Canada's Nuclear Regulator

Physical Design

Design of Reactor Facilities

REGDOC-2.5.2, Version 2

XXXX 20XX

DRAFT

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Canada

Design of Reactor Facilities, Version 2
Regulatory document REGDOC-2.5.2

Cat. No. NNNNN
ISBN NNNNN

Également publié en français sous le titre : Conception d'installations dotées de réacteurs : centrales nucléaires

Document availability
This document can be viewed on the CNSC website. To request a copy of the document in English or French, please contact:

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

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

Publishing history

May 2014	Version 1.0
XXXX 202X	Version 2.0

Preface

This regulatory document is part of the CNSC's Physical Design series of regulatory documents, which also covers design of uranium mines and mills, design of fixed radiography installations, design of nuclear substance laboratories and nuclear medicine rooms, and exposure devices. The full list of regulatory document series is included at the end of this document and can be found on the CNSC's website.

REGDOC-2.5.2, *Design of Reactor Facilities*, Version 2, sets out requirements and guidance for new licence applications for water-cooled reactor facilities. It establishes a set of comprehensive design requirements and guidance that are risk-informed and align with accepted international codes and practices.

This document provides criteria pertaining to the safe design of new water-cooled reactor facilities. All aspects of the design are taken into account, and multiple levels of defence are promoted in design considerations. To the extent practicable, the requirements and guidance provided herein are technology-neutral with respect to water-cooled reactor facilities. An applicant or licensee may put forward a case to demonstrate that the intent of a requirement is addressed by other means and demonstrated with supportable evidence.

REGDOC-2.5.2, *Design of Reactor Facilities*, Version 2, is the second version and supersedes REGDOC-2.5.2, *Design of Reactor Facilities: Nuclear Power Plants*, which was published in May 2014. In addition, REGDOC-2.5.2, *Design of Reactor Facilities*, *Version 2*, supersedes RD-367, *Design of Small Reactor Facilities*, which was published in June 2011.

To a large degree, this regulatory document represents the CNSC's adoption of the principles set forth by the International Atomic Energy Agency in SSR-2/1, *Safety of Nuclear Power Plants: Design*, as adapted to align with Canadian requirements.

This regulatory document considers all licensing phases, as information from the design process feeds into the processes for reviewing an application for a licence to construct a water-cooled reactor facility, and other licence applications.

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

For existing facilities[1]: the requirements contained in this document do not apply unless they have been included, in whole or in part, in the licensing basis.

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

[1] Existing facilities in this document are effectively those first licensed before 2014.

For information on the implementation of regulatory documents and on the graded approach, see REGDOC-3.5.3, *Regulatory Fundamentals*.

The words “shall” and “must” are used to express requirements to be satisfied by the licensee or licence applicant. “Should” is used to express guidance or that which is advised. “May” is used to express an option or that which is advised or permissible within the limits of this regulatory document. “Can” is used to express possibility or capability.

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

Table of Contents

Design of Reactor Facilities

1. Introduction

1.1 Purpose

This regulatory document sets out the requirements of the Canadian Nuclear Safety Commission (CNSC) for the design of new water-cooled reactor facilities. It establishes a set of comprehensive design requirements and guidance that are risk-informed and align with accepted national and international codes and practices.

1.2 Scope

This regulatory document deals with a wide variety of topics related to the design of new reactor facilities. To the extent practicable, this document is technology-neutral with respect to water-cooled reactor facilities, and includes requirements and guidance for:

1. establishing the safety goals and objectives for the design
2. utilizing safety principles in the design
3. applying safety management principles
4. designing structures, systems and components (SSCs)
5. interfacing engineering aspects, plant features and facility layout
6. integrating safety assessments into the design process

To a large degree, this document represents the CNSC's adoption of the principles set forth in the International Atomic Energy Agency (IAEA) document SSR-2/1, Safety of Nuclear Power Plants: Design, and the adaptation of those principles to align with Canadian practices.

It is recognized that specific technologies may use alternative approaches. If a design other than a water-cooled reactor is to be considered for licensing in Canada, the design is subject to the safety objectives, high-level safety concepts and safety management requirements associated with this regulatory document. However, the CNSC will review such designs on a case-by-case basis.

When an applicant proposes to construct more than one reactor on a site, the design of the multi-reactor site shall meet the safety objectives in this regulatory document. The design of each reactor facility shall also satisfy the safety and design requirements in this document. In addition, the applicant shall ensure that the impact on the safety of all reactors on the site due to interactions between reactors, common-cause failure events, and any sharing of SSCs between reactors is assessed for normal operation, anticipated operational occurrences (AOOs) and accident conditions.

Conventional industrial safety is addressed only from a high-level perspective, with a focus on design requirements that are related to nuclear safety.

1.3 Relevant legislation

The following provisions of the *Nuclear Safety and Control Act* (NSCA) and the regulations under it are relevant to this document:

- NSCA, subsection 24(4) and 24(5)
- *General Nuclear Safety and Control Regulations* (GNSCR), paragraphs 3(1)(i), 12(1)(f)
- *Class I Nuclear Facilities Regulations*, paragraphs 3(b), 5(a), (d), (e), (f), (i) (k) and 6(a), (b), (h), (j), (k) and 7(f)

- 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 reactor facility

2. Safety objectives and concepts

The safety objectives and concepts described in this section apply to a reactor facility during operation or during an accident.

Four common plant states are defined: normal operation, anticipated operational occurrence (AOO), design-basis accident (DBA), and beyond-design-basis accident (BDBA). This document also introduces the plant state "design extension conditions" (DECs), as a subset of BDBAs that are considered in the plant design.

2.1 General nuclear safety objective

In support of the NSCA and its associated regulations, the CNSC endorses the objective established by the IAEA that reactor facilities be designed and operated in a manner that will protect individuals, society and the environment from harm. This objective relies on the establishment and maintenance of effective defences against radiological hazards in reactor facilities.

The general nuclear safety objective is supported by three complementary safety objectives, which deal with radiation protection, the technical aspects of the design, and environmental protection. The technical safety objective is interdependent with administrative and procedural measures that are taken to ensure defence against hazards due to ionizing radiation.

2.1.1 Radiation protection objective

The radiation protection objective is to ensure that during normal operation, or during anticipated operational occurrences, radiation exposures within the reactor facility or due to any planned release of radioactive material from the reactor facility are kept below prescribed limits and as low as reasonably achievable (ALARA).

Provisions shall be made for the mitigation of the radiological consequences of any accidents considered in the design.

2.1.2 Technical safety objectives

The technical safety objectives are to provide all reasonably practicable measures to prevent accidents in the reactor facility, and to mitigate the consequences of accidents if they do occur. This takes into account all possible accidents considered in the design, including those of very low probability.

When these objectives are achieved, any radiological consequences will be below prescribed limits, and the likelihood of accidents with serious radiological consequences will be extremely low.

2.1.3 Environmental protection objective

The environmental protection objective is to provide all reasonably practical mitigation measures to protect the environment during the operation of a reactor facility and to mitigate the consequences of an accident.

The design shall include provisions to control, treat and monitor releases to the environment and shall minimize the generation of radioactive and hazardous wastes.

2.2 Application of the technical safety objectives

The NSCA and the technical safety objectives provide the basis for the following criteria and goals:

1. dose acceptance criteria
2. safety goals

Safety analyses shall be performed to confirm that these criteria and goals are met, to demonstrate effectiveness of measures for preventing accidents and mitigating radiological consequences of accidents if they do occur.

2.2.1 Dose acceptance criteria

The acceptance criteria for normal operations are provided in section 6.4.

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

This dose shall be less than or equal to the dose acceptance criteria of:

1. 0.5 millisievert (mSv) for any AOO or
2. 20 mSv for any DBA

The values adopted for the dose acceptance criteria for AOOs and DBAs are consistent with accepted international practices, and take into account the recommendations of the IAEA and the International Commission on Radiological Protection.

2.2.2 Safety goals

Qualitative safety goals

A limit is placed on the societal risks posed by reactor facility operation. For this purpose, the following two qualitative safety goals have been established:

Individual members of the public shall be provided a level of protection from the consequences of reactor facility operation, such that there is no significant additional risk to the life and health of individuals.

Societal risks to life and health from reactor facility operation shall be comparable to or less than the risks of generating electricity by viable competing technologies, and shall not significantly add to other societal risks.

Quantitative application of the safety goals

For practical application, quantitative safety goals have been established so as to achieve the intent of the qualitative safety goals. The three quantitative safety goals are:

1. core damage frequency
2. small release frequency

3. large release frequency

A core damage accident results from a postulated initiating event (PIE) followed by the failure of one or more safety system(s) or safety support system(s). Core damage frequency is a measure of the plant's accident prevention capabilities.

Small release frequency and large release frequency are measures of the plant's accident mitigation capabilities. They also represent measures of risk to society and to the environment due to the operation of reactor facilities.

The applicant shall ensure that the impact on the safety of all reactors on the site due to interactions between reactors, common-cause failure events, and any sharing of SSCs between reactors is assessed for normal operation, AOOs and accident conditions.

Core damage frequency

The sum of frequencies of all event sequences that can lead to significant core degradation shall be less than 10^{-5} per reactor year.

Small release frequency

The sum of frequencies of all event sequences that can lead to any release to the environment that requires temporary evacuation of the local population or a release to the environment of more than 10^{15} becquerels of iodine-131, shall be less than 10^{-5} per reactor year.

Large release frequency

The sum of frequencies of all event sequences that can lead to any release to the environment that requires long-term relocation of the local population or a release to the environment of more than 10^{14} becquerels of cesium-137 shall be less than 10^{-6} per reactor year.

Guidance

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, analyzes the containment behaviour, evaluates the radionuclides released from the failed fuel, and quantifies the releases to the environment. An exemption from performing a Level 2 PSA is granted if it is shown that core damage frequency in the Level 1 PSA is sufficiency low (i.e., less than the large release frequency limit).

