustness against malevolent acts

The engineering safety aspects of robustness and protection from malevolent acts should account for:

- basic design approach
- structural performance objectives
- threat characterisation
- loading development
- material properties
- principles of analysis and design
- structural acceptance criteria
- design of SSCs

The basis for identifying malevolent acts considered in the design is the potential to cause a release of radioactivity to the public and the environment.

7.22.1 Design principles

The identification of vital areas involves the identification and location of SSCs that require protection, in order to prevent unacceptable radiological consequences. The design includes the reactor building and the spent fuel pool, including the structure housing the spent fuel pool. The protection measures for these identified vital areas should be assessed.

Based on identified threats, definition and development of the design basis threat (DBT) and beyond design basis threat (BDBT) sets of load cases should be selected. Each load case should be selected as the worst case scenario for a given threat.

7.22.2 Design methods

Vital areas are designed according to the tiered approach related to the level of the threat. For the loadings induced by DBT, the structural design methodology applies conservative design measures and sound engineering practices that meet codes and standards.

For more severe events, the first tier BDBT, sufficient structural integrity to protect important systems is provided. The design code criteria may be relaxed; however, the design methodology is followed.

For extreme events, the second tier BDBT, degradation of the containment barrier may be accepted; however, the degradation is limited. The structures of vital areas are designed for the second tier BDBT that may exceed design code limits but within documented material and structural limits.

The aircraft crash loading functions related to DBTs and BDBTs are "classified", and are available to licensees and applicants upon request to the CNSC.

It is acceptable to model the whole aircraft as a load that impacts the structure. However, the design should be such that the loading functions due to the crash of the modelled aircraft against a rigid target envelope are acceptable.

Two distinct types of structural failure modes need to be reviewed: local (punching - brittle) failure and global (flexural - plastic) failure. The loading characteristics and structural behaviour for these two failure modes are different, and should be reviewed separately. However, it should be noted that, in some cases, these two failure modes (e.g., an aircraft crash) may act simultaneously or quasi-simultaneously.

Local structural behaviours under a malevolent-act-induced loading case should be assessed. Local damage to the target can be defined using the following descriptions:

- penetration – the depth of the crater due to the missile impact
- spalling – the ejection of the target material from the front face of the target (impacted face)
- scabbing – the ejection of material from the rear face of the target
- just perforation – the missile just penetrates the target with residual velocity equal to zero

Most technical references consider engines, in the case of an aircraft crash, as the critical missiles. Such local damage modes would not, in general, result in structural collapse; but they can cause damage to safety-related systems or components. Application of empirical formulae for perforation and scabbing is an acceptable approach to assess structural behaviour under local, concentrated loading.

Global structural response effects refer to the overall building behaviour in response to the applied impact loading. The global response can be characterized by major structural damage, such as significant perforation or collapse of large portions of the building walls, floors, and load carrying frames. The impact could also potentially induce significant vibrations or "shock loading" throughout the building.

In the case of an aircraft crash, local damage associated with the impact of a missile into the wall may result in scabbing of concrete from the rear face. Ultimately, it may result in local fracture of rebar, allowing perforation of the wall by the residual crushed engine mass and remaining portion

of the shaft. Global structural damage, however, is generally associated with the deformation of the entire structural system.

The design of the facility's physical protection system should consider changes in threat, enhanced understanding of the potential vulnerabilities of the facility, its systems and structures as well as advances in physical protection approaches, systems, and technologies.

7.22.3 Acceptance criteria

The acceptance criteria for both local and global behaviour should be satisfied simultaneously.

The structural acceptance criteria for local behaviour should include the following:

- DBT – no scabbing of the rear face of structural elements, possibly with limited, superficial spalling of concrete, easily repairable
- severe BDBTs – no scabbing of the rear face of structural element, or possible limited scabbing (concrete cover), if confined by the steel liner. The steel liner should remain leak-tight
- extreme BDBTs – no perforation, according to the applicable formula with a corresponding increase factor of 1.2 applied to the calculated thickness

Detailed structural analyses of representative containment structures indicate that large displacements of the containment would be expected as well as induced vibrations. The structural acceptance criteria for global behaviour are related to the limitation of structural deflections (DBT and severe BDBT) or overall damage (extreme BDBT). Therefore, special attention should be given to:

- damage to the internal structures and to the containment due to extensive deformations of the containment building
- shock damage to fragile components directly attached to the containment wall
- induced vibration
- structural integrity of the reserve water tank (e.g., CANDU design)
- structural integrity of the polar crane

Structural acceptance criteria for reinforced concrete elements are given in Table 1.

Acceptance criteria for steel are given in Table 2.

Table 1: Structural acceptance criteria for reinforced concrete elements adapted from the American Concrete Institute, ACI 349-06, *Code Requirements for Nuclear Safety-related Concrete Structures and Commentary* and U.S. Department of the Army, TM 5-1300, *Structures to Resist the Effects of Accidental Explosions*, 1990. (superseded by UFC 3-340-02, 2008).

Element type	Controlling stress	Ductility, μ_a	Support rotation in degrees[3,4], θ_a		
			DBT	First Tier BDBTs	Second Tier BDBTs
Beams	Flexure	[2]	essentially elastic behavior [6]	2	4
	Shear: [1]				
	concrete only	1.3			
	concrete + stirrups	1.6			
	stirrups only	3.0			
	compression	1.3			
Slabs	Flexure	[2]	essentially elastic behavior [6]	4	8
	Shear: [1]				
	concrete only	1.3			
	concrete + stirrups	1.6			
	stirrups only	3.0			
	compression	1.3			
Beam-columns, walls and slabs in compression	Flexure	1.3 [5]	essentially elastic behavior [6]	2	4
	Compression	1.3			
Shear walls, diaphragms	Flexure	3	essentially elastic behavior [6]	1.5	2
	Shear – In-plane	1.5			

Table Legend

(1) shear controls when shear resistance is less than 120% of flexural resistance per ACI-349
(2) when flexure controls, permissible ductility ratio = $0.05/(\rho - \rho') < 10$ or rotational capacity in radians is limited to $0.0065(d/c) < 0.07$ radians = 4 degrees
(3) stirrups are required for support rotations greater than 2 degrees
(4) these rotation criteria (in degrees) are, in general, consistent with those in the ACE Technical Manual which does not specify allowable inelastic deformation in terms of ductility ratio-criteria for flexure
(5) for additional detailed criteria, see section F.3.8 of ACI-349
(6) essentially elastic behavior means elastic structural analysis using design strain acceptance criteria of 1% for reinforcement in tension and 0.35% for concrete in compression

Table 2: Structural acceptance criteria - allowable strains for steel

Material	Strain measure	Allowable value DBTs	Allowable value for First Tier BDBTs
Carbon steel plate	Membrane principal strain (tensile)	0.01	0.050
	Local ductile tearing effective strain	NA	0.140/TF
304 stainless steel plate	Membrane principal strain (tensile)	0.01	0.067
	Local ductile tearing effective strain	NA	0.275/TF
Grade 60 reinforcing steel	Tensile strain	0.01	0.050
Post–tensioning steel (ungrouted tendons)	Tensile strain	0.010	0.030
Post–tensioning steel (grouted tendons)	Tensile strain	0.010	0.020

Conservatively, TF (triaxiality factor) value can be taken equal to 2.

$$TF = \frac{\sigma_1 + \sigma_2 + \sigma_3}{\sigma_e}$$

Where σ_1, σ_2 and σ_3 are principal stresses and σ_e is effective or equivalent stress.

The values in Table 1 and Table 2 are maximum values under the loading condition. For reinforced and pre-stressed concrete the maximum compression strain for DBTs is 0.0035. For the First Tier BDBTs, this strain is 0.005. The strains for second tier BDBTs can be deducted from support rotations given in Table 2. It should be noted that the acceptance criteria presented in Tables 1 and 2 are applicable to large structural portions impacted by large impulsive loading.

Further information on the design and construction for containment and other safety-related structures can be found in the CSA N287 series of standards, and in CSA N291-08, *Requirements for Safety-Related Structures for CANDU Nuclear Power Plants*, respectively.

Additional information

Further information is available in:

- CNSC G-274, *Security Programs for Category I or II Nuclear Material or Certain Nuclear Facilities*, 2003
- CNSC G-208, *Transportation Security Plans for Category I, II or III Nuclear Material*, 2003
- CNSC RD-363, *Nuclear Security Officer Medical, Physical, and Psychological Fitness*, 2008
- IAEA TECDOC-967 (Rev.1), *Guidance and considerations for the implementation of INFCIRC/225/Rev.5, The Physical Protection of Nuclear Material and Nuclear Facilities*, 2002
- IAEA *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* (INFCIRC/225/Rev.5), 2011
- IAEA TECDOC-1276, *Handbook on the physical protection of nuclear materials and facilities*, 2002
- Communications Security Establishment, TRA-1, *Harmonized Threat and Risk Assessment (TRA) Methodology*, 2007
- CSA N291-08, *Requirements for Safety-Related Structures for CANDU Nuclear Power Plants*, 2008
- American Society of Civil Engineers (ASCE), *Design of Blast-Resistant Buildings in Petrochemical Facilities*, 2010
- ACI Standard 349, *Code requirements for Nuclear Safety-Related Concrete Structures and Commentary*, 2007
- U.S. Department of the Army, TM 5-1300, *Structures to Resist the Effects of Accidental Explosions*, 1990. Superceded by UFC 3-340-02, 2008
- American Society of Civil Engineers (ASCE), *Structural Analysis and Design of Nuclear Plant Facilities: 58 (ASCE Manual and Reports on Engineering Practice),*1980
- United Kingdom Atomic Energy Authority, (UK AEA), *Guidelines for the design and assessment of concrete structures subjected to impact,* 1990
- Nuclear Energy Institute, NEI 07-13, *Methodology for Performing Aircraft Impact Assessments for New Plant Designs*, 2011

7.22.4 Cyber security

The security of computer-based I&C systems is designed to provide a secure development environment with defensive features, and to protect against cyber attacks. Applicable codes and standards should be used, and industry best practices should be consulted.

The design of a cyber security program should consider:

- documentation for how the design authority establishes, implements and maintains the program to provide high assurance that the systems subject to security protective measures are protected
- application of defence in depth protective strategies, to provide a high level of assurance that the program has adequate cyber security capability
- addressing of potential security vulnerabilities in each phase of the computer-based I&C systems lifecycle for computer-based systems important to safety

- inclusion of security controls for a secure development environment during the development phases
- site specific program should include the following elements but not limited:
    - defensive strategy
    - asset identification, and security controls
    - roles, responsibilities
    - policies and procedures
    - awareness and training
    - configuration management
    - information protection
    - coordination with other security programs
    - incident reporting and recovery plan
    - program maintenance

RD-337 version 2 states *"the design of computer-based instrumentation and control systems important to safety shall provide a cyber security defensive architecture"*. The defensive architecture should have cyber security defensive levels separated by security boundaries. The systems requiring the greatest degree of security should be located within the most secure boundaries.

The design authority should identify the design features that provide a secure operational environment of the systems important to safety.

Security design requirements for computer-based I&C systems should be informed by vulnerability analyses. Vulnerabilities addressed in the design should include:

- deficiencies in the design that may allow inadvertent, unintended, or unauthorized access or modifications to the systems (hardware and software), which may degrade the reliability, integrity or functionality of the systems during operations
- non-performance of the safety functions by the systems in the presence of undesired behaviour of the connected systems

The following should be considered for the protection of computer-based I&C systems and components important to safety functions:

- the computer-based I&C systems and components important to safety should be protected, along with those support systems and components which, if compromised, would adversely affect safety functions
- cyber attacks include either physical or logical threats (with either malicious or non-malicious intent), originated from inside and outside of the perimeter of the system's facility
- computer-based systems and components includes computer hardware, software, firmware, and interfaces
- any computer-based system, either autonomous or non-autonomous, should be protected
- computer-based systems and components for the functions of emergency preparedness system, physical security and safeguards, should be protected, if applicable for the design

The computer-based I&C systems important to safety should be protected from physical attacks and unauthorized physical or logical access, such that:

- all systems, components and network cabling important to safety should be installed in a plant location that physically secures the equipment
- effective methods should be used, such as including appropriate combinations of programmatic controls and physical security measures (e.g., locked enclosures, locked rooms, alarms on enclosure doors)
- unnecessary or unauthorized access to the setpoint adjustments and calibration adjustments should be limited, because of their importance to preventing degraded system performance due to potential errors in operation or maintenance
- connections needed for temporary use should be disabled when not in use (e.g., connection of maintenance and development computers)
- unused data connections should be disabled
- all data connections for systems and components should be placed within enclosures
- any remote access to the safety system from a computer located in an area with less physical security than the safety system should be limited
- access to the safety systems should be logged, and the security logs should be checked periodically
- wireless communication should not be implemented for the safety systems
- safety systems should be designed such that virus protection software is not required
- communication of plant data between the plant and the emergency control centre (either onsite or offsite) should be via unidirectional links

RD-337 version 2 states that "*cyber security features shall not adversely affect the functions or performance of SSCs important to safety*". Security functions and security supporting functions of I&C systems should not adversely affect the functions of systems and components important to safety. The design should ensure that neither the operation nor failure of security measures implemented will adversely affect the ability of the systems important to safety.

Implementation of any individual security control/function or of the complete set of applied controls for safety systems, the following should be considered:

- implementation should not impact performance, including response time, effectiveness or operation of safety functions
- where practical, implementation directly in the safety system should be avoided
- if implemented in safety system displays and controls, the security control should not adversely impact the operator's ability to maintain the safety of the plant
- if implemented within the safety system, adequate measures should be taken to ensure that the security controls do not adversely affect the ability of the system to perform its safety functions
- security controls within a safety system should be developed and qualified to the same level of qualification as the system in which the control resides

Provisions should be taken for periodic and post-maintenance verification, to verify that the security features are properly configured and operating.

Additional information:

Further information is available in:

- IAEA Nuclear Security Series No. 17, *Computer Security at Nuclear Facilities*, 2011
- IEEE 7-4.3.2, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*, 2010
- IEC 61513, *Nuclear Power Plant-Implementation and control important to safety - General requirements for systems*, 2011
- NEI 08-09 Rev.6, *Cyber Security Plan for Nuclear Power Reactors*, 2010
- U.S. NRC, Regulatory Guide 5.71, *Cyber Security Programs for Nuclear Facilities*, 2010

7.23 Safeguards

For the purposes of this document, the term "safeguards" denotes a system of inspection and other verification activities undertaken by IAEA in order to evaluate a state's compliance with its obligations, pursuant to its safeguards agreement with the IAEA, under the *Treaty on the Non-Proliferation of Nuclear Weapons*. The objective of the Canada-IAEA safeguards agreement is for the IAEA to provide annual assurance to Canada and to the international community that all declared nuclear material is employed in peaceful, non-explosive uses, and that there is no indication of undeclared nuclear material or activities. The CNSC is the governmental authority responsible for implementing the Canada-IAEA safeguards agreement.

The integration of safeguards considerations during the early design phase of a new NPP is a well established practice in the Canadian nuclear industry. This approach can avoid the retrofitting of safeguards equipment after a design is completed, which could otherwise result in substantial cost increases in terms of redesign work, timeline extensions and additional demands on human resources. If there is a requirement to install IAEA safeguards equipment to monitor nuclear material flows and inventories, accurate plant layout requirements should be identified early in the process, so as to ensure that appropriate "design space" is allocated for critical safeguards installations.

The CNSC requires that licensees put in place a program and appropriate procedures to ensure that safeguards can be implemented effectively and in a manner consistent with Canada's obligations.

Additional information:

Further information is available in:

- CNSC RD-336, *Accounting and Reporting of Nuclear Material*, 2010
- CNSC GD-336, *Guidance for Accounting and Reporting of Nuclear Material*, 2010

7.24 Decommissioning

As stated in RD-337 version 2, "*future plant decommissioning and dismantling activities shall be taken into account*". This should include considerations of experience gained from the decommissioning of existing plants, as well as those plants that are in long-term safe storage. Experience suggests that the decommissioning of NPPs could be facilitated if it received greater attention at the design stage. The consideration of decommissioning at the design stage is expected to result in lower worker doses and reduced environmental impacts.

Additional information

Further information is available in:

- CNSC G-219, *Decommissioning Planning for Licensed Activities*, 2000
- Nuclear Energy Agency (NEA) No. 6833, *Decommissioning Considerations for New Nuclear Power Plants*, OECD 2010
- NEA 6924, *Applying Decommissioning Experience to the Design and Operation of New Nuclear Power Plants*, OECD 2010
- IAEA TECDOC-1657: *Design Lessons Drawn from the Decommissioning of Nuclear Facilities*, 2011
- CSA N294-09, *Decommissioning of Facilities Containing Nuclear Substances*, 2009
- IAEA Safety Guide WS-G-2.1, *Decommissioning of Nuclear Power Plants and Research Reactors*, 1999

8.0 Guidance on System-Specific Requirements

8.1 Reactor core

The design of the reactor core should provide confidence that the permissible design limits, under operational states and accident conditions, are not exceeded, taking into account engineering tolerances and uncertainties associated with the calculations.

8.1.0.1 Nuclear design

The nuclear design deals with flux and power distribution within the reactor core, the design and use of reactivity control systems for normal operation and for shutting down the reactor, core stability, the various reactivity feedback characteristics, and the physics of the fuel.

General expectations

The reactor core design should take into account all practical means so that, in the power operating range, the net effect of the prompt inherent nuclear feedback characteristics tends to compensate for a rapid increase in reactivity and power. The consequences of those accidents that would be aggravated by a positive reactivity feedback should be either acceptable, or be satisfactorily mitigated by other design features.

The design should take into account measurements made in previous reactors and critical experiments and their use in the uncertainty analyses, and the measurements to be made, including startup confirmatory tests and periodically required measurements.

The design should provide for I&C to:

- maintain the variables and systems within prescribed operating ranges
- monitor variables and systems that can affect the fission process over anticipated ranges for operational states and accident conditions

These I&Cs should be demonstrated to be effective.

Defence in depth

The nuclear design should incorporate inherently safe features to reduce the reliance on engineered safety systems or operational procedures. Defence in depth and related principles

should be applied in the design of the reactivity control safety function, such that the fission chain reaction is controlled during operational states, and, when necessary, terminated for accident conditions.

The nuclear design should provide for effective means to ensure success of the following safety functions to:

- prevent unacceptable reactivity transients
- shut down the reactor as necessary to prevent progression of AOOs to DBAs, or DBAs to DECs
- maintain and monitor the reactor in a safe shutdown state

Core power densities and distributions

The design limits for the power densities and power distributions should be determined from an integrated consideration of fuel design limits, thermal limits, decay heat limits, and AOO and accident analyses. For power distribution, the reactor core design should demonstrate the following:

a) There is a high level of confidence that the proposed design limits can be met within the expected operational range of the reactor, taking into account:

- the analytical methods and data for the design calculations
- uncertainty analyses and experimental comparisons presented for the design calculations
- the sufficiency of design cases calculated covering times in fuel reload cycle, or during on-power fuelling (depending upon the reactor design, reactivity devices configurations, and load-follow transients)
- special problems (such as power spikes due to densification), possible asymmetries, and misaligned reactivity devices

b) There is a high level of confidence that, during normal operation, the design limits will not be exceeded, based on consideration of information received from the power distribution monitoring instrumentation. The processing of that information should include:

- calculations (instrument-calculation correlations) involved in the processing
- operating procedures used
- the requirements for periodic check measurements
- the accuracy of design calculations used in developing correlations when primary variables are not directly measured
- the uncertainty analyses for the information and processing system
- the requirements for instruments, the calibration and calculations involved in their use, and the uncertainties involved in conversion of instrument readings into power distribution
- the limits and setpoints for control actions, alarms, or automatic trip for instrument systems and demonstration that these systems can maintain the reactor within design power distribution limits (including the instrumentation alarms for the limits of normal operation (e.g., offset limits, control bank limits) and for abnormal situations (e.g., flux tilt alarms)
- measurements in previous reactors and critical experiments, including their use in the uncertainty analyses
- measurements needed for startup confirmatory tests and the required periodical measurements

The limiting power distributions should be determined such that the limits on power densities and peaking factors can be maintained in operation. These limiting power distributions may be

maintained (i.e., not exceeded) administratively (i.e., not by automatic shutdown), provided a suitable demonstration is made that sufficient, properly translated information and alarms are available from the reactor instrumentation to keep the operator informed.

The design should establish the correlation between design power distributions and operating power distributions, including instrument-calculation correlations, operating procedures used, and measurements that will be taken. Necessary limits on these operations should be established.

The breakdown of design power distributions into the following components should be established:

- power generated in the fuel
- power generated directly in the coolant and moderator
- power generated directly in the core internals

The reference design core power distributions (axial, radial, and local distributions and peaking factors) used in AOO and accident analyses should be established. In addition, power distributions within fuel pins should be established.

The design limits for power densities (and thus for peaking factors) during normal operation should be such that acceptable fuel design limits are not exceeded during AOOs and that other limits are not exceeded during accident conditions. The design limits, along with related uncertainties, operating limits, instrument requirements, and setpoints, should be incorporated into OLCs.

Reactivity coefficients

The design should establish and characterize the bounding (conservative) reference values for reactivity coefficients.

The range of plant states to be covered should include the entire operating range – from cold shutdown through full-power – and the extremes reached in AOOs and accident conditions. It should include the full range of the fuelling cycle, and an appropriate range of reactivity device configurations.

The design calculations of reactivity coefficients should cover the full applicable range of the variables and modelling approximations in AOO and accident analyses, including approximations related to modelling and nodalization of the reactor cooling system. Where applicable, the difference between intra- and inter-assembly moderator coefficients needs to be established.

Conservatism should be considered based on:

- the use of a coefficient (i.e., the analyses in which it is important)
- whether state of the art tools have been used for calculation of the coefficient
- the uncertainty associated with such calculations, experimental checks of the coefficient in operating reactors
- any required checks of the coefficient in the startup program following significant core reconfiguration

The design calculation should cover and be supported by the following:

- calculated nominal values for the reactivity coefficients, such as the coolant and moderator coefficients (temperature, void, or density coefficients), the Doppler coefficient and power coefficients
- uncertainty analyses for nominal values, including the magnitude of the uncertainty and the justification of the magnitude (by examination of the accuracy of the methods used in

calculations), and comparison, where possible, with reactor experiments. For comparisons to experiments, it is important to show that the experiments are applicable and relevant, and the experimental conditions overlap the operating and anticipated accident conditions.
- combination of nominal values and uncertainties to provide suitably conservative values for use in reactor steady-state analysis (primarily control requirements), stability analyses, and the AOO and accident analyses

The power coefficient of reactivity should be negative, or the design authority should demonstrate that operation with a positive power coefficient is acceptable for certain rare operating states, by showing:

- a bounding value of power coefficient of reactivity has been calculated for all permitted operating states and used in control, stability, and safety analyses
- measurements of the power coefficient of reactivity are conducted at startup and periodically for certain operating limiting core conditions to demonstrate that measured values are bounded by calculated values with adequate margin
- the reactor control system is designed with adequate reliability and has the capability to automatically accommodate for a positive power coefficient of reactivity for a wide range of AOOs

The design should ensure that the likelihood of exceeding specified criteria of the AOOs without shutdown is sufficiently small, by demonstrating either that the criteria are met, or that a diverse shutdown means is installed, which reduces significantly the probability of a failure to shutdown.

Criticality

The nuclear design should ensure that the criticality of the reactor during refuelling is controlled. If on-power refuelling is used to compensate for core reactivity depletion, the nuclear design should establish the values of core excess reactivity, maximum local powers, amount of fuel loaded per refuelling operation and frequency of refuelling load; the design should also ensure that the maximum core excess reactivity and predicted local power peaks will not exceed the control system capability and fuel thermal limits.

Core stability

Power oscillations that could result in conditions exceeding specified acceptable fuel design limits should not be possible, or should be reliably and readily detected and suppressed.

Assessment of reactor core stability should include:

- phenomena and reactor aspects that influence the stability of the nuclear reactor core
- calculations and considerations given to xenon-induced spatial oscillations
- potential stability issues, due to other phenomena or conditions
- verification of the analytical methods for comparison with measured data

Analytical methods

The analytical methods and database used for nuclear design and reactor physics analyses should be consistent with modern best practices. Also, the experiments used to validate the analytical methods should be adequate representations of fuel designs in the reactor and ranges of key parameters in the validation database should overlap those expected in design and safety analysis.

The design should be such that the analytical methods used in the nuclear design (including those for predicting criticality, reactivity coefficients, burnup and stability) as well as the database and nuclear data libraries used for neutron cross-section data and other nuclear parameters (including delayed neutron and photo neutron data and other relevant data) are adequate and fit for application, based on adequate qualification. The qualification should be based on proven practices for validation and verification, using the acceptable codes and standards.

Core internals and vessel

The nuclear design should establish:

- neutron flux spectrum above 1 million electron volts (MeV) in the core, at the core boundaries, and at the inside vessel wall, if applicable
- assumptions used in the calculations, these include the power level, the use factor, the type of fuel cycle considered, and the design life of the vessel
- computer codes used in the analysis
- the database for fast neutron cross-sections
- the geometric modelling of the reactor core, internals, and vessel(s)
- uncertainties in the calculations

Additional information

Further information is available in:

- CSA N290.4-11, *Requirements for the Reactor Control Systems of Nuclear Power Plants*, 2011
- CSA CAN3-N290.1-80, *Requirements for the Shutdown Systems of CANDU Nuclear Power Plants*, reaffirmed 2011
- CSA N286.7-99, *Quality Assurance of Analytical, Scientific, and Design Computer Programs for Nuclear Power Plants*, reaffirmed 2007
- CSA N286.7.1-09, *Guideline for the application of N286.7-99, Quality assurance of analytical, scientific, and design computer programs for nuclear power plan*ts, 2009
- IAEA NS-G-1.12, *Design of the Reactor Core for Nuclear Power Plants*, 2005
- IAEA NS-G-2.5, *Core Management and Fuel Handling for Nuclear Power Plants*, 2002
- U.S. NRC Regulatory Guide 1.77, *Assumptions Used for Evaluating a Control Rod Ejection Accident for Pressurized Water Reactors*, 1974
- U.S. NRC Regulatory Guide 1.203, *Transient and Accident Analysis Methods*, 2005

8.1.0.2 Core management and fuel handling

The reactor design should be such that the plant will operate within the specified operating limits for the entire reactor lifecycle (including intermediate reactor core states).

The design should provide for functional tests to be performed periodically for monitoring the health of the reactor components.

The design should provide for the capability to monitor online important core parameters, to ensure that the acceptable operating limits for the reactor are not exceeded during normal operation. The types of detectors and other devices used in monitoring the core parameters should be described.

The reactor control strategy should be defined, to ensure that the reactor will be restored to an acceptable safe state if any reactor parameter deviates from its allowed domain. The control strategy should be such that fuel integrity will be maintained for all AOOs.

The refuelling scheme should be developed to ensure that the intermediate refuelling configurations do not have more reactivity than the most reactive configuration approved in the design. The core parameters for the intermediate configurations should be within their approved limits.

The design should allow for data acquisition during reactor operation and record-keeping for later retrieval and analysis.

The design should take into account the details of fuel management strategy including the loading of fuel into the fresh core, and the criteria for determining the location of fuel assemblies to be unloaded from the reactor and loaded with fresh fuel.

For reactor designs with batch fuelling, the design should provide for diagnostic tests performed at the beginning of a fuel cycle, so as to verify that the core parameters are within their allowed range.

Important reactivity coefficients and physics parameters should be shown to be within safe limits, as described in the safety analysis.

8.1.0.3 Reactor internals

The reactor internal components designated as ASME Code, Section III, *Core Support Structures* should be designed, fabricated, and examined in accordance with the provisions of Section III, subsection NG, of the ASME Code.

Those reactor internals components not designated as ASME Code, Section III, *Core Support Structures* should be designated as internal structures in accordance with ASME Code, Section III, Subsection NG-1122. The design criteria, loading conditions, and analyses that provide the basis for the design of reactor internals (other than the core support structures) should meet the guidelines of ASME Code, Section III, Subsection NG-3000, and constructed so as to not adversely affect the integrity of the core support structures. If other guidelines (e.g., manufacturer standards or empirical methods based on field experience and testing) are the bases for the stress, deformation, and fatigue criteria, those guidelines should be identified and their use justified in the design.

For non-ASME code structures and components, design margins presented for allowable stress, deformation, and fatigue should be equal to or greater than margins for other plants of similar design with successful operating experience. Any decreases in design margins should be justified.

Specific reactor internals components designated as Class 1, Class 2, and Class 3 should be designed, fabricated, and examined in accordance with the applicable codes and standards, such as ASME Section III for light water reactors (LWR), and CSA N285.0, *General requirements for pressure-retaining systems and components in CANDU nuclear power plants* for CANDU.

8.1.1 Fuel elements and assemblies

The fuel design and qualification should provide assurance that the reactor core design requirements in section 8.1 of RD-337 version 2 are met.

8.1.1.1 Fuel design

Acceptance criteria should be established for fuel damage, fuel rod failure, and fuel coolability. These criteria should be derived from experiments that identify the limitations of the material properties of the fuel and fuel assembly. The fuel design criteria and other design considerations are provided below.