Calculations of the safety goals include all internal and external events as per REGDOC-2.4.2, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*. However, aggregation of internal events and other hazard risk metrics performed through simple addition to demonstrate that the risk metrics (core damage frequency, small release frequency and large release frequency) are not exceeded might not be appropriate. It is recognized that when the risk metrics for external events are conservatively estimated, their summation with the risk metrics for internal events can lead to misinterpretation. Should the aggregated total exceed the safety goals, conclusions should not be derived from the aggregated total until the scope of the conservative bias in the other hazards is investigated.

Further details on PSAs are contained in section 9.5 of this document and CNSC REGDOC- 2.4.2, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*.

2.2.3 Safety analyses

To demonstrate achievement of the safety objectives, a comprehensive hazard analysis, a deterministic safety analysis, and a probabilistic safety assessment shall be carried out. These analyses shall identify all sources of exposure in order to evaluate potential radiation doses to workers at the plant and to the public, and to evaluate potential effects on the environment.

The safety analyses shall examine plant performance for:

1. normal operation
2. AOOs
3. DBAs
4. BDBAs, including DECs (DECs could include severe accident conditions)

Based on these analyses, the capability of the design to withstand PIEs and accidents shall be confirmed, the effectiveness of the items important to safety demonstrated, and requirements for emergency response established. The results of the safety analyses shall be fed back into the design.

The safety analyses are discussed in further detail in section 9.0.

2.2.4 Accident mitigation and management

The design shall include provisions to limit radiation exposure in normal operation and AOOs to ALARA levels, and to minimize the likelihood of an accident that could lead to the loss of normal control of the source of radiation. However, given that there is a remaining probability that an accident may occur, measures shall be taken to mitigate the radiological consequences of accidents.

These measures shall include:

1. consideration of inherent safety features
2. incorporation of engineered design features
3. onsite accident management procedures established by the operating organization
4. establishment of offsite intervention measures by responsible authorities

The design shall apply the principle that plant states that could result in high radiation doses or radioactive releases have a very low frequency of occurrence, and that plant states with significant frequency of occurrence have only minimal – if any – potential radiological consequences.

The design shall facilitate the clear transfer of control between procedures for operational states, accident conditions, severe accident management and onsite emergency response.

Additional information

Additional information may be found in:

- Canadian Nuclear Safety Commission (CNSC), G-129, rev 1, Keeping Radiation Exposures and Doses "As Low as Reasonably Achievable (ALARA)," Ottawa, Canada, 2004.
- CNSC, REGDOC-2.3.2, Accident Management: Severe Accident Management Programs for Nuclear Reactors, Ottawa, Canada, 2013.

- International Atomic Energy Association (IAEA), Safety Guide NS-G-2.15, *Severe Accident Management Programmes for Nuclear Power Plants*, Vienna, 2009.

2.3 Safety concepts

2.3.1 Defence in depth

The concept of defence in depth shall be applied to all organizational, behavioural, and design-related safety and security activities to ensure that they are subject to overlapping provisions. The levels of defence in depth shall be independent to the extent practicable.

If a failure were to occur, the defence-in-depth approach allows the failure to be detected, and to be compensated for or corrected.

This concept shall be applied throughout the design process and operation of the plant to provide a series of levels of defence aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails.

The design shall provide all of the following five levels of defence during normal operation; however, some relaxations may be specified for certain shutdown states. These levels are introduced in general terms below, and are discussed in greater detail in section 6.1.

Level One

The aim of the first level of defence is to prevent deviations from normal operation, and to prevent failures of SSCs important to safety.

Level Two

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

Level Three

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

Level Four

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

Level Five

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

Section 6.1 discusses the application of levels of defence in further detail.

Additional information

Additional information may be found in:

- IAEA, INSAG-10, *Defence in Depth in Nuclear Safety*, Vienna, 2010.

2.3.2 Physical barriers

An important aspect of implementing defence in depth in the reactor facility design shall be the provision of a series of physical barriers to confine radioactive material at specified locations. Physical barriers are discussed in further detail in section 6.1.1.

2.3.3 Operational limits and conditions

Operational limits and conditions (OLCs) are the set of limits and conditions that can be monitored by or on behalf of the operator and that can be controlled by the operator.

OLCs shall be established to ensure that plants operate in accordance with design assumptions and intent (parameters and components), and include the limits within which the facility has been shown to be safe. OLCs shall be documented in a manner that is readily accessible for control room personnel, with the roles and responsibilities clearly identified. Some OLCs may include combinations of automatic functions and actions by personnel.

OLCs shall include:

1. safety limits
2. limiting safety system settings
3. OLCs for normal operation and AOOs, including shutdown states
4. control system constraints and procedural constraints on process variables and other important parameters
5. requirements for surveillance, maintenance, testing and inspection of the plant to ensure that SSCs function as intended in the design and comply with the requirement for optimization by keeping radiation exposures ALARA, as per the *Radiation Protection Regulations*
6. specified operating configurations, including operational restrictions in the event of the unavailability of SSCs important to safety
7. action statements, including completion times for actions in response to deviations from the operational limits and conditions

The basis on which the OLCs are derived shall be readily available in order to facilitate the ability of plant personnel to interpret, observe and apply the OLCs.

Guidance

The approaches and terminologies used for 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 OLC terminology. 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 should be defined for a suitable set of bounding plant operating configurations, and be based on the final design of the plant.

Additional information

Additional information may be found in:

- CSA Group, N290.15, Requirements for the safe operating envelope of nuclear power plants, Toronto, Canada.
- IAEA Safety Guide NS-G-2.2, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, Vienna, 2000.

2.3.4 Interface of safety with security and safeguards

Safety measures, nuclear security measures and arrangements for the system of accounting for, and control of, nuclear material for a reactor facility shall be designed and implemented in an integrated manner so that they do not compromise one another.

2.4 Graded approach

For information and guidance on the implementation and use of the graded approach, refer to REGDOC-3.5.3, *Regulatory Fundamentals.*

2.4.1 Application of the graded approach

When a graded approach is applied, factors to be considered could include:

- reactor power
- reactor safety characteristics
- amount and enrichment of fissile and fissionable material
- fuel design
- type and mass of moderator, reflector and coolant
- utilization of the reactor
- presence of high energy sources and other radioactive and hazardous sources
- safety design features
- source term
- siting
- proximity to populated areas

3. Safety management in design

The applicant or licensee shall be ultimately responsible for the design of the reactor facility and shall establish a management system for ensuring the continuing safety of the plant design throughout the lifetime of the reactor facility.

The reactor facility design shall:

1. meet Canadian regulatory requirements
2. meet the design specifications
3. be confirmed by safety assessment
4. take into account current safety practices
5. fulfill the requirements of an effective management system
6. incorporate only those design changes that have been justified by technical and safety assessments

The design process shall be carried out by technically qualified and appropriately trained staff at all levels, and shall include:

1. a clear division of responsibilities with corresponding lines of authority and communication
2. clear interfaces between the groups engaged in different parts of the design, and between designers, utilities, suppliers, builders and contractors, as appropriate
3. design control measures (such as processes, procedures, and practices) as part of an established management system
4. a management system that recognizes the importance of a healthy safety culture

3.1 Design authority

During the design phase, formal design authority typically rests with the organization that has overall responsibility for the design. Prior to plant start-up, this authority shall be transferred to the operating organization.

The design authority may assign responsibility for the design of specific parts of the plant to other organizations, known as responsible designers. The tasks and functions of the design authority and any responsible designer shall be established in formal documentation; however, the overall responsibility remains with the design authority.

The applicant or licensee shall confirm that the design authority has achieved the following objectives for the design:

1. established a knowledge base of all relevant aspects of the plant design and kept it up to date, while taking experience and research findings into account
2. ensured the availability of the design information that is needed for safe plant operation and maintenance
3. established the requisite security provisions in accordance with the Nuclear Security Regulations and associated regulatory documents
4. maintained design configuration control
5. reviewed, verified, approved and documented design changes
6. established and controlled the necessary interfaces with responsible designers or other suppliers engaged in design work
7. ensured that the necessary engineering and scientific skills and knowledge have been maintained
8. ensured that, with respect to individual design changes or multiple changes that may have significant interdependencies, the associated impact on safety has been properly assessed and understood

Additional information

Additional information may be found in:

- CSA Group, N286, Management system requirements for nuclear power plants, Toronto, Canada.
- IAEA, Safety Standards Series GS-G-3.5, The Management System for Nuclear Installations Safety Guide, Vienna, 2009.
- IAEA, INSAG-19, Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life, Vienna, 2003.

3.2 Design management

Appropriate design management shall achieve the following objectives:

1. SSCs important to safety meet their respective design requirements.
2. Due account is taken of the human capabilities and limitations of personnel.
3. Safety design information - necessary for safe operation and maintenance of the plant and for any subsequent plant modifications - is preserved.
4. OLCs are provided for incorporation into the plant administrative and operational procedures.
5. The plant design facilitates maintenance and aging management throughout the life of the plant.
6. The results of the hazard analysis, deterministic safety analysis and probabilistic safety assessment are taken into account.
7. Due consideration is given to the prevention of accidents and mitigation of their consequences.
8. The generation of radioactive and hazardous waste is limited to minimum practicable levels, in terms of both activity and volume.
9. A change control process is established to track design changes in order to provide configuration management during manufacturing, construction, commissioning and operation.
10. Physical protection systems and cyber security programs are provided to address design-basis threats.

3.3 Design control measures

Processes, procedures and practices shall be established as part of the overall management system so as to achieve the design objectives. This shall include identifying all performance and assessment parameters for the plant design, as well as detailed plans for each SSC, in order to ensure consistent quality of the design and the selected components.

The design controls shall be such that the initial design, and any subsequent change or safety improvement, is carried out in accordance with established processes and procedures, which call on appropriate standards and codes and address applicable requirements and design bases.

Appropriate design control measures shall also facilitate identification and control of design interfaces.

The adequacy of the design, including design tools and design inputs and outputs, shall be verified or validated by individuals or groups that are independent from those who originally performed the work. Verifications, validations, and approvals shall be completed before the detailed design is implemented.

The computer software used for design and analysis calculations shall be qualified in accordance with applicable standards.

Guidance

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

- design initiation, including identification of scope
- work control and planning of design activities
- selection of competent staff
- identification and control of design inputs
- establishment of design requirements
- evaluation of design concepts and selection of preferred concept
- selection of design tools and computer software
- conduct of conceptual safety analysis to assess preferred design concept
- conduct of detailed design and production of design documentation and records
- definition of any limiting conditions for safe operation
- design verification and validation
- configuration management

- identification and control of design interfaces

CSA N286, 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 reactor facilities. CNSC G-149, Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors, and CSA N286.7, Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants, provide complementary requirements and guidance for analytical, scientific and design computer programs.

Organizations from nations not using the aforementioned 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, referenced publications, and ISO 9001:2008 Quality Management Systems – Requirements. Such control measures should be mapped to the requisite CSA N286 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 reactor facility 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-based, electronic or Web-based) they intend to use to control their design activities.

Additional information

Additional information may be found in:

- American Society of Mechanical Engineers (ASME), NQA-1-2008, Quality Assurance Requirements for Nuclear Facility Applications, New York, 2008.
- CNSC, G-149, Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors, Ottawa, Canada, 2000.
- CSA Group, N286, Management system requirements for nuclear power plants, Toronto, Canada.
- CSA Group, N286.7.1, Guideline for the application of N286.7-99, Quality assurance of analytical, scientific, and design computer programs for nuclear power plants, Toronto, Canada.
- IAEA, GS-R-3, The Management System for Facilities and Activities, Vienna, 2006.
- Nuclear Information and Records Management Association/American National Standards Institute (ANSI), 1.0, Standard Configuration Management, Washington, D.C., 2007.

3.4 Proven engineering practices

The design authority shall identify the modern codes and standards that will be used for the plant design, and evaluate those codes and standards for applicability, adequacy, and sufficiency to the design of SSCs important to safety.

Where needed, codes and standards shall be supplemented to ensure that the final quality of the design is commensurate with the necessary safety functions.

SSCs important to safety shall be of proven design, and shall be designed according to the standards and codes identified for the reactor facility.

When a new SSC design, feature or engineering practice is introduced, adequate safety shall be demonstrated by a combination of supporting research and development programs and by examination of relevant experience from similar applications. An adequate qualification program shall be established to verify that the new design meets all applicable safety requirements. New designs shall be tested before being brought into service and shall be monitored while in service so as to verify that the expected behaviour is achieved.

The design authority shall establish an adequate qualification program to verify that the new design meets all applicable design safety requirements.

In the selection of equipment, due attention shall be given to spurious operation and to unsafe failure modes (e.g., failure to trip when necessary). Where the design has to accommodate an SSC failure, preference shall be given to equipment that exhibits known and predictable modes of failure, and that facilitates repair or replacement.

3.5 Operational experience and safety research

The reactor facility design shall draw on operational experience that has been gained in the nuclear industry, and on the results of relevant research programs.

Guidance

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 applicable 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 ALARA

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

Additional information

Additional information may be found in:

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

3.6 Safety assessment

Safety assessment is a systematic process applied throughout the design phase to ensure that the design meets all relevant safety requirements. The safety assessment for the design shall include the requirements set by the operating organization and by regulatory authorities. The basis for the safety

assessment shall be the data derived from the safety analysis, previous operational experience, results of supporting research, and proven engineering practices.

The safety assessment shall be part of the design process, with iteration between the design and analyses, and shall increase in scope and level of detail as the design process progresses.

Before the design is submitted, an independent peer review of the safety assessment shall be conducted by individuals or groups separate from those carrying out the design.

Safety assessment documentation shall identify those aspects of operation, maintenance and management that are important to safety. This documentation shall be maintained in a dynamic suite of documents, to reflect changes in design as the plant evolves.

Safety assessment documentation shall be presented clearly and concisely, in a logical and understandable format, and shall be made readily accessible to designers, operators and the CNSC.

Guidance

As per IAEA GSR Part 4, Safety Assessment for Facilities and Activities, aspects considered in the safety assessment should include:

- defence in depth
- 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

The independent peer review should be performed by suitably qualified and experienced individuals.

Additional information

Additional information may be found in:

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

3.7 Design documentation

Design documentation shall include information to demonstrate the adequacy of the design and shall be used for procurement, construction, commissioning and safe operation, including maintenance, aging management, modification and eventual decommissioning of the reactor facility.

The design documentation shall include:

1. design description
2. design requirements
3. classification of SSCs
4. description of plant states
5. security system design, including a description of physical security barriers and cyber security programs
6. operational limits and conditions
7. identification and categorization of initiating events
8. acceptance criteria and derived acceptance criteria
9. deterministic safety analysis
10. probabilistic safety assessment (PSA)
11. hazard analysis

Guidance

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.

For additional guidance on derived acceptance criteria, refer to CNSC regulatory document REGDOC-2.4.1, Deterministic Safety Analysis.

Additional information

Additional information may be found in:

- CNSC, RD/GD-369, Licence Application Guide: Licence to Construct a Nuclear Power Plant, Ottawa, Canada, 2011.
- CNSC, REGDOC-2.4.1, Deterministic Safety Analysis, Ottawa, Canada, 2014.

4. Safety requirements

4.1 Application of defence in depth

The design of a reactor facility shall incorporate defence in depth. The levels of defence in depth shall be independent to the extent practicable.

Defence in depth shall be achieved at the design phase through the application of design provisions specific to the five levels of defence.

Level One

Achievement of Level One defence in depth shall include conservative design and high-quality construction to provide confidence that plant failures and deviations from normal operations are minimized and accidents are prevented.

This shall entail careful attention to selection of appropriate design codes and materials, design procedures, equipment qualification, control of component fabrication and plant construction, and use of operational experience.

Level Two

Level Two shall be achieved by controlling plant behaviour during and following a postulated initiating event (PIE) using both inherent and engineered design features to minimize or exclude uncontrolled transients to the extent possible.

Level Three

Achievement of Level Three defence in depth shall include the provision of inherent safety features, fail-safe design, engineered design features, and procedures that minimize the consequences of DBAs. These provisions shall be capable of leading the plant first to a controlled state, and then to a safe shutdown state, and maintaining at least one barrier for the confinement of radioactive material. Automatic activation of the engineered design features shall minimize the need for operator actions in the early phase of a DBA.

Level Four

Level Four shall be achieved by providing equipment and procedures to manage accidents and mitigate their consequences as far as practicable.

Most importantly, adequate protection shall be provided for the confinement function by way of a robust containment design. This includes the use of complementary design features to prevent accident progression and to mitigate the consequences of DECs. The confinement function shall be further protected by severe accident management procedures.

Level Five

The design shall provide adequately equipped emergency support facilities, and plans for onsite and offsite emergency response.

Guidance

IAEA INSAG-10, *Defence in Depth in Nuclear Safety*, provides information regarding 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 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 paid 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.

To ensure that different levels of defence are independently effective, any design features that aim to prevent an accident should not belong to the same level of defence as design features that aim to mitigate the consequences of the accident.

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 fourth defence level.

4.1.1 Physical barriers

To ensure that the overall safety concept of defence in depth is maintained, the design shall provide multiple physical barriers to the uncontrolled release of radioactive materials to the environment. Such barriers shall include the fuel matrix, the fuel cladding, the reactor coolant pressure boundary, and the containment. In addition, the design shall provide for an exclusion zone.

To the extent practicable, the design shall prevent:

1. challenges to the integrity of physical barriers
2. failure of a barrier when challenged
3. failure of a barrier as a consequence of failure of another barrier
4. the possibility of failure of engineered barriers from errors in operation and maintenance that could result in harmful consequences

The design shall also allow for the fact that the existence of multiple levels of defence does not normally represent a sufficient basis for continued power operation in the absence of one defence level.

4.2 Safety functions

The reactor facility design shall provide adequate means to:

1. maintain the plant in a normal operational state
2. ensure the proper short-term response immediately following a PIE
3. facilitate the management of the plant in and following DBAs and DECs

The following fundamental safety functions shall be available in operational states, DBAs and DECs, except where the postulated accident involves a loss of that function:

1. control of reactivity

2. removal of heat from the fuel
3. confinement of radioactive material
4. shielding against radiation
5. control of operational discharges and hazardous substances, as well as limitation of accidental releases
6. monitoring of safety-critical parameters to guide operator actions

These safety functions shall apply to the reactor as well as fuel storage and handling.

SSCs necessary to fulfill safety functions following a PIE shall be identified. This approach shall identify the need for such functions as reactor shutdown, emergency core cooling, containment, emergency heat removal and power systems.

4.3 Accident prevention and plant safety characteristics

The design shall apply the principles of defence in depth to minimize sensitivity to PIEs. Following a PIE, the plant is rendered safe by:

1. inherent safety features
2. passive safety features
3. specified procedural actions
4. action of control systems
5. action of safety systems
6. action of complementary design features

4.4 Radiation protection and acceptance criteria

Achievement of the general nuclear safety objective (discussed in section 4.1) depends on all actual and potential sources of radiation being identified, and on provision being made to ensure that sources are kept under strict technical and administrative control.

Radiation doses to the public and to site personnel shall be as low as reasonably achievable. During normal operation, including maintenance and decommissioning, doses shall be regulated by the limits prescribed in the *Radiation Protection Regulations*.

The design shall include provisions for the prevention and mitigation of radiation exposures resulting from DBAs and DECs.

The design shall also ensure that potential radiation doses to the public from AOOs and DBAs do not exceed dose acceptance criteria provided in section 4.2.1. The calculated overall risk to the public shall meet the safety goals in section 4.2.2.

Guidance

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 reactor facility design. Radiation doses resulting from the operation of the reactor facility 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 should include the expected occupancy of the reactor facility's radiation areas, along with estimated annual person-Sievert 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

Additional information may be found in:

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

4.5 Exclusion zone

The design shall include adequate provision for an appropriate exclusion zone. The appropriateness of the exclusion zone shall be based on several factors, including:

1. evacuation needs
2. land usage needs
3. security requirements
4. environmental factors

Guidance

The exclusion zone for reactor facilities in Canada has been typically defined as 914 metres from the reactor building. Rather than prescribe a particular size for the exclusion zone, this regulatory document specifies 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.