Fuel damage

Fuel damage criteria should be included for all known damage mechanisms in normal operation. The damage criteria should assure that fuel dimensions remains within operational tolerances, and that functional capabilities are not reduced below those assumed in the safety analysis. When applicable, the fuel damage criteria should consider high burn-up effects based on irradiated material properties data. The criteria should include stress, strain or loading limits, the cumulative number of strain fatigue cycles, fretting wear, oxidation, hydriding (deuteriding in CANDU reactors), build-up of corrosion products, dimensional changes, rod internal gas pressures, worst-case hydraulic loads, and LWR control rod reactivity and insertability.

Fuel rod failure

Fuel rod failure applies to operational states and accident conditions. Fuel rod failure criteria should be provided for all known fuel rod failure mechanisms. The design should ensure that fuel does not fail as a result of specific causes during operational states. Fuel rod failures may occur during accident conditions, and are accounted for in the safety analysis.

The methods used in the assessment of the fuel failure mechanisms, reactor loading and power manoeuvring limitations, and fuel duty which lead to an acceptably low probability of failure, should be stated. When applicable, the fuel rod failure criteria should consider high burnup effects, based on data of irradiated material properties. The criteria should include:

- hydriding
- cladding collapse
- cladding overheating
- fuel pellet overheating
- excessive fuel enthalpy
- pellet-clad interaction
- stress-corrosion cracking
- cladding bursting
- mechanical fracturing

Fuel coolability

Fuel coolability applies to DBAs and, to the extent practicable, DECs. Fuel coolability criteria and LWR control rod insertability criteria should be provided for all damage mechanisms in accident conditions. The fuel should be designed to ensure that fuel rod damage will not interfere with effective emergency core cooling. The cladding temperatures should not reach a temperature high enough to allow a significant metal-water reaction to occur, thereby minimizing the potential for offsite fission product release. The criteria should include cladding embrittlement, violent expulsion of fuel, generalized cladding melting, fuel rod ballooning, structural deformation and, in CANDU, beryllium braze penetration.

Other design considerations

The design should also include:

- all expected fuel handling activities
- the effects of post-irradiation fuel assembly handling
- cooling flow of other components of LWR fuel assembly (such as control rods, poison rods, instrumentation, or neutron sources)

Fuel testing, inspection, and surveillance programs

Programs for testing and inspection of new fuel, as well as for online fuel monitoring and post-irradiation surveillance of irradiated fuel should be established.

Fuel specification

The design should establish the specification of fuel rods and assembly (including LWR control rods) in order to minimize design deviations and to determine whether all design bases are met (such as limits and tolerances).

Additional information

Further information is available in:

- CNSC G-144, *Trip Parameter Acceptance Criteria for the Safety Analysis of CANDU Nuclear Power Plants*, 2006
- U.S. NRC NUREG-0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Fuel System Design, Section 4.2*, 2007
- ANSI/ANS-57.5-1996, *Light Water Reactor Fuel Assembly Mechanical Design and Evaluation*, 1996

8.1.1.2 Reactor core thermalhydraulic design

The thermalhydraulic design should be such that sufficient margin exists with regard to maintaining adequate heat transfer from the fuel to the reactor coolant system, to prevent fuel sheath overheating. The design requirements can be demonstrated by meeting a set of derived acceptance criteria (DAC), as required by RD-310, *Safety Analysis for Nuclear Power Plants*.

Critical heat flux (CHF) is defined as the heat flux at departure from nucleate boiling (DNB), commonly used in pressurized water reactors (PWRs), or at dryout, commonly used in CANDU designs.

It should be noted that, although a thermal margin criterion is sufficient to demonstrate that overheating from a deficient cooling mechanism can be avoided; other mechanistic methods may be acceptable as CHF is not considered as a failure mechanism. In some designs, CHF conditions during transients can be tolerated if it can be shown by other methods that the sheath temperatures do not exceed well-defined acceptable limits. However, any other criteria than the CHF criterion should address sheath temperature, pressure, time duration, oxidation, embrittlement etc., and these new criteria should be supported by sufficient experimental and analytical evidence. In the absence of such evidence, the core thermal-hydraulic design is expected to demonstrate a thermal margin to CHF.

The demonstration of thermal margin is expected to be presented in a manner that accounts for all possible reactor operational states and conditions, as determined from operating maps including all AOOs. The demonstration should also include long term effects of plant aging and other expected changes to core configuration over the operating life of the plant.

The demonstration of thermal margin should thoroughly address uncertainties of various parameters affecting the thermal margin. The design should identify all sources of significant uncertainties that contribute to the uncertainty of thermal margin. The uncertainty for each of the sources should be quantified with supportable evidence.

In addition to the demonstration of thermal margin, the core thermal-hydraulic design should also address possible core power and flow oscillations and thermal-hydraulic instabilities. The design should be such that power and flow oscillations that result in conditions exceeding specified acceptable fuel design limits are not possible or can be reliably and readily detected and suppressed.

8.1.2 Control system

As stated in RD-337 version 2, "*the reactor core control system shall detect and intercept deviations from normal operation, with the goal of preventing AOOs from escalating to accident conditions*".

Reactivity control

The reactivity control should ensure that:

- the acceptable fuel design limits are not exceeded as a result of a wide range of AOOs
- no single malfunction of the reactivity control function can cause a violation of the acceptable fuel design limits

The nuclear design reactivity control requirements and control provisions should:

- compensate for long-term reactivity changes of the core; this includes reactivity changes due to depletion of the fissile material in the fuel, depletion of burnable poison in some of the fuel rods (where applicable), and buildup of fission products and transuranic isotopes
- compensate for the reactivity change caused by changing the temperature of the reactor from the zero power hot condition to the cold shutdown condition
- compensate for the reactivity effects caused by changing the reactor power level from full-power to zero power
- assure reactivity management during the fuelling cycle, and intermediate times during the fuel cycle
- compensate for the effects on the power distribution and stability of the high cross-section neutron capture of the fission product nuclide xenon-135
- cover uncertainties associated with the control rods, including:
    - manufacturing tolerances
    - methods errors
    - operation other than planned
    - control element absorber depletion
    - measurement uncertainty in shutdown margin demonstration

Reactivity devices configurations and reactivity worth

The nuclear design should establish the following for reactivity device configurations, including (where applicable) control rod patterns, and reactivity worth for:

- reactivity devices configurations expected throughout a fuel reload cycle, power manoeuvring, and load-following (where applicable). This includes operation of single rods, or of groups or banks of rods, rod withdrawal order, and insertion limits, as a function of power and core life
- predicted reactivity devices' worth and reactivity insertion rates. It should be reasonably bounded to values that may occur in the reactor. Note: These values are typically used in the safety analysis, and judgments as to the adequacy of the uncertainty allowances are made in the review of the safety analysis

- allowable deviations from the patterns indicated above, such as for misaligned rods, stuck rods, or rod positions used for spatial power shaping
- maximum worth of individual rods or banks as a function of position for power and cycle life conditions appropriate to rod withdrawal, rod ejection (or drop) accidents and other conceivable failures of reactivity control components leading to positive reactivity insertions
- maximum rates of reactivity increase associated with reactivity device withdrawals and any other conceivable change in the configuration of reactivity devices, due to failures in reactivity control system. It should also include experimental confirmation of rod worth, or other factors justifying the reactivity increase rates used in control rod accident analyses, as well as equipment, administrative procedures and alarms which may be employed to restrict potential rod worth
- trip (or scram) rundown reactivity, as a function of time after trip (scram) initiation and other pertinent parameters, including methods for calculating the rundown reactivity
- equipment, operating limits, and administrative procedures necessary to restrict potential rod worth or reactivity insertion rates

8.2 Reactor coolant system

In order to meet safety requirements of the reactor coolant system (RCS), the design should have adequate provisions with regards to reactor coolant system and reactor auxiliary systems. The design should meet design limits for the worst conditions encountered in normal operation, AOOs and DBAs, including pressurized thermal shock and water hammer loads. The reactor coolant system and reactor auxiliary systems should meet – or contribute to meeting – the following:

- maintain sufficient reactor coolant inventory for core cooling both in and after all postulated initiating events considered in the design basis
- remove heat from the core after a failure of the reactor coolant pressure boundary, in order to limit fuel damage
- remove heat from the core in appropriate operational states and in accident conditions with the reactor coolant pressure boundary intact
- transfer heat from other safety systems to the ultimate heat sink

The design of each reactor auxiliary system should ensure that automatic action by the system cannot impair a safety function.

The design authority should demonstrate the adequacy of the following:

- flow rate and pressure drops across major components
- major thermalhydraulic parameters, such as operating pressure and temperature ranges
- valve performance (flow, pressure drop, opening and closing times, stability, water-hammer)
- pump performance (head, flow, two-phase flow, seal performance)
- vibration of components and pipes
- control of gas accumulation (in particular, prevention of combustible gas accumulation)
- maximum allowable heat-up and cool-down rates
- consideration of pressurized thermal shock due to operation (including inadvertent operation) of auxiliary systems
- flow stability, including loop-to-loop stability and void-enthalpy oscillations (CANDU)
- design of instrumentation taps

The following provides a few examples of design expectations of the reactor coolant system and reactor auxiliary system:

Pressurizer

For designs that include a pressurizer, the design authority should demonstrate the adequacy of the following:

- volume and capability to accommodate load changes
- capability to withstand thermal shock, particularly in spray nozzles and connections to the main RCS circuit
- control of pressure via heaters, sprays or coolers

Primary pressure relief

The design authority should demonstrate the adequacy of the following:

- flow rate in single and two phase flow
- consideration of corrosion of valve surfaces
- provisions for ensuring that relief discharge does not lead to an unacceptable harsh environment inside containment
- relief valve stability

Primary reactor coolant pumps

For designs that use forced primary flow, the design authority should demonstrate the adequacy of the following:

- primary pump performance characteristics, including head and flow characteristics, flow coastdown rate, single and two-phase pump performance
- pump operating parameters (e.g., speed, flow, head)
- pump net positive suction head needed to avoid cavitation
- pump seal design and performance (including seal temperature limitations, if applicable)
- vibration monitoring provisions

Additional information

Further information is available in:

- IAEA NS-G-1.9, *Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants Safety Guide*, 2004

8.2.1 In-service pressure boundary inspection

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

8.2.2 Inventory

As stated in RD-337 version 2, *"taking volumetric changes and leakage into account, the design shall provide control of coolant inventory and pressure, so as to ensure that specified design limits are not exceeded in operational states*". In meeting this requirement, the design should take

into account the provision of adequate capacity, volumetric changes, leakage, flow rate and storage volumes in the systems performing this function.

8.2.3 Cleanup

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

8.2.4 Removal of residual heat from reactor core

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

8.3 Steam supply system

Guidance related to the steam supply system can be found in chapter 10 of U.S. NRC NUREG-0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition – Steam and Power Conversion System.*

8.3.1 Steam lines

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

8.3.2 Steam and feedwater system piping and vessels

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

8.3.3 Turbine generators

The design of turbine generators should meet the following expectations:

- a turbine control and over-speed protection system should control turbine action under all normal or abnormal operating conditions, and should ensure that a full load turbine trip will not cause the turbine to over-speed beyond acceptable limits
- the over-speed protection system should meet the single failure criterion, and should be testable when the turbine is in operation
- the turbine main steam stop and control valves, and the reheat steam stop and intercept valves should protect the turbine from exceeding set speeds, and should protect the reactor system from abnormal surges
- the turbine generator set should have the capability to permit periodic testing of components important to safety while the unit is operating at rated load
- an in-service inspection and testing program for main steam and reheat valves should be established
- the arrangement of connection joints between the low-pressure turbine exhaust and the main condenser should prevent adverse effects on any safety-related equipment in the turbine room in the event of a rupture (it is preferable not to locate safety-related equipment in the turbine room)

8.4 Means of shutdown

As stated in RD-337 version 2, *"the design shall include two separate, independent, and diverse means of shutting down the reactor"*.

For the two means to be independent of each other, they must not share components. If both means act inside the core and complete separation is not possible, adequate separation of ex-core components should be demonstrated.

The design uses diverse methods for all aspects of the shutdown means such as:

- the insertion of solid control rods and injection of a solution of neutron absorbing material are the diverse methods normally used in water-cooled reactors
- diverse methods should be considered in the design of sensors, logic and actuation of the shutdown means

As stated in RD-337 version 2, "*redundancy shall be provided in the fast acting means of shutdown"* unless the safety analysis demonstrates that, for any AOO or DBA coincident with failure of a single fast acting means of shutdown, the acceptance criteria can be met.

For shutdown means based on injection of a neutron absorbing solution, chemistry-related issues (such as avoiding precipitation) should be addressed.

The design authority should specify the requirements for inspection, test and maintenance, including commissioning tests to verify the speed and depth of shutdown for each shutdown means.

For LWR designs, fuel rod bowing can lead to loads on control rod guide tubes which may impair a rod-based shutdown means. The fuel design should ensure that this does not occur in operational states and DBAs.

As stated in RD-337 version 2*, "at least one means of shutdown shall be independently capable of rendering the reactor subcritical from normal operation, in AOOs and DBAs, and maintaining the reactor subcritical by an adequate margin and with high reliability, for even the most reactive conditions of the core"*. This normally includes a core with maximum allowable excess reactivity (for example, following batch refuelling) and the most reactive conditions for coolant and moderator temperature and density (for example, at cold shutdown conditions for a reactor with a negative temperature coefficient of reactivity).

For CANDU reactors, there is a possibility of an in-core LOCA. This poses a special challenge to reactivity control systems. In particular, hydraulic loads from an in-core LOCA can damage shutoff rod guides, and possibly damage poison injection nozzles. If shutdown action is required for an in-core LOCA, the design specification should identify how many reactivity devices may be damaged by the in-core LOCA. This should be consistent with the assumptions in the safety analysis. The results of the analysis of the damage extent and supporting experiments should be provided.

The performance criteria for the speed and depth of a fast acting shutdown means should be provided by the design authority. A shutdown means is considered to be effective if the safety analysis acceptance criteria are met. The performance criteria for an adequate subcriticality margin of a shutdown means should be provided by the design authority.

For LWRs, in particular pressurized water reactors (PWRs), a large LOCA can lead to significant hydraulic loads on core internals, such as control rod guides in the upper plenum. Core barrel distortion could lead to misalignments. If control rod insertion is credited in the safety analysis for a large LOCA (most PWRs do not credit rod movement), the design should demonstrate that control rod insertion will not be impeded.

8.4.1 Reactor trip parameters

The effectiveness of trip parameters is assessed through safety analysis performed in accordance with CNSC RD-310, *Safety Analysis for Nuclear Power Plants*. Further guidance is provided in CNSC GD-310, *Guidance on Safety Analysis for Nuclear Power Plants*.

Trip coverage should be demonstrated across the full range of operating states, for all credited shutdown means and all credited trip parameters. Note that the number of credited shutdown means and the number of credited trip parameters can vary with the event, the reactor design, and whether there is a direct trip available.