The exclusion zone boundary should be defined with consideration for the capabilities of onsite and offsite emergency response. Environmental factors that can affect the response times should be taken into consideration. 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 hazards (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 that may have an impact on the size of the exclusion zone include local meteorological conditions that could affect the radiological dose received by members of the public. The design authority may use generic site data and 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 normal operation of the reactor facility.

Additional information

Additional information may be found in:

- CNSC, RD-346, Site Evaluation for New Nuclear Power Plants, Ottawa, Canada, 2008.

4.6 Reactor facility layout

The reactor facility layout shall take into account PIEs to enhance protection of SSCs important to safety.

The design shall take into account the interfaces between the safety, security and safeguard provisions of the reactor facility and other aspects of the facility layout, such as:

1. access routes for normal operational actions and maintenance
2. access control to minimize radiation exposures
3. actions taken in response to internal or external events
4. egress routes
5. movement of hazardous substances, nuclear materials, and radioactive materials
6. movement of authorized and unauthorized personnel
7. interaction of building and support functions

It is likely that some design requirements associated with these factors will conflict with others in the determination of facility layout requirements. The design, therefore, shall reflect an assessment of options, demonstrating that an optimized configuration has been sought for the facility layout.

4.6.1 Requirements for multiple units

The design shall take due account of challenges to multiple units at a site. Specifically, the risk associated with common-cause events affecting more than one unit at a time shall be considered.

Guidance

The presence of multiple units at a site or common-cause 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. These challenges should be identified and the available resources and mitigation strategies shown to be adequate.

5. General design requirements

5.1 Safety classification of structures, systems and components

The design authority shall classify SSCs using a consistent and clearly defined classification method. The SSCs shall then be designed, constructed, and maintained such that their quality and reliability is commensurate with this classification.

In addition, all SSCs shall be identified as either important or not important to safety. The criteria for determining safety importance is 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

SSCs important to safety shall include:

1. safety systems
2. complementary design features
3. safety support systems
4. other SSCs whose failure may lead to safety concerns (e.g., process and control systems)

Appropriately designed interfaces shall be provided between SSCs of different classes in order to minimize the risk of having SSCs less important to safety adversely affect the function or reliability of SSCs of greater importance.

Guidance

The method for classifying the safety significance of SSCs should be based primarily on deterministic methodologies, complemented (where appropriate) by probabilistic methods and engineering judgment. 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 PIEs
- grouping and identification of bounding PIEs
- identification of plant-specific safety functions to prevent or mitigate the PIEs
- safety categorization of the safety functions, in accordance with their safety significance and role in achieving fundamental safety functions
- identification of SSCs that provide the safety functions
- assignment of SSCs to a safety class corresponding to the safety category
- verification of SSC classification
- 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. The number of categories and classes may be chosen to allow for graded design rules.

The time following the PIE 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. The severity should be based on the consequences that could arise if the function was not performed. The consequences of a function failure should be determined assuming that the safety functions belonging to the subsequent level of defence in depth remain functional.

Some specific SSCs classification guidelines are given below:

- SSCs whose failure cannot be accepted because the failure will certainly result in unacceptable consequences should be allocated to the highest safety class.
- Supporting SSCs that are essential to achieve the safety function of the frontline SSCs to be supported should be assigned to the same class as that of the frontline SSCs.

- An SSC that contributes to the performance of several safety functions of different categories should be assigned to the class corresponding to the highest category of those safety functions requiring the commensurate design rules.
- 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. This is to ensure that the failure of a lower safety class SSC will not propagate to an SSC belonging to a higher safety class.

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.

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 very severe consequences. SSCs that provide these safety functions should be assigned a safety category commensurate with the safety significance. For certain complementary design features (such as onsite portable equipment) with high redundancy and extremely low probability of being called upon, a low safety class may be appropriate. It should be noted that not all portable equipment is included in SSCs important to safety.

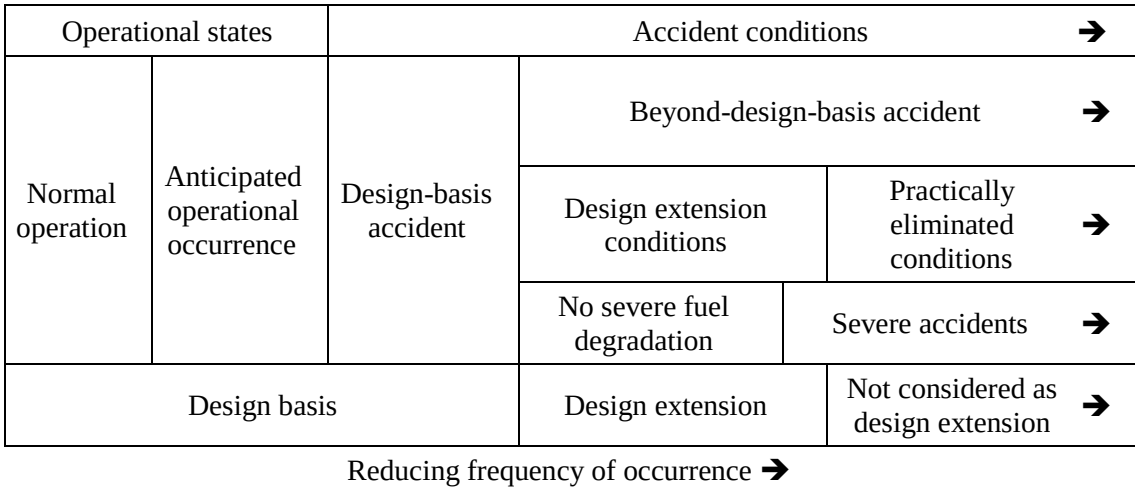
Firstly, SSCs are identified as important or not important to safety. By virtue of their roles, safety systems, complementary design features and safety support systems will be identified as important to safety. Additionally, other SSCs that can have a significant impact on nuclear safety will also be identified as important to safety.

After the SSCs important to safety are identified, they are classified. The safety classification considers a number of factors as listed above. The safety classification enables appropriate design rules to be selected as described in section 7.5.

5.2 Plant design envelope

The design authority shall establish the plant design envelope, which comprises all plant states considered in the design: normal operation, AOOs, DBAs and DECs, as shown in figure 1.

Figure 1: Plant states



The design basis shall specify the capabilities that are necessary for the plant in operational states and DBAs.

Conservative design measures and sound engineering practices shall be applied in the design basis for operational states and DBAs. This will provide a high degree of assurance that no significant damage will occur to the reactor core, and that radiation doses will remain within established limits.

Complementary design features address the performance of the plant in DECs.

Guidance

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 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, DBAs and DECs.

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

A complementary design feature is a design feature added to the design as a stand-alone SSC (including portable equipment), 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, the design authority should provide reasonable assurance that the complementary design features will function as designed when called upon.

5.3 Plant states

Plant states considered in the design shall be grouped into the following four categories:

1. Normal operation is an operation within specified OLCs, including start-up, power operation, shutting down, shutdown, maintenance, testing, and refuelling.
2. An anticipated operational occurrence (AOO) is a deviation from normal operation that is expected to occur once or several times during the operating lifetime of the reactor facility but that, in view of the appropriate design provisions, does not cause any significant damage to items important to safety, or lead to accident conditions.
3. Design-basis accidents (DBAs) are accident conditions for which a reactor facility is designed according to established design criteria, and for which damage to the fuel and the release of radioactive material are kept within regulated limits.
4. Design extension conditions (DECs) are a subset of beyond-design-basis accidents that are considered in the design process of the facility in accordance with best-estimate methodology to keep releases of radioactive material within acceptable limits. Design extension conditions could include severe accidents.

Acceptance criteria shall be assigned to each plant state considered in the design, taking into account the principle that frequent PIEs will have only minor or no radiological consequences, and that any events that may result in severe consequences will be of extremely low probability.

Guidance

Plant states considered in the design are divided into normal operation, AOOs, DBAs and DECs. 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. Note that the plant states diagram in section 5.2 identifies BDBA as a plant state. However, only a subset of BDBAs is considered in the design. These are DECs.

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 reactor facility's operating life
- methods of transferring the plant between different operating configurations
- final safe configurations after AOOs, DBAs, and DECs

5.3.1 Normal operation

The design shall facilitate the safe operation of the plant within a defined range of parameters, with an assumed availability of a minimum set of specified support features for safety systems.

The design shall minimize the unavailability of safety systems. It shall address the potential for accidents to occur when the availability of safety systems may be reduced, such as during shutdown, start-up, low power operation, refuelling and maintenance.

The design shall establish a set of requirements and limitations for safe normal operation, including:

1. limits important to safety
2. constraints on control systems and procedures

3. plant maintenance, testing, and inspection requirements to ensure that SSCs function as intended, taking the ALARA principle into consideration
4. clearly defined operating configurations, such as start-up, power production, shutdown, maintenance, testing, surveillance, and refuelling – these configurations shall include relevant operational restrictions in the event of safety system and safety support system outages

These requirements and limitations, together with the results of safety analysis, shall form the basis for establishing the OLCs according to which the plant will be authorized to operate, as discussed in section 4.3.3 of this document.

Guidance

The design ensures that normal operations are carried out safely, thereby ensuring 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 prescribed limits specified in the *Radiation Protection Regulations*, and will meet the requirements of section 4.1.1 of this regulatory document.

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

- normal reactor start-up (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.

5.3.2 Anticipated operational occurrences

The design shall include provisions such that releases to the public following an AOO do not exceed the dose acceptance criterion provided in section 4.2.1.

The design shall also provide that, to the extent practicable, SSCs not involved in the initiation of an AOO shall remain operable following the AOO.

The response of the plant to a wide range of AOOs shall allow safe operation or shutdown, if necessary, without the need to invoke provisions beyond Level 1 defence in depth or, at most, Level 2.

The facility layout shall be such that equipment is placed at the most suitable location to ensure its immediate availability when operator intervention is required, allowing for safe and timely access during an AOO.

Guidance

The guidance in this subsection also covers elements common to AOO and DBA.

In accordance with the requirements of section 4.3.1 of this regulatory document 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 REGDOC-2.4.1, Deterministic Safety Analysis) can mitigate the event even when acting alone.

In the analysis of AOOs and DBAs for each group of PIEs, 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 component temperatures
- 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.

Additional information

Examples of AOOs may be found in:

- CNSC, REGDOC-2.4.1, *Deterministic Safety Analysis,* Ottawa, Canada, 2014.

5.3.3 Design-basis accidents

The set of DBAs shall set the boundary conditions according to which SSCs important to safety are designed.

The design shall be such that releases to the public following a DBA will not exceed the dose acceptance criterion provided in section 4.2.1.

In order to prevent progression to a more severe condition that may threaten the next barrier, the design shall include provisions to automatically initiate the necessary safety systems when prompt and reliable action is required in response to a PIE.

Provision shall also be made to support timely detection of, and manual response to, conditions when prompt action is not necessary. This shall include responses such as manual initiation of systems or other operator actions.

The design shall take into account operator actions that may be necessary to diagnose the state of the plant and to put it into a stable long-term shutdown condition in a timely manner. Such operator actions shall be facilitated by the provision of adequate instrumentation to monitor plant status, and controls for manual operation of equipment.

Any equipment necessary for manual response and recovery processes shall be placed at the most suitable location to allow safe and timely worker access when needed.

Guidance

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

See also section 7.3.2 of this regulatory document for guidance common to AOOs and DBAs.

Additional information

Examples of DBAs may be found in:

- CNSC, REGDOC-2.4.1, *Deterministic Safety Analysis,* Ottawa, Canada, 2014.

5.3.4 Design extension conditions

The design authority shall identify the set of design extension conditions (DECs) based on deterministic and probabilistic methods, operational experience, engineering judgment and the results of research and analysis. These DECs shall be used to further improve the safety of the reactor facility by enhancing the plant's capabilities to withstand, without significant radiological releases, accidents that are either more severe than DBAs or that involve additional failures.

The design shall be such that plant states that could lead to significant radioactive releases are practically eliminated. For plant states that are not practically eliminated, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public, and sufficient time shall be made available to implement these measures.

Complementary design features shall be provided to cope with DECs. Their design shall be based on a combination of phenomenological models, engineering judgment, and probabilistic methods.

The rules and practices that have been applied to the complementary design features shall be identified. These rules and practices do not necessarily need to incorporate the same degree of conservatism as those applied to the design basis.

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 source term is referred to as the reference source term and shall be based on a set of representative core damage accidents established by the design authority.

To the extent practicable, the design shall provide biological shielding of appropriate composition and thickness in order to protect operational personnel during DECs.

In the case of plants with multiple units at a site, the use of available support from other units shall only be relied upon if the safe operation of the other units is not compromised.

Guidance

DECs are the subset of BDBAs that are considered in the design. BDBAs are all events less frequent than DBAs; there is no lower frequency bound.

For identifying DECs, consideration should be given to:

- factors of the accident progression (i.e., physical conditions, processes and phenomena)
- BDBA (including severe accident) scenarios resulting from initiating events, human actions, and SSC operability (success or failure)
- selection of bounding events that are considered in design and determination of limiting values and 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:

1. be independent, to the extent practicable, of those used in more frequent accidents
2. 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.

For use in the specification of the complementary design features for DECs, the 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 the potential use of safety, non-safety and temporary systems
- 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.

Accident conditions with a significant release are considered to have been practically eliminated:

- if it is physically impossible for the condition to occur, or
- if the condition can be considered with a high degree of confidence to be extremely unlikely to arise

Physical impossibility can be demonstrated by a design feature that would preclude initiation or further progress of an accident scenario. Care should be taken when assumptions are used to support the demonstration. Such assumptions should be adequately acknowledged and addressed.

To demonstrate practical elimination as extremely unlikely with a high degree of confidence, the following should be considered:

- The degree of substantiation provided for the demonstration of practical elimination should take account of the assessed frequency of the situation to be eliminated and of the degree of confidence in the assessed frequency.
- Practical elimination of an accident should not be claimed solely based on compliance with a probabilistic cut-off value. Even if the probability of an accident sequence is very low, any additional design features, operational measures or accident management procedures to lower the risk further should be implemented to the extent practicable.
- The most stringent requirements for the demonstration of practical elimination should apply in the case of an event with the potential to lead directly to a severe accident – i.e., from Level 1 to Level 4 for defence in depth. For example, demonstration of practical elimination of a heterogeneous boron dilution event in a pressurized water reactor (PWR) would require a detailed substantiation.
- The necessary high confidence in low likelihood should, wherever possible, be supported by means such as:
  - multiple layers of protection
  - application of the safety principles of independence, diversity, separation, redundancy
  - use of passive safety features
  - use of multiple independent controls
- It should be ensured that the practical elimination provisions remain in place and valid throughout the plant lifetime: for example, through in-service and periodic inspections.

In each case, the demonstration should show sufficient knowledge of the accident sequence analyzed and of the phenomena involved, substantiated by relevant evidence.

To minimize uncertainties and to increase the robustness of a plant's safety case, demonstration of practical elimination should preferably rely on the criterion of physical impossibility, rather than the second probabilistic criterion (extreme unlikelihood with high confidence).

Portable equipment should be classified based on its safety importance.

There may be different options available to fulfill the fundamental safety functions during DECs. However, when called upon, the portable onsite or offsite equipment credited is expected to be effective with reasonable confidence.

Portable onsite or offsite equipment may be one of the means for mitigation in support of the severe accident management guidelines.

Additional information

Examples of BDBAs may be found in:

- CNSC, REGDOC-2.4.1, *Deterministic Safety Analysis*, Ottawa, Canada, 2014.

5.3.4.1 Severe accidents within design extension conditions

The design shall be balanced such that no particular design feature or event makes a dominant contribution to the frequency of severe accidents, taking uncertainties into account.

Early in the design process, the various potential barriers to core or fuel degradation shall be identified, and features that can be incorporated to halt core or fuel degradation at those barriers shall be provided.

The design shall also identify the equipment to be used in the management of severe accidents, including equipment that is available onsite and offsite.

The design shall include redundant connection points to provide for water and electrical power that may be needed to support severe accident management actions.

Provisions for testing the equipment shall be provided to the extent practicable.

A reasonable level of confidence that this equipment will perform as intended in the case of a severe accident shall be demonstrated by fire and seismic assessments, and consideration of environmental conditions.

Consideration shall be given to the plant's full design capabilities, including the possible use of safety, non-safety, and temporary systems, beyond their originally intended function. This shall apply to any system that can be shown with a reasonable degree of assurance to be able to function in the environmental conditions expected during a severe accident.

For DECs with severe core damage, the containment shall maintain its role as a leak-tight barrier for a period that allows sufficient time for the implementation of offsite emergency procedures following the onset of core damage. Containment shall also prevent uncontrolled releases of radioactivity after this period.

Particular attention shall be placed on the prevention of potential containment bypass in severe accidents.

The design authority shall establish initial severe accident management guidelines**,** taking into account the plant design features, including requirements for multiple units at a site, and the understanding of accident progression and associated phenomena.

Consideration shall be given to the prevention of recriticality following severe accidents.

Guidance

"Severe accidents" refers to accidents 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 fuel 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 REGDOC-2.3.2, *Accident Management: Severe Accident Management Programs for Nuclear Reactors*.

Containment leakage in a severe accident should remain below the design leakage rate limit (as defined in section 8.6.4) for sufficient time to allow implementation of emergency measures. Beyond this time, containment leakage that would lead to exceeding the small and large release safety goals should be precluded. This may be achieved by provision of adequate filtered containment venting along with other features.

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
- thermal-chemical interaction between corium, steel components and vessel
- heat transfer from corium to vessel or end-shield
- hydrogen burn
- steam explosion due to molten fuel-coolant interaction
- 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.

Redundant connection points for water and electrical power that may be needed to support severe accident management actions should use standard connections and be readily accessible. These connection points 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

Additional information may be found in:

- CNSC, RD-327, Nuclear Criticality Safety, section 16 - Nuclear Criticality Accident Emergency Planning and Response, Ottawa, Canada, 2010.

5.4 Postulated initiating events

The design for the reactor facility shall apply a systematic approach to identifying a comprehensive set of postulated initiating events, such that all foreseeable events with the potential for serious consequences or with a significant frequency of occurrence are anticipated and considered.

Postulated initiating events can lead to AOOs, DBAs or BDBAs, and include credible failures or malfunctions of SSCs, as well as operator errors, common-cause internal hazards, and external hazards.

For a site with multiple units, the design shall take due account of the potential for specific hazards simultaneously impacting several units on the site.

Guidance

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.

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 reactor facility, if the failure has a significant impact on nuclear safety.

CNSC REGDOC-2.4.1, *Deterministic Safety Analysis*, and REGDOC-2.4.2, *Probabilistic Safety Assessments*, provide the requirements and guidance for establishing the scope of PIEs, and for classifying the PIEs in accordance with their anticipated frequencies and other factors, as appropriate.

For further information on the safety analysis for the identified PIEs, refer to section 9.0 of this document.

Additional information

Additional information may be found in:

- CNSC, REGDOC-2.4.1, *Deterministic Safety Analysis,* Ottawa, Canada, 2014.

5.4.1 Internal hazards

SSCs important to safety shall be designed and located in a manner that minimizes the probability and effects of hazards (e.g., fires and explosions) caused by external or internal events.

The plant design shall take into account the potential for internal hazards, such as flooding, missile generation, pipe whip, jet impact, fire, smoke, and combustion by-products, or release of fluid from failed systems or from other installations on the site. Appropriate preventive and mitigation measures shall be provided to ensure that nuclear safety is not compromised.

Internal events that the plant is designed to withstand shall be identified, and AOOs, DBAs and DECs shall be determined from these events.

The possible interaction of external and internal events shall be considered, such as external events that may initiate internal fires or floods, or that may lead to the generation of missiles.

Guidance

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

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
- failures of isolating devices

The design considers internal missiles that 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 following actions should be taken:

- 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 a safe shutdown state are identified
- a loss of these potentially impacted components is evaluated to determine if sufficient redundancy remains to achieve and maintain a safe shutdown state

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

5.4.2 External hazards

All natural and human-induced external hazards that may be linked with significant radiological risk shall be identified. External hazards that the plant is designed to withstand shall be selected and classified as DBAs or DECs**.**

Various interactions between the plant and the environment, such as population in the surrounding area, meteorology, hydrology, geology and seismology shall be identified during the site evaluation and environmental assessment processes. These interactions shall be taken into account in determining the design basis for the reactor facility.