Defining derived acceptance criteria appropriate to a particular design is the responsibility of the design authority. CNSC RD-310, *Safety Analysis for Nuclear Power Plants,* provides the requirements.

Derived acceptance criteria should be defined separately for AOOs and DBAs. The derived acceptance criteria should be set to give an appropriate level of confidence that a fundamental safety function is assured, or that a barrier to fission product release will not fail. The derived acceptance criteria should:

- be quantifiable and well understood
- account for the fact that the safety analysis is stylized, and the plant condition at the time of the accident may be significantly different from the analyzed state
- cover uncertainties in analysis, input plant and analysis parameters, as well as code validation

Direct trips are the preferred means of actuating a shutdown means, due to their robustness and low dependence on calculational models.

Diverse trip parameters measure different physical variables on the reactor, thus providing additional protection against common mode failure. Where it is impracticable to provide full diversity of trip parameters, different measurement locations, different instrument types and different processing computers should be provided. Manual trip is considered an acceptable trip parameter, if the operator has adequate time to initiate the shutdown action following unambiguous indication of the need to perform the action (in accordance with RD-337 version 2 section 8.10.4).

It is the responsibility of the design authority to identify and justify those trip parameters that can be considered “direct”. The design authority should also demonstrate that any trip parameters that are a measure of the event, but not a measure of the challenge to acceptance criteria, cannot be “masked” or “blinded” by control system action or other means.

Trips that are dependent on a number of measured variables, such as low DNBR (departure from nucleate boiling ratio) trips in PWRs can only be considered direct if all the variables are direct.

RD-337 version 2 states that *“for each credited means of shutdown, the design shall specify a direct trip parameter to initiate reactor shutdown for all AOOs and DBAs in time to meet the*

respective derived acceptance criteria. Where a direct trip parameter does not exist for a given credited means, there shall be two diverse trip parameters specified for that means.

For all AOOs and DBAs, there shall be at least two diverse trip parameters unless it can be shown that failure to trip will not lead to unacceptable consequences".

The first paragraph is interpreted to apply to each assigned individual means of shutdown credited in the plant's safety case, for all AOOs and DBAs. It requires only one trip parameter, as long as it is "direct" in nature. If a direct parameter is not available, then there must be two diverse parameters for that assigned means.

The second paragraph is interpreted to distinguish between reactor designs:

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

Table 3 of CNSC GD-310, *Guidance on Safety Analysis for Nuclear Power Plants*, provides the minimum expectations for the number of trip parameters.

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 8.10.4) and the reliability of manual shutdown meets the reliability requirements for an automatic trip.

8.4.2 Reliability

As stated in RD-337 version 2, section 7.6*, "the safety systems and their support systems shall be designed to ensure that the probability of a safety system failure on demand from all causes is lower than 10^{-3}"*.

The reliability calculation should include sensing the need for shutdown, initiation of shutdown, and insertion of negative reactivity. All elements necessary to complete the shutdown function must be included.

The reliability evaluation should be such that the reliability of the shutdown function is such that the cumulative frequency of failure to shutdown on demand can be shown to be less than 10^{-5} failures per demand, and the contribution of all sequences involving failure to shutdown to the large release frequency of the safety goals can be shown to be less than 10^{-7}/yr.

Section 7.6.2 of RD-337 version 2 requires that the shutdown function is delivered even in the presence of any single failure and even during the worst configuration from testing and maintenance. For example, for a rod based system to meet the SFC, the safety analysis may assume that the two highest worth control rods are unavailable (one for testing, and one assumed to fail on demand, in accordance with the SFC). In this case, no further testing of rods would be allowed until the rod under testing becomes available.

8.4.3 Monitoring and operator action

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

8.5 Emergency core cooling system

As stated in RD-337 version 2, "*The design shall take into account the effect on core reactivity of the mixing of ECCS water with reactor coolant water, including possible mixing due to in-leakage*." For example, PWRs often credit soluble boron in the ECCS accumulators and storage tanks, to supplement control rod insertion for long term reactivity control. The design authority should describe any reactivity control function performed by the ECCS, together with necessary limits and conditions.

ECCS designs should be proven by appropriate experimental programs and computer modelling. It should be demonstrated that there is adequate experimental evidence of ECCS effectiveness.

Examples of items that could be important in the ECCS design include:

- mechanisms for core bypassing (e.g., downcomer bypass during blowdown in PWRs, or core bypass via steam generators in CANDU)
- effects of non-condensable gas on ECCS performance
- phenomena that can impede core refill and rewet (such as periods of stagnation, steam binding in PWR steam generators, parallel channel effects in CANDU)
- effect of multi-dimensional flow in heat transport system headers in CANDU
- effect of non-uniform channel flow resistance in the CANDU core (e.g., peripheral low-flow and low-power channels having much higher flow resistance for ECCS refill)
- effect of the pressurizer

Section 8.5 of RD-337 version 2 requires that the ECCS is capable of removing residual heat over an extended period. This normally involves recovering water spilled from the break, cooling it and returning it to the reactor. It should be demonstrated that:

- the design is capable of recirculating coolant even in the presence of the maximum quantity of debris that may be present after a LOCA
- possible chemical effects in the reactor building recovery sump have been considered, and any chemical precipitates and other species (such as gels, colloids etc.) cannot significantly impair ECCS recovery flow (for example, at strainers or the heat exchangers)
- recovery actions (such as transfer to hot leg injection of ECCS, or transfer to the normal residual heat removal system) are described and shown to be achievable; long-term removal of heat by boiling in the core could potentially lead to deposition or fouling (for example, precipitation of boric acid crystals) impairing flow and heat transfer
- wear on bearings and seals has been considered – including abrasion by small particles and chemical corrosion
- natural circulation flows, where credited, are capable of providing sufficient flows and cannot be impaired by such effects as accumulation of non-condensable gas or adverse temperature distributions

Sections 7.14 and 7.16 of RD-337 version 2, describe the inspection, test and maintenance requirements which should include:

- commissioning tests to verify flow, pressure drop and (if applicable) tank isolation after injection for accumulators and other makeup tanks
- commissioning tests to verify pump head, flow and system pressure drop for pumped injection

As stated in RD-337 version 2, "*in the event of an accident when injection of emergency coolant is required, it shall not be readily possible for an operator to prevent the injection from taking place.*" This can be achieved by a variety of methods to ensure that the blocking action is intentional (such as requiring multiple actions, sequential actions, actions that are spatially separated, or actions that have to be performed by different people).

Emergency operating procedures should prohibit blocking of ECCS injection, unless there is clear and unambiguous indication that it is not needed (for example, if there is clear indication that there is adequate inventory to ensure core cooling, and that the inventory is not decreasing).

Injection of a large volume of cold water may cause pressurized thermal shock to the reactor coolant pressure boundary, or distortion of reactor internals. The design authority should demonstrate that thermal shock has been adequately addressed in the design, in terms of calculating transient fluid conditions at key locations, as well as resulting metal temperature and the corresponding stresses.

Water hammer loads may be generated by operation of valves, or by condensation when cold water is injected into steam filled systems. The design authority should demonstrate that a water hammer assessment has been performed.

8.6 Containment

8.6.1 Guidance on general requirements

The design should establish acceptance criteria for inspection, test and maintenance provisions including, as applicable:

- containment penetration isolation times
- containment spray performance
- filtered venting capability
- vacuum building actuation
- hydrogen mitigation system capability (e.g., recombiners)
- systems and equipment used for containment heat removal
- concrete condition and possible concrete degradation

The effects of release of compressed air inside the containment after isolation (for example, from air-operated valves) should be considered in calculating containment pressure loads.

Additional information:

Further information is available in:

- CSA N287.3-93 (2009) *Design Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants*, reaffirmed 2009
- CSA N290.0-11/N290.3-11 PACKAGE – Consists of *General requirements for safety systems of nuclear power plants* and N290.3-11, *Requirements for the containment system of nuclear power plants,* 2011

8.6.2 Strength of the containment structure

Section 8.6.12 of RD-337 version 2 indicates that, in addition to the specific requirements for DBAs, consideration is given to severe accident conditions, so as to provide reasonable confidence that the containment will perform as credited in DEC analysis.

For additional guidance on the design of containment structures refer to section 7.15.

8.6.3 Capability for pressure tests

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

8.6.4 Leakage

Leakage rate limits

A modern containment should be able to achieve a leakage rate less than 0.5% containment air mass per day at the maximum containment pressure from any DBA. For example, modern designs achieve a maximum leakage rate of 0.1% to 0.5% containment air mass per day at design pressure.

The safety leakage rate limit is the maximum leakage rate that will allow the dose acceptance criteria to be met for any AOO or DBA; the containment should be designed with a much lower leakage. Testing for compliance throughout the reactor life ensures that the design leakage rate is not exceeded.

Test acceptance leakage rate limits

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

Leak rate testing

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

Additional information

Further information is available in:

- CSA N287.6-11, *Pre-operational Proof and Leakage Rate Testing Requirements for Concrete Containment Structures for Nuclear Power Plants*, 2011
- CSA N287.7-08, *In-service Examination and Testing Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants*, 2008

8.6.5 Containment penetrations

As stated in RD-337 version 2, "*the number of penetrations through the containment shall be kept to a minimum*". Meeting this requirement should consider the need for separation and redundancy, and be consistent with modern designs.

8.6.6 Containment isolation

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

8.6.7 Containment airlocks

Containment openings for the movement of equipment or material through the containment should be designed to be closed quickly and reliably, in the event that isolation of the containment is required.

The need for access by personnel to the containment should be minimized. Following an accident, access to the containment for the purpose of ensuring the safety of the facility (for either short or long term) should not be necessary.

8.6.8 Internal structures of the containment

Acceptable methods should be used to calculate pressure differentials and demonstrate that there will be no loss of safety function to load-bearing structures and safety systems during AOOs and accident conditions (including consideration of hydrogen). In particular, the analyses of a large LOCA, main steamline break and design basis earthquake are expected to lead to challenging conditions. Analysis assumptions should ensure that they are conservative with respect to containment pressure, compartment differential pressure and hydrogen distribution, as well as the safety functions of SSCs.

Sufficient openings should be provided between compartments, so as to preclude potential hydrogen accumulation at dead ends. If appropriate, phenomena such as flame acceleration and standing flames should be taken into account.

The internal structures should provide adequate return flow paths for coolant (e.g. from a postulated pipe break to the containment sump) if credited in the safety analysis. The possibility of obstruction of the flow paths by debris should be considered.

For additional guidance on the design of internal structures refer to section 7.15.

Additional information

Further information is available in:

- CSA N291-08 *Requirements for Safety-Related Structures for CANDU Nuclear Power Plants*, 2008

8.6.9 Containment pressure and energy management

The means of providing systems to remove heat and reduce pressure in the containment can vary widely between designs and may employ systems such as:

- pressure suppression pools, ice condensers, vacuum chambers
- containment coolers and fans
- sump or in-containment water cooling systems used as part of a LOCA recirculation
- passive containment cooling
- containment spray or dousing systems
- free volume inside the reactor building
- containment venting through filters or scrubbers

Equipment credited in DBAs is treated as part of the containment system. For example, if credited, fan motors should be designed for operation in post-accident combustible gas conditions.

For DECs, all heat sources should be considered, including combustion of gases, metal-water reactions and the formation of solid solutions (including eutectics). The design should ensure that the heat removal capacity is consistent with analysis of containment conditions.

Air systems (such as instrument air and breathing air) should be reliably isolated after a postulated initiating event that requires containment isolation, in order to prevent containment over-pressurization and to reduce combustion and explosion effects.

8.6.10 Control and cleanup of the containment atmosphere

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

8.6.11 Coverings, coatings and materials

The design authority should demonstrate that there is confidence that interference with safety functions and other safety systems by coverings, coatings, and materials is minimized. Examples include:

- insulation materials, corrosion products, delaminated paints and coatings that may foul ECC recovery flow paths or prevent operation of equipment
- use of rubberized sealing materials that could melt or otherwise fail, and lead either to additional containment leakage or failure of a safety-related component or system
- materials that may react under post-accident conditions to generate combustible, corrosive or poisonous gases

Where large structures in containment are credited as heat sinks in computing post-accident pressure and temperature in containment, calculations should use consistent information about coating materials and their thermal properties.

8.6.12 Design extension conditions

Provisions for design extension conditions (DECs) vary greatly between designs. The claimed functionality and analysis should be supported by adequate evidence.

Containment leakage rate in DECs does not exceed the design leakage rate for a sufficient period to allow for the implementation of offsite emergency measures. This period should be demonstrated, with reasonable confidence, to be at least 24 hours.

Containment venting design should take into account such factors as:

- ignition of flammable gases
- impact on filters by containment environmental conditions, such as radioactive materials, high temperature and high humidity

Experimental or analytical evidence should be provided to demonstrate that venting will not lead to unfiltered and uncontrolled releases of radioactive materials into the environment.

8.7 Heat transfer to an ultimate heat sink

The safety significance and reliability requirements of the heat transfer to an ultimate heat sink should be addressed with respect to any claims made in the safety case for their availability to provide cooling for operational states and accident conditions.

8.8 Emergency heat removal system

The emergency heat removal system is to provide a path to ultimate heat sink, in the case that normal heat removal capabilities are not available. The purpose of this system is to prevent accident conditions from escalating and to mitigate their consequences.

Emergency heat removal relates to post-accident heat removal and may be provided by a number of systems, depending on circumstances:

- post-LOCA heat removal may be provided by ECCS (refer to section 8.5)
- for non-LOCA events, emergency heat removal may be through primary or secondary cooling systems

For all means of emergency heat removal, the design should be such that all equipment is appropriately designed to function in the class of accidents for which it is credited.

If the system credited has another role in normal operation, then the design should be such that the system will meet the requirements of a safety system when used under accident conditions. The design basis requirements for the system in this role should be provided.

Many of the actions associated with operation of the systems credited for emergency heat removal may not be initiated automatically. When there is reliance on manual operation, the review of human factors considerations should have very high importance.

Primary side emergency heat removal could be through normal shutdown cooling means. The design should be such that:

- a means of depressurizing the primary system is provided and the means of depressurization meets the requirements of a safety system, or
- the shutdown cooling system is capable of being operated at full primary pressure and temperature

Passive or non-passive (e.g., natural circulation or pumped) heat removal may be used. Non-passive systems require emergency power. Natural circulation systems should demonstrate the capability over the full range of applicable operating conditions.

Secondary side emergency heat removal that relies on water being provided to the secondary side of steam generators may be through a separate pumped supply or through a secondary depressurization and gravity feed. The water supply meets the requirements of a safety system.