Applicable natural external hazards shall include such hazards as earthquakes, droughts, floods, high winds, tornadoes, tsunami, and extreme meteorological conditions**.** Human induced external hazards shall include those that are identified in the site evaluation, such as potential aircraft crashes, ship collisions, and terrorist activities.

Guidance

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 hazards (of human or natural origin)
- design assumptions or values, in terms of recurrence probability of external hazards
- definition of the design basis for external hazards
- 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 considered in the design process should 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 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 components
- geomagnetic storm (solar flare and electromagnetic pulses)
- combinations of extreme weather conditions that could reasonably be assumed to occur at the same time

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

- a phenomenon that occurs slowly or with adequate warning with respect to the time required to take appropriate protective action
- a phenomenon that in itself has no significant impact on the operation of a reactor facility and its design basis
- an individual phenomenon that has an extremely low probability of occurrence
- the reactor facility 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 (e.g., storm-surge and seiche included in flooding or accidental small aircraft crash enveloped by tornado loads)

Human induced hazards considered in the design process should 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 ultimate heat sink 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 hazard (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.

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

Additional information

Additional information may be found in:

- American Nuclear Society (ANS), 2.3, Estimating Tornado, Hurricane, and Extreme Straight Line Wind Characteristics at Nuclear Facility Sites, La Grange Park, Illinois, 2011.
- CNSC, RD-346, Site Evaluation for New Nuclear Power Plants, Ottawa, Canada, 2008.
- IAEA, NS-G-3.1, External Human Induced Events in Site Evaluation for Nuclear Power Plants, Vienna, 2002.
- National Research Council (NRC), *National Building Code of Canada*, Ottawa, Canada, 2010.

5.4.3 Combination of events

Combinations of randomly occurring individual events that could credibly lead to AOOs, DBAs, or DECs shall be considered in the design. Such combinations shall be identified early in the design phase, and shall be confirmed using a systematic approach.

Events that may result from other events, such as a flood following an earthquake, shall be considered to be part of the original PIE.

Guidance

Where the results of engineering judgment, deterministic safety assessments and probabilistic safety assessments indicate potential combinations of events, such combinations should be considered to be AOOs, DBAs or DECs, depending on their likelihood of occurrence.

5.5 Design rules and limits

The design authority shall specify the engineering design rules for all SSCs. These rules shall comply with appropriate accepted engineering practices.

The design shall also identify SSCs to which design limits are applicable. These design limits shall be specified for operational states, DBAs and DECs.

Guidance

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

The engineering design rules for all SSCs should be determined based on their importance to safety, in accordance with 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
  - separation
  - diversity
  - independence
  - fail-safe design
- equipment qualification:
  - environmental qualification
  - seismic qualification
  - qualification against electromagnetic interference
- operational considerations:
  - testability
  - inspectability
  - maintainability
  - aging management
- 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 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 reactor facility should be specified for all operational states, DBAs and DECs. The design limits specified are consistent with relevant national and international codes and standards.

5.6 Design for reliability

All SSCs important to safety shall be designed with sufficient quality and reliability to meet the design limits. A reliability analysis shall be performed for each of these SSCs.

Where possible, the design shall provide for testing to demonstrate that the reliability requirements will be met during operation.

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 model for each system may use realistic failure criteria and best-estimate failure rates, considering the anticipated demand on the system from PIEs.

Design for reliability shall take account of mission times for SSCs important to safety.

The design shall take into account the availability of offsite services upon which the safety of the plant and protection of the public may depend, such as the electricity supply and external emergency response services.

Guidance

The design for reliability is based on meeting applicable regulatory requirements and industry standards. The design should provide assurance that the requirements of CNSC RD/GD-98, *Reliability Programs for Nuclear Power Plants*, will be met during operation. Not all SSCs important to safety identified in the design phase will necessarily be included in the reliability program.

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 reliability of SSCs assumed in the design stage needs to be realistic and achievable.

Deterministic analysis or other methods may be used if the PSA lacks effective models or data to evaluate the reliability of SSCs.

5.6.1 Common-cause failures

The potential for common-cause failures (CCFs) of items important to safety shall be considered in determining where to apply the principles of separation, diversity and independence so as to achieve the necessary reliability. Such failures could simultaneously affect a number of different items important to safety. The event or cause could be a design deficiency, a manufacturing deficiency, an operating or maintenance error, a natural phenomenon, a human-induced event, or an unintended cascading effect from any other operation or failure within the plant.

Guidance

Failure of a number of devices or components to perform their functions could occur as a result of a single specific event or cause. CCFs could also occur when multiple components of the same type fail at the same time. This could be caused by occurrences such as a change in ambient conditions, saturation of signals, repeated maintenance error or design deficiency.

Additional information

Additional information may be found in:

- United States Nuclear Regulatory Commission (U.S. NRC), NUREG/CR-7007, *Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems*, Washington, D.C., 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*, Washington, D.C., 2007.
- U.S. NRC, NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, Washington, D.C., 1994.

5.6.1.1 Separation

The design shall provide sufficient physical separation between:

1. redundant divisions of a safety system
2. redundant divisions of a safety support system
3. a safety support system and a process system

This shall apply to equipment and to the routing of items, including:

1. electrical cables for power and control of equipment
2. piping for service water for the cooling of fuel and process equipment
3. tubing and piping for compressed air or hydraulic drives for control equipment

Where physical separation by horizontal distance alone may not be sufficient for some CCFs (such as flooding), vertical separation or other protection shall be provided.

Where physical separation is not possible, safety support system equipment may share physical space. In such cases, the reasons for the lack of separation and justification for the space sharing arrangement shall be explained in the design documentation.

Where space sharing is necessary, services for safety systems and for other process systems important to safety shall be arranged in a manner that incorporates the following considerations:

1. A safety system designed to act as backup shall not be located in the same space as the primary safety system.
2. If a safety system and a process system must share space, then the associated safety functions shall also be provided by another safety system in order to counter the possibility of failures in the process system.

The design shall provide effective protection against common-cause events where sufficient physical separation among individual services or groups of services does not exist. The design authority shall assess the effectiveness of specified physical separation or protective measures against common-cause events.

Guidance

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.

5.6.1.2 Diversity

Diversity shall be applied to redundant systems or components that perform the same safety function by incorporating different attributes into the systems or components. Such attributes shall include different principles of operation, different physical variables, different conditions of operation, or production by different manufacturers.

It is important that any diversity used achieves the desired increase in reliability. For example, to reduce the potential for a CCF, the application of diversity shall be examined for any similarity in materials, components, and manufacturing processes, or subtle similarities in operating principles or common support features. If diverse components or systems are used, there shall be a reasonable assurance that such additions are of overall benefit, taking into account associated disadvantages such as the extra complication in operational, maintenance, and test procedures, or the consequent use of equipment of lower reliability.

Guidance

The design should implement adequate diversity, such as:

- design diversity
- equipment diversity
- functional diversity
- human factor engineering diversity

The design for I&C systems should also consider:

- signal diversity
- software diversity

For I&C systems important to safety, an automated diverse backup system is recommended. 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 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.

5.6.1.3 Independence

Interference between safety systems or between redundant elements of a safety system shall be prevented by means such as electrical isolation, functional independence, and independence of information (e.g., data transfer), as appropriate.

Guidance

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 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 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.

5.6.2 Single-failure criterion

All safety groups shall function in the presence of a single failure. The single-failure criterion requires that each safety group can perform all safety functions required for a PIE in the presence of any single component failure, as well as:

1. all failures caused by that single failure
2. all identifiable but non-detectable failures, including those in the non-tested components
3. all failures and spurious system actions that cause (or are caused by) the PIE

Each safety group shall be able to perform the required safety functions under the worst permissible systems configuration, taking into account such considerations as maintenance, testing, inspection and repair, and equipment outage.

Analysis of all possible single failures, and all associated consequential failures, shall be conducted for each component of each safety group until all safety groups have been considered.

Unintended actions and failure of passive components shall be considered as two of the modes of failure of a safety group.

The single failure shall be assumed to occur prior to the PIE, or at any time during the mission time for which the safety group is required to function following the PIE. Passive components may be exempt from this requirement.

Exceptions to the single-failure criterion shall be infrequent, and clearly justified.

Exemptions for passive components may be applied only to those components that are designed and manufactured to high standards of quality, that are adequately inspected and maintained in service, and that remain unaffected by the PIE. Design documentation shall include justification of such exemptions, by analysis, testing or a combination of analysis and testing. The justification shall take loads and environmental conditions into account, as well as the total period of time after the PIE for which the functioning of the component is necessary.

Check valves shall be considered to be active components if they must change state following a PIE.

Guidance

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. The SSCs inside the safety group should include both the primary SSCs and the supporting SSCs.

The detectability of failures is implicit in the application of the SFC. Detectability is a function of the system design and the specified tests. A failure that cannot be detected through periodic testing, or revealed by alarm or anomalous indication, is non-detectable. An objective in a single-failure analysis is to identify non-detectable failures. To deal with identifiable but non-detectable failures, the following actions should be considered:

- preferred action: the system or the test scheme should be redesigned to make the failure detectable
- alternative action: when analyzing the effect of each single failure, all identified non-detectable failures should be assumed to have occurred. Therefore, the design should take appropriate measures to address these non-detectable failures, such as adequate redundancy and diversity

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 risk 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

Additional information may be found in:

- IAEA, Safety Series No. 50-P-1, *Application of the Single Failure Criterion*, Vienna, 1990.
- Institute of Electrical and Electronics Engineers (IEEE), Standard 379, *Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*, Piscataway, New Jersey, 1988.

5.6.3 Fail-safe design

The concept of fail-safe design shall be incorporated, as appropriate, into the design of systems and components important to safety. To the greatest extent practicable, the application of this principle shall enable plant systems to pass into a safe state if a system or component fails, with no necessity for any action.