8.9 Electrical power systems

Design of electrical power systems

A systematic approach should be followed to identify the electrical power systems needed in order to ensure that SSCs necessary to fulfill the safety functions are powered from electrical power supplies with appropriate safety classification and reliability

The design bases, design criteria, regulatory documents, standards, and other documents that will be used to design the electrical power systems should be specified.

For each of the electrical power systems, the design bases include:

- consideration of all modes of operation, plant states up to DECs and all credible events that could impact the electrical power systems
- reliability and availability targets for systems and key equipment
- capacity and performance requirements
- identification of all loads (i.e., the systems and equipment that require electric power to perform their safety functions) including electrical characteristics, maximum demand conditions, and safety classification
- protective schemes and coordination of protection
- specification of acceptable ranges of voltage and frequency for continuous operation of the connected loads for each electrical power system
- identification of acceptable ranges for onsite and offsite transient disturbance events that could impact electrical power systems

The design should specify the requirements for the preferred power supply (PPS) (i.e. the normal AC power supplies for plant electrical systems important to safety) and the plant interface with the transmission grid to reduce the potential for loss of normal AC power supplies.

Transmission system studies should be undertaken for reasonably expected grid system conditions and disturbances to demonstrate that normal AC power supplies will not be degraded to a level that causes unnecessary challenges to safety systems, standby and emergency power supply systems. Performance criteria should be established for:

- unit generator performance during defined frequency and voltage excursions to ensure that generators remain connected to the electrical grid
- lightning and surge protection design provisions to protect the plant electrical distribution systems against transient over-voltage conditions such as switching and lightening surges

The normal AC electrical power systems should have the capacity and capability to supply all plant electrical loads during operational states and accident conditions.

Normal AC power supplies should be designed to:

- prevent deviations from normal operation
- prevent single failures from impacting more than one redundant division of electrical power supply
- avoid preventable challenges to standby and emergency systems as a result of an electrical system disturbance, transient, or upset condition (e.g. turbine-generator trip)

Electrical power supply from the offsite power system to the onsite power system should be supplied by a minimum of two physically independent transmission lines designed and located in order to minimize~~,~~ the likelihood of their simultaneous failure. The safety analysis should provide information concerning offsite power circuits coming from the transmission system to the plant switchyard. A switchyard common to both circuits is acceptable but separate transmission line towers should be used. For some reactor designs, it might be justified that only one offsite power connection is sufficient.

Each of the plant's offsite transmission lines should have the capacity and capability to supply power to all plant electrical loads under all plant states.

A minimum of one off-site transmission line and associated PPS should be designed to be automatically available to provide power to its associated safety divisions within a few seconds following an AOO or a DBA.

A second PPS circuit should be designed to be available within a period of time commensurate with the requirement to support plant safety functions during AOOs and DBAs.

For plants designed for house load operation, the normal AC power system should be designed to accommodate generator voltage and frequency transients associated with transferring from normal operation to the house load operating mode.

Additional information

Further information is available in:

- CSA Standard N290.5-06 (R2011)- *Requirements for Electrical Power and Instrument Air Systems of CANDU Nuclear Power Plants* (Reaffirmed 2011) (Note**:** CSA N290.5 is a CANDU specific document which particularly addresses the two group design philosophy)
- IEEE 308-2001, *IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations*, 2001
- IEEE 387-1995, *IEEE Standard Criteria for Diesel-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations*, 1995
- IEEE 141-1993, *IEEE Recommended Practice for Electric Power Distribution for Industrial Plants*, (Red Book), 1993
- IEEE 242-2001, *IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems*, (IEEE Buff Book), 2001
- IEEE 279-1971, *IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations*, 1971
- IEEE 665-1995, *IEEE Standard for Generating Station Grounding* (Reaffirmed 2001)
- IEEE 1050-1996, *Guide for Instrumentation and Control Equipment Grounding in Generating Stations*, 1996
- IEEE C62.23-1995, *IEEE Application Guide for Surge Protection of Electric Generating Plants*

8.9.1 Standby and emergency power systems

Standby and emergency power sources should consist of complete electrical generating units including all support auxiliaries, a stored energy supply for starting and a dedicated and independent fuel supply system with on-site storage.

The stored energy supply for starting standby or emergency power sources should have sufficient stored energy for five consecutive start attempts.

DC power systems

DC power systems important to safety should be designed to be independent of the effects of DBAs to which they must respond, and be fully functional during and following such accidents.

Redundant load groups should each have a DC power supply division consisting of one or more batteries, one or more battery chargers, distribution system, protection and isolation features.

Each DC power supply division should be independent and physically separate from other DC divisions.

Each battery set should, without a battery charger, be capable of meeting all required load demands and conditions for the specified mission time (including duty cycles and electrical transients) during the plant states specified in the design basis, considering factors such as design margins, temperature effects, any recent discharge, and aging.

Each battery charger should have sufficient capacity to:

- maintain the battery in a fully charged state during normal operation
- restore the battery from a fully discharged state (i.e. lower voltage limit of the battery discharge cycle) to a charged state in a specified period of time while supplying the maximum DC load demand

Battery chargers should be designed to prevent transients on the AC supply from affecting the functioning of the DC system, and from DC transients affecting the AC supply.

As stated in RD-337 version 2, *the electrical power systems shall include appropriate protection, control, monitoring and testing facilities* to perform periodic capacity testing for the required mission times.

Uninterruptible AC power systems

Uninterruptible AC power systems important to safety should be designed to be independent of the effects of design basis accidents to which they must respond, and be fully functional during and following such accidents.

Each division of uninterruptible AC power system should consist of:

- an AC power supply and a DC power supply to an inverter,
- a separate AC power supply from the same division
- a feature to automatically switch between the inverter output and the separate AC supply

The electrical characteristics and requirements of the connected loads should be considered in the design so that interactions with the uninterruptible AC power system do not degrade the safety support functions of the loads supplied.

Uninterruptible AC power systems should be designed to prevent transients on the AC supply to the battery charger or on the DC supply to the inverter from affecting the functioning of the inverter.

8.9.2 Alternate AC power supply

The plant's capability to maintain critical parameters (reactor coolant inventory, containment temperature and pressure, room temperatures where critical equipment is located) and to remove decay heat from irradiated fuel should be analyzed for the period that the plant is in a SBO condition.

The capability of the DC systems required to monitor critical parameters and power the lighting and communication systems during a SBO should be evaluated for adequacy.

8.10 Control facilities

8.10.1 Main control room

There should be sufficient displays in the main control room (MCR) to monitor all safety functions.

The design should prevent unsafe manual operations (e.g., by using a logic interlocking, depending on the plant status).

Where safety and non-safety system are brought into close proximity, the design should keep adequate functional isolation and physical separation.

As stated in RD-337 version 2, "*for any PIE, at least one control room shall be habitable, and accessible by means of a qualified route"*. This indicates that there will be adequate routes through which, under emergency conditions, the operation staff from one control room can safely leave and reach another control room.

Appropriate measures are taken, including the provision of barriers between the control rooms and the external environment, and adequate information is provided for the protection of occupants of the control room against hazards such as high radiation levels resulting from accident conditions, release of radioactive material, fire, or explosive or toxic gases.

The manual initiation of safety function provides a form of defence in depth for abnormal conditions (including the common-cause failure of the automatic control and protection systems) and supports long-term post-accident operation. Manual actuation should be provided to both system and component levels, where appropriate.

The display and manual controls for critical safety functions initiated by operator action should be diverse from computerized automatic safety systems.

The MCR, secondary control room (SCR) and the emergency support centre (ESC) should have at least two diverse communications links with each other, and also with:

- areas where communications are needed during AOOs or accident conditions
- offsite emergency services
- associated facilities

Examples of diverse communications links include standard telephones, battery operated telephones, and self-powered telephones.

The diverse communication links identified above should be:

- routed such that they will not both be affected by the same failure, fires, or PIE
- capable of operating in case of loss of both the onsite and offsite power systems

8.10.1.1 Safety parameter display system

The primary function of the safety parameter display system (SPDS) is to serve as an operator aid in the rapid detection of abnormal conditions, by providing a display of plant parameters from which the safety status of operation may be assessed in the control room. The display system may include other functions that aid operating personnel in evaluating plant status. The design of the

display system should be flexible to allow for future incorporation of advanced diagnostic concepts and evaluation techniques.

The SPDS should display a minimum set of plant parameters or derived variables from which the safety status of the plant can be assessed. These parameters and variables include:

- reactivity control
- reactor core and irradiated fuel cooling
- heat removal from primary system
- reactor coolant system integrity
- radioactivity control
- containment integrity

The SPDS should:

- have sufficient availability and reliability
- not display unreliable or invalid data and alarms
- be designed to meet the specified human factor usability requirements

The display of abnormal operating conditions significant to safety should be distinctly different in appearance from the display depicting normal operating conditions.

The information displayed by the SPDS display should be presented in ways that are easy for the operators to read and understand.

The display should be designed to improve the operator's recognition, comprehension, and detection of abnormal operating states.

8.10.2 Secondary control room

Sufficient controls, indications, alarms and displays should be provided in the SCR to bring the plant to a safe state, to provide assurance that a safe state has been reached and maintained, and to provide operators with information on the status of the plant and the trends in key plant parameters.

Suitable provisions outside the MCR should be made for transferring control to the SCR whenever the MCR is abandoned.

Refer to section 8.10.1 for other applicable design guidance and expectations.

8.10.3 Emergency support centre

The design provides an emergency support centre (ESC) to facilitate the following functions:

- management of overall emergency response
- coordination of radiological and environmental monitoring
- determination of recommended public protective actions
- coordination of emergency response activities with federal, provincial, and municipal agencies

Facilities should be provided in the ESC for the acquisition, display, and evaluation of all radiological, meteorological, and plant system data pertinent to determine offsite protective measures.

Facilities used in performing essential ESC functions should be located within the ESC complex. However, supplemental calculations and analytical support of ESC evaluations may be provided from facilities outside the ESC.

The ESC data system should be designed to achieve an appropriate level of reliability.

The location of the ESC should ensure optimum functional and reliability characteristics for carrying out its specific functions.

8.10.4 Guidance on equipment requirements for accident conditions

The design should ensure that no failure of monitoring or display systems will influence the functioning of other safety systems.

As stated in RD-337 version 2, "*if operator action is required for actuation of any safety system or safety support system equipment following indication of the necessity for operator action inside the control rooms, there is at least 30 minutes available before the operator action is required*".

The time available to perform the actions should be based on the analysis of the plant response to AOOs and accident conditions, using realistic assumptions. The time required for operator action should be based on a human factors engineering (HFE) analysis of operator response time, which (in turn) is based on a documented sequence of operator actions. Uncertainties in the analysis of time required are identified and assessed. An adequate time margin should also be added to the analyzed time.

If operator action is required for actuation of any safety function, other than meeting the requirements of RD-337 version 2, the analysis should also demonstrate that:

- there is sufficient time available for the operator to perform the required manual action
- the operator can perform the actions correctly and reliably in the time available

The sequence of actions should use only alarms, controls, and displays that would be available in locations where the tasks will be performed and should be available in all scenarios analysed. A preliminary validation should be conducted, to provide independent confirmation to the validity of the estimated "time available" and "time required" for human actions. The preliminary validation results should support the conclusion that the time required, including margin, to perform individual steps and the overall documented sequence of manual operator actions are reasonable, realistic, repeatable, and bounded by the initial analysis.

An integrated system test should also be conducted, to validate the manual actions credited in the safety analysis, using a full-scale simulator. Tasks conducted outside the control room should be included in the integrated system validations.

Additional information

Further information is available in:

- CSA N290.4-11, *Requirements for Reactor Control Systems of Nuclear Power Plants*, 2011
- IEC 60964-2009, *Nuclear power plants - Control rooms – Design*, 2009
- IEC 60965-2009, *Nuclear power plants - Control rooms - Supplementary control points for reactor shutdown without access to the main control room*, 2009
- U.S. NRC NUREG-0696, *Functional Criteria for Emergency Response Facilities*, 1981

8.11 Waste treatment and control

8.11.1 Control of liquid releases to the environment

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

8.11.2 Control of airborne material within the plant

Radiological zones may be established in the NPP design, according to the potential contamination hazards in each area. The ventilation system should be designed such that any air movement between various zones, due to pressure difference, takes place from an area of lower contamination to an area of increasing contamination. Recirculation of air within one zone or room may be permitted, but recirculation from the central ventilation system is not.

8.11.3 Control of gaseous releases to the environment

A gaseous waste management system is designed to collect all active or potentially active gases, vapours, or airborne particulates which may occur, in order to monitor and filter the effluent prior to its release to the atmosphere. The filter units should be placed in a fully enclosed room, with sufficiently thick concrete walls and floors, so as to protect station personnel from radiation. Monitors are provided in the stack to detect any activity in the effluent. Gaseous activity from areas such as the fuel storage pools, service areas and active laboratories are also monitored and filtered before discharge to the atmosphere.

Additional information

Further information is available in:

- CNSC G-129, *Keeping Radiation Exposures and Doses "As Low as Reasonably Achievable (ALARA)*", 2004
- CSA N292.3-08, *Management of Low-and Intermediate-level Radioactive Waste*, 2008
- IAEA Safety Standards Series GS-G-3.3, *The Management System for the Processing, Handling and Storage of Radioactive Waste Safety Guide*, 2008

8.12 Fuel handling and storage

The design provides the basis for the fuel handling and storage systems. The design includes provisions for monitoring and alarming, for criticality prevention, and for shielding, handling, storage, cooling, transfer and transport of nuclear fuel.

Considerations such as packaging, fuel accounting systems, storage, criticality prevention, fuel integrity control, foreign material exclusion procedures and fuel security, should be taken into account in the design.

The requirements for criticality safety requirements are provided in RD-327, *Nuclear Criticality Safety*. Comprehensive guidance on criticality safety and complete technical reference is provided in GD-327, *Guidance on Nuclear Criticality Safety*.

The design should include provisions to prevent contamination of the fuel by foreign materials (greases, tramp uranium etc.) and prevent the spread of contamination into the reactor.

Additional information

Further information is available in:

- IAEA NS-G-1.4, *Design of Fuel Handling and Storage Systems for Nuclear Power Plants,* 2003
- IAEA NS-G-2.5, *Core Management and Fuel Handling for Nuclear Power Plants*, 2002
- ANSI/ANS-57.1-1992, American National Standard *Design Requirements for Light Water Reactor Fuel Handling Systems* (as applicable), 1992

8.12.1 Handling and storage of non-irradiated fuel

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

8.12.2 Handling and storage of irradiated fuel

Hydrogen mitigation in the spent fuel pool area is particularly important, if it is envisaged that the pool may be used for fission product scrubbing, as part of containment venting.

8.12.3 Detection of failed fuel

As stated in RD-337 version 2, "*the design shall provide a means for allowing reliable detection of fuel defects in the reactor, and the subsequent removal of failed fuel, if action levels are exceeded"*.

The design should specify the criterion for continued operation with failed fuel in the core, or to unload the fuel assembly from the core. The amount of failed fuel left in the core may impact the safety case of the design.

The design should allow for the removal of failed fuel in as timely a manner as possible. The design should provide for the inspection and quarantine of failed fuel in the fuel handling and storage facilities.

8.13 Radiation protection

The NPP should be divided into zones based on predicted dose rates, radioactive contamination levels, concentration of airborne radionuclides, access requirements and specific requirements (such as the need to separate safety trains). The criteria and rationale for radiation zone designations – including zone boundaries for normal, refuelling and accident conditions – should be provided. These criteria should be used as the basis for the radiation shielding design.

From a radiological protection perspective, careful assessment should be made of the access requirements for operation, inspection, maintenance, repair, replacement and decommissioning of equipment; these considerations should be incorporated into the design. The design should also provide lay down space for special tools and ease for servicing activities. The design should also have features such as platforms or walkways, stairs, or ladders that permit prompt accessibility for servicing or inspection of components located in higher radiation zones.

The use of remote technology for maintenance and surveillance in high radiation areas should be considered and incorporated. Preference should be given to the use of appropriate engineering controls and design features, over process or administrative controls.

Reliable equipment that requires minimum surveillance, maintenance, testing and calibration should be chosen.

Operating experience should be reflected in the criteria and rationale provided in the design.

Additional information

Further information is available in:

- IAEA Safety Standards Series NS-G-1.13, *Radiation Protection Aspects of Design for Nuclear Power Plants*, 2005
- CNSC G-129, *Keeping Radiation Exposures and Doses "As Low as Reasonably Achievable (ALARA)"*, 2004
- IAEA Safety Guide RS-G-1.1, *Occupational Radiation Protection,* 1999

8.13.1 Design for radiation protection

Shielding should be designed based on the zone delineation described in 8.13. The shielding design criteria (including the methodology for shield parameters and choice of shield material) should be provided. In establishing specifications for shielding, account should be taken of the buildup of radioactive materials over the lifetime of the NPP.

8.13.2 Access and movement control

Provisions should be made for controlling the exit(s) from the radiation zones. Monitoring of personnel and materials should be established at the access and egress points for the radiation zones. Access to areas of high dose rates or high levels of radioactive contamination should be controlled through the provision of lockable doors and interlocks. Routes for personnel through radiation zones and contamination zones should be minimized, in order to reduce the time spent in transiting these zones. Radiation zones where personnel spend substantial time should be designed to the lowest practical dose rates and ALARA.

Within the radiation zones, changing areas for personnel should be provided at selected locations, to prevent the spread of radioactive contamination during maintenance and normal operation. Within these change areas, consideration should be given to the need for decontamination facilities for personnel, radiation monitoring instruments and storage areas for protective clothing. A physical barrier should clearly separate the clean area from the potentially contaminated area.

8.13.3 Monitoring

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

8.13.4 Sources

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

8.13.5 Monitoring environmental impact

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

Additional guidance can be found in CSA N288.4-M90 (R2008), *Guidelines for Radiological Monitoring of the Environment*.

9.0 Safety Analyses

9.1 General

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

9.2 Analysis objectives

As described in the *Class I Nuclear Facilities Regulations*, a preliminary safety analysis report demonstrating the adequacy of the NPP design is required for an application for a licence to construct a Class I nuclear facility. A final safety analysis report reflecting the "as-built" design is required for an application for a licence to operate a Class I nuclear facility.

9.3 Hazards analysis

The objective of the hazards analysis is to determine the adequacy of protection of the nuclear power plant against internal and external hazards, while taking into account the plant design and site characteristics. To ensure the availability of required safety functions and operator actions, all the SSCs important to safety (including the main control room, secondary control room and emergency support centre) should be adequately protected against relevant internal and external hazards.

The hazards analysis should establish a list of relevant internal and external hazards that may affect plant safety. For the relevant hazards, the review should demonstrate, by using deterministic and probabilistic techniques, that the probability or consequences of the hazard are sufficiently low so that no specific protective measures are necessary, or that the preventive and mitigating measures against the hazard are adequate.

All internal and external hazards are considered as part of postulated initiating events (PIEs). The hazards that make an insignificant contribution to plant risk can be screened out from the detailed analysis; however, the rationale for this screening should be provided. The remaining PIEs constitute the scope of the hazard analysis. The design should specify design basis hazards, establishing clear criteria. The design basis hazards should be analyzed using the deterministic safety analysis rules and criteria provided in section 9.4. Such analysis should also demonstrate the adequacy of the complementary design features in mitigating radiological consequences of design extension conditions.

The hazards analysis should demonstrate that the design incorporates sufficient safety margins to mitigate cliff-edge effects.

Additional information

Further information is available in:

- CNSC RD-346, *Site Evaluation for New Nuclear Power Plants*, 2008
- CNSC RD/GD-369, *Licence Application Guide: Licence to Construct a Nuclear Power Plant*, 2011
- CSA N293-07, *Fire protection for CANDU nuclear power plants*, 2007

- CSA N289.4-M86, *Testing procedures for Seismic Qualification of CANDU Nuclear Power Plant*, reaffirmed 2008
- IAEA NS-G-3.1, *External Human Induced Events in Site Evaluation for Nuclear Power Plants*, 2002
- IAEA SSG-18, *Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations*, 2011
- IAEA SSG-9, *Seismic Hazards in Site Evaluation for Nuclear Installations*, 2010
- IAEA NS-G-1.5, *External Events Excluding Earthquakes in the Design of Nuclear Power Plants*, 2003
- IAEA NS-G-3.4, *Meteorological Events in Site Evaluation for Nuclear Power Plants*, 2003
- IAEA NS-G-3.5, *Flood Hazard for Nuclear Power Plants on Coastal and River Sites*, 2003
- IAEA NS-G-1.6, *Seismic Design and Qualification for Nuclear Power Plants*, 2003
- IAEA NS-G-3.3, *Evaluation of Seismic Hazards for Nuclear Power Plants*, 2002
- IAEA NS-G-1.7, *Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants*, 2004
- IAEA NS-G-1.11, *Protection Against Internal Hazards other then Fires and Explosions in the Design of Nuclear Power Plants*, 2004

9.4 Deterministic safety analysis

Information on deterministic safety analysis can be found in:

- CNSC RD-310, *Safety Analysis for Nuclear Power Plants*, 2008
- CNSC GD-310, *Guidance on Safety Analysis for Nuclear Power Plants*, 2012
- CNSC RD/GD-369, *Licence Application Guide: Licence to Construct a Nuclear Power Plant*, 2011
- CSA N286.7-99, *Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants*, reaffirmed 2007
- IAEA SSG-2, *Deterministic Safety Analysis for Nuclear Power Plants*, 2009
- IAEA NS-G-1.2, *Safety Assessment and Verification for Nuclear Power Plants*, 2001

9.5 Probabilistic safety analysis

Information on probabilistic safety analysis can be found in:

- CNSC S-294, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*, 2005
- CNSC RD/GD-369, *Licence Application Guide: Licence to Construct a Nuclear Power Plant*, 2011
- IAEA SSG-3, *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants*, 2010
- IAEA SSG-4, *Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants*, 2010
- IAEA, Safety Report Series No.10, *Treatment of Internal Fires in Probabilistic Safety Assessment for Nuclear Power Plants*, 1998
- IAEA, Safety Series No. 50-P-7, *Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants*, 1995
- IAEA Safety Series No. 50-P-10, *Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants*, 1995

- IAEA Safety Reports Series No. 25, *Review of Probabilistic Safety Assessments by Regulatory Bodies,* 2002
- ASME/ANS RA-Sa-2009, *Standard for Level 1/Large Early Release Frequency PRA for Nuclear Power Plant Applications*, 2009

10.0 Environmental Protection and Mitigation

10.1 Design for environmental protection

The design should incorporate the "best available technology and techniques economically achievable" (BATEA) principle for aspects of the design related to environmental protection.

10.2 Release of nuclear and hazardous substances

The design authority should demonstrate adherence to the principles of optimization and pollution prevention, through the demonstration of the application of the ALARA and BATEA principles.

The lifecycle assessment referenced in RD-337 version 2 should include an initial estimate of the total inventory of all radioactive and hazardous materials which will be used or generated during the plant's lifetime. All systems at the reactor site should be accounted for, and consideration given to substances such as hydrazine, carbon dioxide, CFC (chloro-fluoro-carbons), VOC (volatile carbon compounds), NO_x (nitrogen oxides), TOC (total organic carbon), dust or suspended solids, detergent, solvents, heavy metals (e.g., copper), chlorine, phosphorous, ammonia and ammonium, morpholine, oil or grease. The nature of such substances (solid, liquid, gas, pH, temperature), their management and the wastes created should be accounted for.

The selected condenser cooling technology should incorporate the latest in mitigation technology and techniques.

Additional information

Further information is available in:

- CNSC P-223, *Protection of the Environment,* 2001
- CNSC S-296, *Environmental Protection Policies, Programs and Procedures at Class I Nuclear Facilities and Uranium Mines and Mills*, 2006
- CNSC G-296, *Developing Environmental Protection Policies, Programs and Procedures at Class I Nuclear Facilities and Uranium Mines and Mills*, 2006

11.0 Alternative Approaches

Sufficient information for this section is found in RD-337 version 2, *Design of New Nuclear Power Plants*. No additional guidance is provided.

Abbreviations

ALARA	as low as reasonably achievable
AOO	anticipated operational occurrence
BATEA	best available technology and techniques economically achievable
BDBA	beyond design basis accident
BDBT	beyond design basis threat
CCF	common-cause failure
CHF	critical heat flux
DBA	design basis accident
DBE	design basis earthquake
DBT	design basis threat
DEC	design extension condition
ECCS	emergency core cooling system
EHRS	emergency heat removal system
EMI	electromagnetic interface
EPS	emergency power supply
EQ	environmental qualification
ESC	emergency support centre
GSS	guaranteed shutdown state
HCLPF	high confidence low probability of failure
HF	human factors
I&C	instrumentation and control
LBB	leak before break
LOCA	loss of coolant accident
LWR	light water reactor
MCR	main control room
MSIV	main steam isolation valve
OLC	operational limits and conditions
PIE	postulated initiating event
PPS	preferred power supply
PSA	probabilistic safety assessment
PWR	pressurized water reactor
RCS	reactor coolant system
SBO	station blackout
SCR	secondary control room
SFC	single failure criterion
SPDS	safety parameter display system
SSCs	structures, systems, and components
TRA	threat and risk assessment
UHS	ultimate heat sink

Glossary

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

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

For the purposes of this document, accidents include design basis accidents and beyond design basis accidents. Accidents exclude anticipated operational occurrences, which have negligible consequences from the perspective of protection or safety.

accident conditions
Deviations from normal operation more severe than anticipated operational occurrences, including design basis accidents and design extension conditions.

aging management
Engineering, operations and maintenance actions to control, within acceptable limits, the effects of physical aging and obsolescence of structures, systems and components.

anticipated operational occurrence
An operational process deviating from normal operation, which is expected to occur at least once during the operating lifetime of a facility, but which, in view of the appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.

best estimate
Unbiased estimate, obtained by the use of a mathematical model, calculation method or data to realistically predict behaviour and important parameters.

beyond design basis threat
Threat conditions more severe than a design basis threat, which may result in structural degradation and may involve containment degradation.

cliff-edge effect
A large increase in the severity of consequences caused by a small change of conditions. Note: cliff-edges can be caused by changes in the characteristics of the environment, the event or changes in the plant response.

combustion
A chemical process that involves oxidation sufficient to produce heat or light.

commissioning
A process of activities intended to demonstrate that the installed structures, systems, components and equipment perform in accordance with their specifications and design intent before they are put into service.

common-cause event
An event that leads to common-cause failures.

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

complementary design feature
A design feature added to the design as a stand-alone structure, system or component (SSC) or added capability to an existing SSC to cope with design extension conditions.

confinement
A continuous boundary without openings or penetrations (such as windows) that prevents the transport of gases or particulates out of the enclosed space.

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.

containment
A confinement structure designed to maintain confinement at both high temperature and pressures, and for which isolation valving on penetrations is permitted.

core damage
Core degradation resulting from event sequences more severe than design basis accidents.

crediting
Assuming the correct operation of a structure, system or component or correct operator action, as part of an analysis.

critical groups
A group of members of the public that is reasonably homogeneous with respect to its exposure for a given radiation source, and is typical of individuals receiving the highest effective dose or equivalent dose (as applicable) from the given source.

cyber security
Protection of digital computer-based systems or components throughout the lifecycle of the system from threats and malicious actions, or inadvertent actions that result in unintended consequences; this includes protection for unauthorized, unintended and unsafe modifications to the system, and for unauthorized disclosure and retention of information, software or data associated with the system that could be used to perform malicious or misguided acts that could affect the functionality and performance of the system.

design authority
The entity that has overall responsibility for the design process, or the responsibility for approving design changes and for ensuring that the requisite knowledge is maintained.

design basis
The range of conditions and events taken explicitly into account in the design of the facility, according to established criteria, such that the facility can withstand them without exceeding authorized limits by the planned operation of safety systems.

design basis accident
Accident conditions for 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.

design basis threat
A set of malevolent acts that the CNSC considers possible.

design extension conditions
Accident conditions, not considered design basis accidents, which are taken into account in the design of the facility.

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.

direct trip parameter
A process or neutronic parameter that is used to trigger a shutdown action and that is a direct measure of the challenge to derived acceptance criteria or a direct measure of the event taking place.

division
The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components.

diversity
The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common-cause failure.

environment
The components of the Earth, including:

1. land, water, and air, including all layers of the atmosphere
2. all organic and inorganic matter and living organisms
3. interacting natural systems that include components referred to in (1) and (2)

equipment qualification
The process for certifying equipment as having satisfied the requirements for operability under conditions relevant to its safety function(s). This includes the generation and maintenance of evidence to ensure that equipment will operate on demand, under specified service conditions, to meet system performance requirements.

exclusion zone
Pursuant to section 1 of the *Class I Nuclear Facilities Regulations,* a parcel of land within or surrounding a nuclear facility, on which there is no permanent dwelling and over which a licensee has the legal authority to exercise control.

external event
Events unconnected with the operation of a facility or activity that could have an effect on the safety of the facility or activity.
Note: External events include, but are not limited to, earthquakes, floods, and hurricanes.

fail-safe design
Design whose most probable failure modes do not result in a reduction of safety.

fire
A process of combustion characterized by heat emission and accompanied by smoke or flame, or both.

hazard analysis
The process used to systematically identify and assess hazards to evaluate the potential internal, external, human-made and natural events that can cause the identified hazards to initiate faults that develop into accidents.

heat sink
A system or component that provides a path for heat transfer from a source (such as heat generated in the fuel) to a large heat-absorbing medium.

human factors
Factors that influence human performance as it relates to the safety of the nuclear power plant, including activities during design, construction, and commissioning, operation, maintenance and decommissioning phases.

independent systems
Systems, each of which is capable of performing its required function while remaining unaffected by the operation or failure of another system.

internal event
An event internal to the nuclear power plant that results from human error or failure in a structure, system, or component.

leak-before-break
A situation where leakage from a flaw is detected during normal operation, allowing the reactor to be shut down and depressurized before the flaw grows to the critical size for rupture.

malevolent act
An illegal action or an action that is committed with the intent of causing wrongful harm.

management system
A set of interrelated or interacting elements (system) for establishing policies and objectives and enabling the objectives to be achieved in an efficient and effective way. The management system integrates all elements of an organization into one coherent system to enable all of the organization's objectives to be achieved. These elements include the structure, resources, and processes. Personnel, equipment, and organizational culture as well as the documented policies and processes are parts of the management system. The organization's processes have to address the totality of the requirements on the organization as established in, for example, IAEA safety standards and other international codes and standards.

missile generation
The hazard associated with the sudden high-speed propulsion of debris.

mission time
The duration of time within which a system or component is required to operate or be available to operate and fulfill its function following an event.