Guidance

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 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.

5.6.4 Allowance for equipment outages

The design shall include provisions for adequate redundancy, reliability, and effectiveness, to allow for online maintenance and online testing of systems important to safety, except where these activities are not possible due to access control restrictions.

The design shall take into account the time allowed for each equipment outage and the respective response actions.

Guidance

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.

5.6.5 Shared systems

In cases where a system performs both process functions and safety functions, the following design requirements shall apply:

1. the process and safety functions are not required or credited at the same time
2. if the process function is operating, and a PIE in that system is postulated, it can be shown that all essential safety functions of the system that are required to mitigate the PIE are unaffected
3. the system is designed to the standards of the function of higher importance with respect to safety
4. if the process function is used intermittently, then the availability of the safety function after each use, and its continued ability to meet requirements, can be demonstrated by testing
5. the requirements for instrumentation sharing are met

5.6.5.1 Shared instrumentation for safety systems

Instrumentation shall not typically be shared between safety systems.

Where justified, there may be sharing between a safety system and a non-safety system (such as a process or control system).

The reliability and effectiveness of a safety system shall not be impaired by normal operation, by partial or complete failure in other systems, or by any cross-link generated by the proposed sharing.

The design shall include provisions to ensure that the sharing of instruments does not result in an increased frequency in demand on the safety system during operation.

If the design includes sharing of instrumentation between a safety system and a non-safety system, then the following requirements shall apply:

1. sharing shall be limited to the sensing devices and their pre-amplifiers or amplifiers as needed to get the signal to the point of processing
2. the signal from each shared sensing device shall be electrically isolated so that a failure of a non-safety system cannot be propagated to a safety system
3. an isolation device shall always be associated with the safety system and shall be classified and qualified accordingly

5.6.5.2 Sharing of SSCs between reactors

SSCs important to safety shall typically not be shared between two or more reactors.

In exceptional cases when SSCs are shared between two or more reactors, such sharing shall exclude safety systems and turbine generator buildings that contain high-pressure steam and feedwater systems, unless this contributes to enhanced safety.

If sharing of SSCs between reactors is arranged, then the following requirements shall apply:

1. safety requirements shall be met for all reactors during operational states, DBAs and DECs
2. in the event of an accident involving one of the reactors, orderly shutdown, cool down, and removal of residual heat shall be achievable for the other reactor(s)

When a reactor facility is under construction adjacent to an operating plant, and the sharing of SSCs between reactors has been justified, the availability of the SSCs and their capacity to meet all safety requirements for the operating units shall be assessed during the construction phase.

5.7 Pressure-retaining structures, systems and components

All pressure-retaining SSCs shall be protected against overpressure conditions, and shall be classified, designed, fabricated, erected, inspected, and tested in accordance with established standards. For DECs, relief capacity shall be sufficient to provide reasonable confidence that pressure boundaries credited in severe accident management will not fail.

All pressure-retaining SSCs of the reactor coolant system and auxiliaries shall be designed with an appropriate safety margin to ensure that the pressure boundary will not be breached, and that fuel design limits will not be exceeded in operational states, or DBA conditions.

The design shall minimize the likelihood of flaws in pressure boundaries. This shall include timely detection of flaws in pressure boundaries important to safety.

Unless otherwise justified, all pressure boundary SSCs shall be designed to withstand static and dynamic loads anticipated in operational states, and DBAs.

SSC design shall include protection against postulated pipe ruptures, unless otherwise justified.

The operation of pressure relief devices shall not lead to significant radioactive releases from the plant.

Where two fluid systems operating at different pressures are interconnected, failure of the interconnection shall be considered. Both systems shall either be designed to withstand the higher pressure, or provision shall be made so that the design pressure of the system operating at the lower pressure will not be exceeded.

Adequate isolation shall be provided at the interfaces between the reactor coolant system and connecting systems operating at lower pressures, in order to prevent the overpressure of such systems and possible loss-of-coolant accidents. Consideration shall be given to the characteristics and importance of the isolation and its reliability targets. Isolation devices shall either be closed or close automatically on demand. The response time and speed of closure shall be in accordance with the acceptance criteria defined for postulated initiating events.

All pressure boundary piping and vessels shall be separated from electrical and control systems to the greatest extent practicable.

Pressure-retaining components whose failure will affect nuclear safety shall be designed to permit inspection of their pressure boundaries throughout the design life. If full inspection is not achievable, then it shall be augmented by indirect methods such as a program of surveillance of reference components. Leak detection is an acceptable method when the SSC is leak-before-break qualified.

Guidance

For the design of pressure-retaining systems and components, the design authority should ensure that the selection of codes and standards is commensurate with the safety class and is adequate to provide confidence that plant failures are minimized. This is achieved by using industry standards – such as CSA N285, *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.

REGDOC-2.5.2 requires the design to 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 reactor facility 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, where applicable, of items such as:

- components in the means of shutdown
- main coolant pumps
- headers
- emergency core cooling system components
- 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 applied only 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 uncontrolled active degradation mechanism should exist in the piping system to be qualified for LBB.
- An evaluation of phenomena such as 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 or equivalent.
- 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 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 (or equivalent) class components, the design authority should ensure that:

- finite element modelling and analysis assumptions are checked to make sure they are justified 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 or load specifications
- linearized stress results, obtained from load combinations, are compared with ASME code (or equivalent) allowable limits

5.8 Equipment environmental qualification

The design shall include an equipment environmental qualification (EQ) program. Development and implementation of this program shall ensure that the following functions can be carried out:

1. the reactor can be safely shut down and kept in a safe shutdown state during and following AOOs and DBAs
2. residual heat can be removed from the reactor after shutdown, and also during and following AOOs and DBAs
3. potential for release of radioactive material from the plant can be limited, and the resulting dose to the public from AOOs and DBAs can be kept within the dose acceptance criteria
4. post-accident conditions can be monitored to indicate whether the above functions are being carried out

The environmental conditions to be accounted for shall include those expected during normal operation, and those arising from AOOs and DBAs. Operational data and applicable design assist analysis tools, such as the probabilistic safety assessment, shall be used to determine the envelope of environmental conditions.

The equipment qualification program for SSCs important to safety shall include the consideration of aging effects due to service life.

Equipment qualification shall also include consideration of any unusual environmental conditions that can reasonably be anticipated, and that could arise during normal operation or AOOs (such as periodic testing of the containment leak rate).

Equipment and instrumentation credited to operate during DECs shall be demonstrated, with reasonable confidence, to be capable of performing their intended safety function(s) under the expected environmental conditions. A justifiable extrapolation of equipment and instrumentation behaviour may be used to provide assurance of operability, and is typically based on design specifications, environmental qualification testing, or other considerations.

Guidance

The designer should provide detailed processes and specifications for an equipment EQ program, for qualifying safety-related equipment associated with systems that are essential to perform the credited safety functions. 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 should identify the EQ-related standards and codes (e.g., CSA, IEEE and ASME). The latest editions of the applicable standards for use in the equipment qualification are preferred; any deviations should be justified.

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

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 a harsh post-accident environment could prevent safety-related equipment from accomplishing its safety function
- accident monitoring equipment

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

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 of qualification (particularly for electrical equipment); 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, radio frequency interference, and power surges – should be addressed.

For mild environment qualification, equipment may be considered qualified, provided that:

- the environmental conditions are set out in a design specification
- the manufacturer provides certification that the equipment meets the specification

Equipment and instrumentation credited under design extension conditions

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

- the accident timeframes for each function
- the equipment type and location used to perform necessary functions in each timeframe
- the functions credited in the accident timeframes that need to be performed to achieve a safe shutdown state for DECs
- the postulated 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

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

Additional information may be found in:

- ASME, QME-1, Qualification of Active Mechanical Equipment Used in Nuclear Power Plants, New York, 2002.
- CSA Group, N290.13, Environmental qualification of equipment for CANDU nuclear power plants, Toronto, Canada.
- Electric Power Research Institute (ERPI), Technical Report rev. 1, Nuclear Power Plant Equipment Qualification Reference Manual, Palo Alto, California, 2010.
- IAEA, Safety Reports Series No. 3, Equipment Qualification in Operational Nuclear Power Plants: Upgrading, Preserving and Reviewing, Vienna, 1998.
- International Electrotechnical Commission (IEC), 60780 ed 2.0, Nuclear Power Plants - Electrical Equipment of the Safety System – Qualification, Geneva, 1998.

- IEEE, Standard 323, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, Piscataway, New Jersey, 2003.
- IEEE, Standard 627, Qualification of Equipment Used in Nuclear Facilities, Piscataway, New Jersey, 2010.

5.9 Instrumentation and control

5.9.1 General

The design shall include provision of instrumentation to monitor plant variables and systems over the respective ranges for operational states, DBAs and DECs, in order to ensure that adequate information can be obtained on plant status.

This shall include 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.

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.

The design shall include provision for testing, including self-checking capabilities.

The design shall provide for periodic testing of the entire channel of instrumentation logic, from sensing device to actuating device.

The design shall facilitate maintenance, detection and diagnosis of failure, safe repair or replacement, and recalibration.

The design shall also include the capability to trend and automatically record measurement of any derived variables that are important to safety.

Instrumentation shall be adequate for measuring plant parameters for emergency response purposes.

The design shall include reliable controls to maintain plant variables within specified operational ranges.

The safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions shall continue until completion.

The design shall minimize the likelihood of operator action defeating the effectiveness of safety and control systems in normal operation and AOOs, without negating correct operator actions following a DBA.

System control interlocks shall be designed to minimize the likelihood of inadvertent manual or automatic override, and to provide for situations when it is necessary to override interlocks to use equipment in a non-standard way.

Various safety actions shall be automated so that operator action is not necessary within a justified period of time from the onset of AOOs or DBAs. In addition, appropriate information shall be available to the operator to confirm the safety action.

Guidance

Particular attention should be paid to the provision of start-up 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 reliable and safe operation.

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

The measurements should include continuous and discrete plant variables. Detection and testing should also consider failure, degradation, unsafe conditions, and 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.

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 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 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.

Testing provisions that are permanently connected to safety systems should be part of the safety systems, and should be the same class as the safety systems unless reliable buffering is in place or system performance is not negatively impacted.