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

nuclear power plant
Any fission reactor installation 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*.

offsite power
The AC power supplied from the transmission system (grid), to the plant electrical power distribution systems.

onsite power
Power supplied from plant alternating current (AC) power systems, direct current (DC) power systems and uninterruptible AC power systems.

operational limits and conditions
A set of rules setting forth parameter limits and the functional capability and performance levels of equipment and personnel, which are approved by the regulatory body for safe operation of an authorized facility. This set of limits and conditions is monitored by, or on behalf of the operator, and can be controlled by the operator.

operational states
States defined under normal operation and anticipated operational occurrences.

plant design envelope
The range of conditions and events (including DECs) that are explicitly taken into account in the design of the nuclear power plant, such that it can be reasonably expected that significant radioactive releases would be practically eliminated by the planned operation of process and control systems, safety systems, safety support systems and complementary design features.

plant states
A configuration of nuclear power plant components, including the physical and thermodynamic states of the materials, and the process fluids in them.

postulated initiating event
An event identified in the design as capable of leading to an anticipated operational occurrence or a design basis accident, or a beyond design basis accident. This means that a postulated initiating event is not necessarily an accident itself; rather it is the event that initiates a sequence that may lead to an anticipated operational occurrence, a design basis accident, or a beyond design basis accident, depending on the additional failures that may occur.

practicable
Technically feasible and justifiable while taking cost-benefit considerations into account.

practically eliminated
The possibility of certain conditions occurring being physically impossible or with a high level of confidence to be extremely unlikely to arise.

preferred power supply
The power supply from the transmission system or the plant generator to the electrical distribution systems classified as important to safety. This is the preferred power supply for safety support functions for normal operation, AOOs, DBAs and DECs.

pressure boundary
A boundary of any pressure-retaining vessel, system, or component of a nuclear or non-nuclear system.

probabilistic safety assessment
A comprehensive and integrated assessment of the safety of the nuclear power plant. 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 nuclear power plant, as follows:

1. 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
2. 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
3. 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

process
Set of interrelated activities that transform inputs into outputs.

process system
A system whose primary function is to support (or contribute to) the production of steam or electricity.

residual heat
The sum of heat originating from radioactive decay, fission in the fuel in the shutdown state, and the heat stored in reactor-related structures, systems and components.

safe shutdown state
A state characterized by subcriticality of the reactor in which the fundamental safety functions can be ensured and maintained stable for a long time.

safeguards
A system of international inspections and other verification activities undertaken by the International Atomic Energy Agency (IAEA) in order to evaluate, on an annual basis, Canada's compliance with its obligations pursuant to the safety agreements between Canada and the IAEA.

safety analysis
Analysis, by means of appropriate analytical tools, which establishes and confirms the design basis for the items important to safety, and ensures that the overall plant design is capable of meeting the acceptance criteria for each plant state.

safety culture
The characteristics of the work environment, such as values, rules and common understandings, which influence the employees' perceptions and attitudes about the importance placed on safety by their organization.

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 AOOs and DBAs are not exceeded. It may include certain safety and safety support systems, and any interacting process system.

safety margin
A margin to a value of a safety variable for a barrier or a system at which damage or loss would occur. Safety margins are considered for those systems and barriers whose failure could potentially contribute to radiological releases.

safety support system
A system designed to support the operation of one or more safety systems.

safety system
A system important to safety, 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.

severe accident
Accident conditions more severe than a design basis accident and involving significant core degradation

shutdown state
A state characterized by subcriticality of the reactor. At shutdown, automatic actuation of safety systems could be blocked and support systems may remain in abnormal configurations.

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

station blackout
A complete loss of alternating current (AC) power from offsite and onsite main generator, standby and emergency power sources. Note that it does not include failure of uninterruptible AC power supplies (UPS) and DC power supplies. It also does not include failure of alternate AC power.

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

Structures are the passive elements: buildings, vessels, shielding etc. A system comprises several components, assembled in such a way as to perform a specific (active) function. A component is a

discrete element of a system. Examples are wires, transistors, integrated circuits, motors, relays, solenoids, pipes, fittings, pumps, tanks and valves etc.

SSCs important to safety
Structures, systems and components of the nuclear power plant associated with the initiation, prevention, detection or mitigation of any failure sequence and that may have the most significant impact in reducing the possibility of damage to fuel, associated release of radionuclides or both.

threat and risk assessment
A threat and risk assessment is an evaluation of the adequacy of an existing or a proposed physical protection system designed to safeguard against:

1. intentional acts that could pose a threat to the security of the nuclear facility
2. the exploitation of weaknesses in the physical protection measures of a nuclear facility

trip parameter
A measurement of a variable that is used to trigger a safety system action when the trip parameter set point is reached.

trip parameter set point
Trip parameter value at which activation of a safety system is triggered.

ultimate heat sink
A medium to which the residual heat can always be transferred and is normally an inexhaustible natural body of water or the atmosphere.

usability
The extent to which a product can be used by specified users, to achieve specified goals, with effectiveness, efficiency, and satisfaction in a specified context of use.

vital area
As defined in the *Nuclear Security Regulations,* a vital area means an area inside a protected area containing equipment, systems, devices or a nuclear substance, the sabotage of which would or would likely pose an unreasonable risk to the health and safety of persons arising from exposure to radiation.

CNSC References

1. S-98 rev 1, *Reliability Programs for Nuclear Power Plants*, 2005
2. S-210, *Maintenance Programs for Nuclear Power Plants,* 2007
3. RD-310, *Safety Analysis for Nuclear Power Plants*, 2008
4. GD-310, *Guidance on Safety Analysis for Nuclear Power Plants*, 2012
5. RD-327, *Nuclear Criticality Safety*, 2010
6. GD-327, *Guidance for Nuclear Criticality Safety*, 2010
7. RD-334, *Aging Management for Nuclear Power Plants*, 2011
8. RD-336, *Accounting and Reporting of Nuclear Material,* 2010
9. GD-336, *Guidance for Accounting and Reporting of Nuclear Material*, 2010
10. RD-346, *Site Evaluation for New Nuclear Power Plants*, 2008
11. RD/GD-369, *Licence Application Guide: Licence to Construct a Nuclear Power Plant*, 2011
12. G-129 rev. 1, *Keeping Radiation Exposures and Doses "As Low as Reasonably Achievable (ALARA)",* 2004
13. G-219, *Decommissioning Planning for Licensed Activities*, 2000
14. G-225, *Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills*, 2001
15. G-274, *Security Programs for Category I or II Nuclear Material or Certain Nuclear Facilities*, 2003
16. P-119*, Policy on Human Factors, 2000*
17. G-276, *Human Factors Engineering Program Plans*, 2003
18. G-278, *Human Factors Verification and Validation Plans*, 2003
19. G-306, *Severe Accident Management Programs for Nuclear Reactors*, 2006
20. G-323, *Ensuring the Presence of Sufficient Qualified Staff at Class I Nuclear Facilities – Minimum Staff Complement*, 2007
21. S-294, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*, 2005
22. P-223, *Protection of the Environment,* 2001
23. S-296, *Environmental Protection Policies, Programs and Procedures at Class I Nuclear Facilities and Uranium Mines and Mills*, 2006
24. G-296, *Developing Environmental Protection Policies, Programs and Procedures at Class I Nuclear Facilities and Uranium Mines and Mills*, 2006
25. G-208*, Transportation Security Plans for Category I, II or III Nuclear Material*, 2003
26. RD-363, *Nuclear Security Officer Medical, Physical, and Psychological Fitness*, 2008

Additional Information

The following documents contain additional information that may be of interest to persons involved in the design of nuclear power plants. The latest or agreed upon edition should be used.

Canadian Standards Association (CSA)

1. N285.0-08, *General requirements for pressure-retaining systems and components in CANDU nuclear power plants*, 2008
2. N285.4-09, *Periodic inspection of CANDU nuclear power plant components*, 2009
3. N285.5-08, *Periodic inspection of CANDU nuclear power plant containment components*, 2008
4. N286-05, *Management System Requirements for Nuclear Power Plants*, reaffirmed 2010
5. N286.7-99, *Quality Assurance of Analytical, Scientific, and Design Computer Programs for Nuclear Power Plants*, reaffirmed 2007
6. N287.3-93 (2009), *Design Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants*, reaffirmed, 2009
7. N287.6-11, *Pre-operational Proof and Leakage Rate Testing Requirements for Concrete Containment Structures for Nuclear Power Plants*, 2011
8. N287.7-08, *In-service Examination and Testing Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants,* 2008
9. N286.7.1-09, *Guideline for the application of N286.7-99, Quality assurance of analytical, scientific, and design computer programs for nuclear power plants*, 2009
10. CAN/CSA-N288.2-M91 (R2008*), Guidelines for Calculating Radiation Doses to the Public from a Release of Airborne Radioactive Material under Hypothetical Accident Conditions in Nuclear Reactors,* 2008
11. N288.4-M90 (R2008), *Guidelines for Radiological Monitoring of the Environment,* reaffirmed 2008
12. N289 series on seismic design and qualification
13. N289.3-10, *Design procedures for seismic qualification of nuclear power plants*, 2010
14. N289.4-M86, *Testing procedures for Seismic Qualification of CANDU Nuclear Power Plant,* reaffirmed 2008
15. N289.5-M91, *Seismic, Instrumentation Requirements for CANDU Nuclear Power Plants*, reaffirmed 2008
16. N290.0-11/N290.3-11 PACKAGE – Consists of *General requirements for safety systems of nuclear power plants* and N290.3-11, *Requirements for the containment system of nuclear power plants*, 2011
17. N290.1-80, *Requirements for the Shutdown Systems of CANDU Nuclear Power Plants*, reaffirmed 2011
18. N290.4-11, *Requirements for Reactor Control Systems of Nuclear Power Plants*, 2011
19. N290.5-06 (R2011)- *Requirements for Electrical Power and Instrument Air Systems of CANDU Nuclear Power Plants* (Reaffirmed 2011)

20. N290.6-09, *Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of an Accident*, 2009

21. N290.13-05, *Environmental Qualification of Equipment for CANDU Nuclear Power Plants,* 2009

22. N290.14-07, *Qualification of pre-developed software for use in safety related instrumentation and control applications in nuclear power plants,* 2007

23. N290.15-10, *Requirements for the safe operating envelope of nuclear power plants*, 2010

24. N291-08, *Requirements for Safety-Related Structures for CANDU Nuclear Power Plants*, 2008

25. N292.3-08, *Management of Low-and Intermediate-level Radioactive Waste,* 2008

26. N293-07, *Fire Protection for CANDU Nuclear Power Plants*, 2007

27. N294-09, *Decommissioning of Facilities Containing Nuclear Substances*, 2009

28. A23.3-04 (R2010), *Design of Concrete Structures*, reaffirmed 2010

29. S16-09, *Design of Steel Structures*, 2009

30. S304.1-04 (R2010), *Design of Masonry Structures*, 2010

International Atomic Energy Agency (IAEA)

1. NS-R-1, *Safety of Nuclear Power Plant: Design*, 2000

2. SSR 2/1, *Safety of Nuclear Power Plants: Design*, 2012 (revision of NS-R-1)

3. SSR 2/2, *Safety of Nuclear Power Plants: Commissioning and Operation*, 2011

4. Safety Series No. 110, *The Safety of Nuclear Installations*, 1993

5. 75-INSAG-3 Rev. 1, INSAG-12, *Basic Safety Principles for Nuclear Power Plants*, 1999

6. INSAG-10*, Defence in Depth in Nuclear Safety*, 1996

7. GS-R-2*, Preparedness and Response for a Nuclear or Radiological Emergency,* 2002

8. GS-R-3, *The Management System for Facilities and Activities*, 2006

9. GS-G-3.3*, The Management System for the Processing, Handling and Storage of Radioactive Waste Safety Guide,* 2008

10. GS-G-3.5, *The Management System for Nuclear Installations*, 2009

11. INSAG-19, *Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life*, 2003

12. General Safety Requirements Part 4, *Safety Assessment for Facilities and Activities*, 2009

13. Safety Reports Series No. 46, *Assessment of Defence in depth for Nuclear Power Plants*, 2005

14. Safety Series No. 50-P-1, *Application of the Single Failure Criterion*, 1990

15. Safety Series No. 50-P-7, *Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants*, 1995

16. Safety Series No. 50-P-10, *Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants*, 1995

17. Safety Report Series No. 8, *Preparation of Fire Hazard Analysis for Nuclear Power Plants*, 1998

18. TECDOC-967 (Rev.1), *Guidance and considerations for the implementation of INFCIRC/225/Rev.4, The Physical Protection of Nuclear Material and Nuclear Facilities*, 2002

19. TECDOC-1276, *Handbook on the physical protection of nuclear materials and facilities*, 2002

20. TECDOC-1657, *Design Lessons Drawn from the Decommissioning of Nuclear Facilities*, 2011

21. WS-G-2.1, *Decommissioning of Nuclear Power Plants and Research Reactors Safety Guide*, 1999

22. Safety Reports Series No. 3, *Equipment qualification in operational nuclear power plants: upgrading, preserving and reviewing*, 1999

23. Safety Reports Series No. 25, *Review of Probabilistic Safety Assessments by Regulatory Bodies,* 2002

24. Safety Guide RS-G-1.1, *Occupational Radiation Protection*, 1999

25. NS-G-1.2, *Safety Assessment and Verification for Nuclear Power Plants*, 2001

26. NS-G-1.4, *Design of Fuel Handling and Storage Systems in Nuclear Power Plants Safety Guide,* 2003

27. NS-G-1.5, *External Events Excluding Earthquakes in the Design of Nuclear Power Plants*, 2003

28. NS-G-1.6, *Seismic Design and Qualification for Nuclear Power Plants*, 2003

29. NS-G-1.8, *Design of Emergency Power Systems of Nuclear Power Plants*, 2004

30. NS-G-1.10, *Design of Reactor Containment Systems for Nuclear Power Plants*, 2004

31. NS-G-1.11, *Protection Against Internal Hazards other then Fires and Explosions in the Design of Nuclear Power Plants,* 2004

32. NS-G-1.12, *Design of the Reactor Core for Nuclear Power Plants*, 2005

33. NS-G-1.13*, Radiation Protection Aspects of Design for Nuclear Power Plants,* 2005

34. NS-G-2.1, *Fire Safety in Operation of Nuclear Power Plants*, 2000

35. NS-G-2.2, *Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants*, 2000

36. NS-G-2.5, *Core Management and Fuel Handling for Nuclear Power Plants*, 2002

37. NS-G-2.6, *Maintenance, Surveillance and In-Service Inspection in Nuclear Power Plants*, 2002

38. NS-G-2.9, *Commissioning for Nuclear Power Plants*, 2003

39. NS-G-2.11, *A System for the Feedback of Experience from Events in Nuclear Installations*, 2006

40. NS-G-3.1, *External Human Induced Events in Site Evaluation for Nuclear Power Plants*, 2002

41. NS-G-3.3, *Evaluation of Seismic Hazards for Nuclear Power Plants*, 2002

42. NS-G-3.4, *Meteorological events in site evaluation for nuclear power plants*, 2003

43. NS-G-3.5, *Flood Hazard for Nuclear Power Plants on Coastal and River Sites,* 2003

44. NS-G-4.6, *Radiation Protection and Radioactive Waste Management in the Design and Operation of Research Reactors*, 2009

45. SSG-2, *Deterministic Safety Analysis for Nuclear Power Plants*, 2009

46. SSG-3, *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants*, 2010

47. SSG-4, *Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants*, 2010

48. SSG-9, *Seismic Hazards in Site Evaluation for Nuclear Installations*, 2010

49. SSG-18, *Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations*, 2011

50. *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* (INFCIRC/225/Rev.5), 2011

51. Nuclear Security Series No. 17, *Computer Security at Nuclear Facilities*, 2011

United States Nuclear Regulatory Commission (U.S. NRC)

1. 10 CFR Part 50, Appendix B, *Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants*, 2007

2. NUREG/CR-6303, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*, 1994

3. NUREG-6393, *Integrated System Validation: Methodology and Review Criteria*, 1997

4. NUREG/CR-7007, *Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems*, 2010

5. Branch Technical Position (BTP) 7-19, *Guidance for Evaluation of Diversity and Defense-in-Depth and in Digital Computer-Based Instrumentation and Control Systems*, 2007

6. Regulatory Guide 1.57, *Design Limits and Loading Combinations for Metal Primary Reactor Containment System Components*, 2007

7. SECY-08-0093, *Resolution of Issues Related to Fire-Induced Circuit Failures*, 2008

8. NUREG 1852, *Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire*, 2007

9. NUREG/CR-2913- Rev. 4, *Two-Phase Jet Loads,* 1983

10. NUREG/CR-6850, EPRI 1011989, *Fire Probabilistic Risk Assessment Methods Enhancements*, 2010

11. Regulatory Guide 1.189, *Fire Protection for Operating Nuclear Power Plants*, 2001

12. NUREG-0700 Revision 2, *Human-System Interface Design Review Guidelines*, 2002

13. NUREG-0711 Revision 2, *Human Factors Engineering Program Review Model*, 2004

14. NUREG 0800, section 3.7.3, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Seismic Subsystem Analysis*, 2007

15. NUREG-0800, section 3.8.1, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Concrete Containment*, 2007

16. NUREG-0800, section 3.8.3, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Concrete and steel internal structures of steel or concrete containments*, 2010

17. NUREG-0800, section 3.8.4, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition – Other Seismic Category I Structures,* 2010

18. NUREG-0800, chapter 8, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Electric Power*, 2007

19. NUREG-0800, section 9.5.1.1, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Fire Protection Program*, 2009

20. NUREG-0800, chapter 10, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition – Steam and Power Conversion System,* 2007

21. NUREG-0800, chapter 14, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition – Initial Test Program and ITAAC – Design Certification*, 2007

22. NUREG-0800, section 14.3.10, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Emergency Planning – Inspections, Tests, Analyses, and Acceptance Criteria,* 2007

23. NUREG-0800, chapter 18, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants – Human Factors Engineering*

24. Regulatory Guide 1.76, *Design Basis Tornado and Tornado Missiles for Nuclear Power Plants,* 2007

25. Regulatory Guide 1.91, *Evaluations of Explosions Postulated to occur on Transportation Routes near Nuclear Power Plants,* 1978

26. NUREG/CR-6486, *Assessment of Modular Construction for Safety-Related Structures at Advanced Nuclear Power Plants,* 1997

27. TECDOC-1657, *Design Lessons Drawn from the Decommissioning of Nuclear Facilities*, 2011

28. NUREG/CR-1278, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications-Final Report*, 2011

29. NUREG/CR-6633, *Advanced Information Systems Design: Technical Basis and Human Factors Review Guidelines*, 2000

30. NUREG-6684, *Advanced Alarm Systems: Revision of Guidance and Its Technical Basis*, 2000

31. NUREG-0696, *Functional Criteria for Emergency Response Facilities,* 1981

32. Regulatory Guide 1.77, *Assumptions Used for Evaluating a Control Rod Ejection Accident for Pressurized Water Reactors*, 1974

33. Regulatory Guide 1.203, *Transient and Accident Analysis Methods*, 2005

34. Regulatory Guide 5.71, *Cyber Security Programs for Nuclear Facilities,* 2010

Other

1. American Concrete Institute (ACI), 349-06, *Code Requirements for Nuclear Safety-Related Concrete Structures & Commentary*, 2007

2. American National Standards Institute, *American National Standard Design Requirements for Light Water Reactor Fuel Handling System,* ANSI/ANS-57.1, 1992

3. American National Standards Institute, *Time Response Design Criteria for Safety-Related Operator Actions*, ANSI/ANS-58.8, 1994

4. American Nuclear Society (ANS), *Categorization of Nuclear Facility Structures, Systems, and Components for Seismic Design,* ANS 2.26, Reaffirmed 2010

5. American Nuclear Society (ANS) 2.3- 2011, *Estimating Tornado, Hurricane, and Extreme Straight Line Wind Characteristics at Nuclear Facility Sites*, 2011

6. American Society of Civil Engineers (ASCE), *Seismic Design Criteria for Structures, Systems and Components in Nuclear Facilities*, ASCE 43-05, 2005

7. American Society of Civil Engineers (ASCE), *Seismic Analysis for Safety-Related Nuclear Structures*, ASCE 04-98, 2000

8. American Society of Civil Engineers (ASCE), *Design of Blast-Resistant Buildings in Petrochemical Facilities*, 2010

9. American Society of Civil Engineers (ASCE), *Structural Analysis and Design of Nuclear Plant Facilities: 58 (ASCE Manual and Reports on Engineering Practice),* 1980

10. American Society of Mechanical Engineers (ASME)*, ASME Boiler and Pressure Vessel Code* – 2010 edition, 2010

11. American Society of Mechanical Engineers, *ASME Boiler and Pressure Vessel Code*, *Section III: Rules for Construction of Nuclear Power Plant Components, Division 1, Subsection NE: Class MC Components*, 2010

12. American Society of Mechanical Engineers, *ASME Boiler and Pressure Vessel Code*, *Section III, Division 2, Section 3, Code for Concrete Containments,* 2010

13. American Society of Mechanical Engineers, *Quality Assurance Requirements for Nuclear Facility Applications*, NQA-1-2008, 2008

14. American Society of Mechanical Engineers, *Qualification of Active Mechanical Equipment Used in Nuclear Power Plants*, QME-1-2002, 2002

15. American Society of Mechanical Engineers*, Standard for Level 1/Large Early Release Frequency PRA for Nuclear Power Plant Applications*, ASME/ANS RA-Sa-2009, 2009

16. Association Française pour les règles de conception, de construction et de surveillance en exploitation des Chaudières Electro-Nucléaires (AFCEN), *Design and Construction Rules for Mechanical Components of PWR Nuclear Islands*, AFCEN RCC-M, 2007

17. Association Française pour les règles de conception, de construction et de surveillance en exploitation des Chaudières Electro-Nucléaires, *Design and Conception Rules for Electrical Components of Nuclear Islands*, AFCEN RCC-E, 2005

18. Association Française pour les règles de conception, de construction et de surveillance en exploitation des Chaudières Electro-Nucléaires, *Design and Conception Rules for Fuel Assemblies of Nuclear Power Plants of Nuclear Islands*, AFCEN RCC-C, 2005

19. Association Française pour les règles de conception, de construction et de surveillance en exploitation des Chaudières Electro-Nucléaires, *EPR Technical Code for Civil Works*, AFCEN ETC-C, 2010

20. Canadian Commission on Building and Fire Codes, *National Building Code of Canada* (NBCC), 2010

21. Communications Security Establishment, *Harmonized Threat and Risk Assessment (TRA) Methodology*, TRA-1, 2007

22. Electric Power Research Institute (EPRI), *Methodology for Developing Seismic Fragilities*, TR-103959, 1994

23. Electric Power Research Institute, Technical Report, *Nuclear Power Plant Equipment Qualification Reference Manual*, Revision 1, 2010

24. European Standard EN 1337-3, *Structural Bearings – Elastomeric Bearings*, 2000

25. European Standard EN 1337-1, *Structural Bearings – General Design Rules*, 2000

26. European Standard EN 15129, *Anti-seismic Devices*, 2009

27. Institute of Electrical and Electronics Engineers (IEEE), *Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*, Standard 379-1988, 1988

28. Institute of Electrical and Electronics Engineers, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*, IEEE 344-2004, 2004

29. Institute of Electrical and Electronics Engineers, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,* IEEE 603, 2009

30. Institute of Electrical and Electronics Engineers, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,* IEEE 7-4.3.2*,* 2010

31. Institute of Electrical and Electronics Engineers, IEEE 497-2010 - *IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations*, 2010

32. Institute of Electrical and Electronics Engineers, (IEEE), *IEEE Standard for Qualification of Equipment Used in Nuclear Facilities,* IEEE-627-2010, 2010

33. Institute of Electrical and Electronics Engineers, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations,* IEEE-323-2003, 2003

34. Institute of Electrical and Electronics Engineers, *IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations*, IEEE 1023, 2004

35. Institute of Electrical and Electronics Engineers, *IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations*, IEEE 1289, 1998

36. Institute of Electrical and Electronics Engineers, *IEEE 308-2001, IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations, 2001*

37. Institute of Electrical and Electronics Engineers, *IEEE 387-1995, IEEE Standard Criteria for Diesel-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations, 1995*

38. Institute of Electrical and Electronics Engineers, *IEEE 141-1993, IEEE Recommended Practice for Electric Power Distribution for Industrial Plants, (Red Book), 1993*

39. Institute of Electrical and Electronics Engineers, *IEEE 242-2001, IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems, (IEEE Buff Book), 2001*

40. Institute of Electrical and Electronics Engineers, *IEEE 279-1971, IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations, 1971*

41. Institute of Electrical and Electronics Engineers, *IEEE 665-1995, IEEE Standard for Generating Station Grounding (Reaffirmed 2001)*

42. Institute of Electrical and Electronics Engineers, *IEEE 1050-1996, Guide for Instrumentation and Control Equipment Grounding in Generating Stations, 1996*

43. Institute of Electrical and Electronics Engineers, *IEEE C62.23-1995, IEEE Application Guide for Surge Protection of Electric Generating Plants*

44. International Organization for Standardization (ISO) ISO 9001:2008 *Quality management systems – Requirements*, 2008

45. International Electrotechnical Commission (IEC), *Nuclear power plants – Instrumentation and control important to safety, General requirements for systems*, IEC 61513, 2011

46. International Electrotechnical Commission, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A fun*ctions, IEC 60880, 2006

47. International Electrotechnical Commission, *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems*, IEC 60987, 2007

48. International Electrotechnical Commission, *Nuclear power plants – Instrumentation and control systems important safety – Surveillance testing*, IEC 60671, 2007

49. International Electrotechnical Commission, *Nuclear power plants – Instrumentation and control important to safety – Methods for assessing the performance of safety system instrument channels*, IEC 62385, 2007

50. International Electrotechnical Commission, *Nuclear power plants - Electrical equipment of the safety system – Qualification,* IEC 60780 edition 2.0, 1998

51. International Electrotechnical Commission, *Nuclear Power Plants – Design of Control Rooms – Functional Analysis and Assessment*, IEC 61839, 2000

52. International Electrotechnical Commission, *Nuclear Power Plants - Control Rooms – Design*, IEC 60964, 2009

53. International Electrotechnical Commission, *Nuclear power plants - Control rooms - Supplementary control points for reactor shutdown without access to the main control room,* IEC 60965-2009, 2009

54. National Fire Protection Association, (NFPA), NFPA 804: *Standard for Fire Protection for Advanced Light Water Reactor Electric Generating Plants*, 2010

55. National Fire Protection Association, NFPA 805: *Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants*, 2010

56. National Fire Protection Association, *Fire Protection Handbook*, 2008

57. Society of Fire Protection Engineers (SFPE) *SFPE Handbook of Fire Protection Engineering*, 2008

58. National Research Council, *National Fire Code of Canada* (NFC), 2010

59. Nuclear Energy Agency (NEA), *Decommissioning Considerations for New Nuclear Power Plants*, NEA No. 6833, OECD, 2010

60. Nuclear Energy Agency, *Applying Decommissioning Experience to the Design and Operation of New Nuclear Power Plants*, NEA No. 6924, OECD, 2010

61. Nuclear Energy Institute (NEI), *Guidance for Post Fire Safe Shutdown Circuit Analysis*, NEI 00-01, 2005

62. Nuclear Energy Institute, *Guidance for Implementing a Risk-Informed, Performance-Based Fire Protection Program under 10 CFR 50.48(c)*, NEI 04-02, Revision 1, 2005

63. Nuclear Energy Institute, NEI 07-13, *Methodology for Performing Aircraft Impact Assessments for New Plant Designs*, 2011

64. Nuclear Energy Institute, NEI 08-09 Rev.6, *Cyber Security Plan for Nuclear Power Reactors*, 2010

65. Nuclear Information and Records Management Association/American National Standards Institute (NIRMA/ANSI), *Standard Configuration Management (CM),* 1.0-2007

66. U.S. Department of the Army, TM 5-1300, *Structures to Resist the Effects of Accidental Explosions*, 1990. Superceded by UFC 3-340-02, 2008