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 described 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

Additional information may be found in:

- CSA Group, N290.14, Qualification of Pre-developed Software for Use in Safety Related Instrumentation and Control Applications in Nuclear Power Plants, Toronto, Canada.
- CSA Group, N290.6, Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of an Accident, Toronto, Canada.
- IAEA, NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Plants, Vienna, 2002.
- IEC, 61226, Nuclear Power Plants - Instrumentation and Control Important to Safety - Classification of Instrumentation and Control Functions, Geneva, 2009.
- IEC, 61513, Nuclear Power Plants – Instrumentation and Control Important to Safety, General Requirements for Systems, Geneva, 2011.
- IEC, 60987, Nuclear Power Plants – Instrumentation and Control Important to Safety – Hardware Design Requirements for Computer-Based Systems, Geneva, 2007.
- IEC, 62385, Nuclear Power Plants – Instrumentation and Control Important to Safety – Methods for Assessing the Performance of Safety System Instrument Channels, Geneva, 2007.
- IEC, 60880, Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems Performing Category A Functions, Geneva, 2006.
- IEC, 60671, Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Surveillance Testing, Geneva, 2007.
- IEEE, 7-4.3.2, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, Piscataway, New Jersey, 2010.
- IEEE, 603, Standard Criteria for Safety Systems for Nuclear Power Generating Stations, Piscataway, New Jersey, 2009.

5.9.2 Use of computer-based systems or equipment

Appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the lifetime of the system or equipment, and in particular, throughout the software development cycle.

A top-down software development process shall be used to facilitate verification and validation activities. This approach shall include verification at each step of the development process to demonstrate that the respective product is correct, and validation to demonstrate that the resulting computer-based system or equipment meets its functional and performance requirements.

If pre-developed software is used in systems or equipment important to safety, then the software (and any subsequent release of the software) shall be developed, inspected, and tested in accordance with standards of a category commensurate with the safety function provided by the given system or equipment.

The software development process, including control, testing, and commissioning of design changes, as well as the results of independent assessment of that process, shall be reviewable and systematically documented in the design documentation.

Where a function important to safety is computer-based, the following requirements shall apply:

1. Functions not essential to safety are separate from and shown not to impact the safety function.
2. The safety function is normally executed in processors separate from software that implements other functions, such as control, monitoring, and display.
3. The requirements associated with diversity apply to computer-based systems that perform similar safety functions – the choice of diversity type shall be justified.
4. The design incorporates fail-safe and fault tolerance features, and the additional complexity ensuing from these features results in an overall gain in safety.

Guidance

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

The I&C development lifecycle includes verification and validation activities. These activities should be identified and use appropriate engineering approaches: e.g., a top-down or bottom-up approach. The relationship between design, verification and validation should be indicated, and the outcome of verification and validation activities should be documented.

The pre-developed software should have the same level of qualification as 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.

When the pre-developed software was not developed to equivalent standards, it may be used to implement IEC 61226 category B and C functions. However, a qualification plan and qualification report should be prepared to demonstrate that this software is fit for its intended purpose and meets the requirements in IEC 62138.

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

- consistency applies to uniform notations, terminology, comments, symbology, and implementation techniques
- modularity ensures 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 provides a thread to antecedent and subsequent documents, and refers 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 refers 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.

Additional information:

Additional information may be found in:

- IAEA, NS-G-1.1, Software for Computer Based Systems Important to Safety in Nuclear Plants, Vienna, 2000.
- IEC, 62138, Nuclear Power Plants – Instrumentation and Control Important for Safety – Software Aspects for Computer-Based Systems Performing Category B or C Functions, Geneva, 2004.

5.9.3 Accident monitoring instrumentation

Instrumentation and recording equipment shall be such that essential information is available to support plant procedures during and following DBAs and DECs by:

1. indicating plant status
2. identifying the locations of radioactive material
3. supporting estimation of quantities of radioactive material
4. recording vital plant parameters
5. facilitating decisions in accident management

Guidance

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, such as:

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

The design should provide the design basis, 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 (section 7.6.2). The design should ensure that there are no common causes that can lead to the failure of instrumentation providing redundant measurements.

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 for instrument channel calibration and testing

Accident monitoring instrumentation is demonstrated to be qualified to perform its required functions for the length of time when its function is required under DBAs and DECs.

Additional information:

Additional information may be found in:

- CSA Group, N290.6, Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of an Accident, Toronto, Canada.
- IEC, 61226, ed. 3.0, Nuclear Power Plants – Instrumentation and Control Important to Safety – Classification of Instrumentation and Control Functions, Geneva, 2009.
- IEC, 62138, ed. 1.0, Nuclear Power Plants – Instrumentation and Control Important for Safety – Software Aspects for Computer-Based Systems Performing Category B or C Functions, Geneva, 2004.
- IEEE, 497, Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations, Piscataway, New Jersey, 2010.

5.10 Safety support system

The safety support systems shall ensure that the fundamental safety functions are available in operational states, DBAs and DECs. Safety support systems provide services such as electrical power, compressed air, water, and air conditioning and ventilation to systems important to safety.

Where normal services are provided from external sources, backup safety support systems shall also be available onsite.

The design shall incorporate emergency safety support systems to cope with the possibility of loss of normal service and, where applicable, concurrent loss of backup systems.

The systems that provide normal services, backup services and emergency services shall have:

1. sufficient capacity to meet the load requirements of the systems that perform the fundamental safety functions
2. availability and reliability commensurate with the systems to which they supply the service

The emergency support systems shall:

1. be independent of normal and backup systems
2. support continuity of the fundamental safety functions until long-term (normal or backup) service is re-established:
   a. without the need for operator action to connect temporary onsite services for at least 8 hours
   b. without the need for offsite services and support for at least 72 hours
3. have a capacity margin that allows for future increases in demand
4. be testable under design load conditions, where practicable

Guidance

The design basis for any compressed air system that serves an item important to safety at the reactor facility 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.

Pre-installed equipment can be credited for accident mitigation 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 onsite, it can normally be credited after 8 hours. However, this should 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 7.3.4.1.

5.11 Guaranteed shutdown state

The design authority shall define the guaranteed shutdown state (GSS) that will support safe maintenance activities of the reactor facility.

The design shall provide two independent means of preventing recriticality from any pathway or mechanism when the reactor is in the GSS.

The shutdown margin for GSS shall be such that the core will remain subcritical for any credible changes in the core configuration and reactivity addition. Where possible, this shall be achieved without operator intervention.

Guidance

A GSS refers to a reactor remaining in a stable, sub-critical state, independent of any perturbation in reactivity 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 and removal, and functional tests to be performed.

5.12 Fire safety

The design of the reactor facility, including that of external buildings and SSCs integral to plant operation, shall include provisions for fire safety.

5.12.1 General

Suitable incorporation of operational procedures, redundant SSCs, physical barriers, spatial separation, fire protection systems, and design for fail-safe operation shall achieve the following general objectives:

1. prevent the initiation of fires
2. limit the propagation and effects of fires that do occur by:
   a. quickly detecting and suppressing fires to limit damage
   b. confining the spread of fires and fire by-products that have not been extinguished
3. prevent loss of redundancy in safety and safety support systems
4. provide assurance of safe shutdown
5. ensure that monitoring of safety-critical parameters remains available
6. prevent exposure, uncontrolled release, or unacceptable dispersion of hazardous substances, nuclear material, or radioactive material due to fires
7. prevent the detrimental effects of event mitigation efforts, both inside and outside of containment

8. ensure structural sufficiency and stability in the event of fire

Buildings or structures shall be constructed using non-combustible or fire retardant and heat resistant material.

Fire is considered an internal hazard. The essential safety functions shall be available during a fire.

Fire suppression systems shall be designed and located such that rupture, or spurious or inadvertent operation, will not significantly impair the capability of SSCs important to safety.

Guidance

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 should be performed to assess compliance with the applicable fire codes and standards used for protection from fires and explosions. 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:

- CSA Group, N293, Fire protection for nuclear power plants, Toronto, Canada.
- NRC, *National Building Code of Canada*, Ottawa, Canada, 2010.
- NRC, *National Fire Code of Canada*, Ottawa, Canada, 2010.

Although CSA N293 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*, Washington, D.C., 2005.

Additional information

Additional information may be found in:

- IAEA, NS-G-2.1, Fire Safety in Operation of Nuclear Power Plants, Vienna, 2000.
- IAEA, Safety Report Series No. 8, Preparation of Fire Hazard Analysis for Nuclear Power Plants, Vienna, 1998.
- IAEA, NS-G-1.7, Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants, Vienna, 2004.
- National Fire Protection Association (NFPA), Fire Protection Handbook, Quincy, Massachusetts, 2008.
- NFPA, 805, Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants, Quincy, Massachusetts, 2010.
- NFPA, 804, Standard for Fire Protection for Advanced Light Water Reactor Electric Generating Plants, Quincy, Massachusetts, 2010.
- NEI, 00-01, Guidance for Post-Fire Safe Shutdown Circuit Analysis, Washington, D.C., 2005.
- NEI, 04-02, rev. 1, Guidance for Implementing a Risk-Informed, Performance-Based Fire Protection Program under 10 CFR 50.48(c), Washington, D.C., 2005.
- Society of Fire Protection Engineers (SFPE), SFPE Handbook of Fire Protection Engineering, Bethesda, Maryland, 2008.
- U.S. NRC, NUREG/CR-6850, EPRI 1011989, Fire Probabilistic Risk Assessment Methods Enhancements, Washington, D.C., 2010.
- U.S. NRC, 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, Washington, D.C., 2009.
- U.S. NRC, Regulatory Guide 1.189, Fire Protection for Operating Nuclear Power Plants, Washington, D.C., 2009.
- U.S. NRC, NUREG-1852, Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire, Washington, D.C., 2007.

5.12.2 Safety to life

The design shall provide protection to workers and the public from event sequences initiated by fire or explosion in accordance with established radiological, toxicological, and human factor criteria so that the following objectives are achieved:

1. Persons not intimate with the initial event (including the public, occupants, and emergency responders) are protected from injury and loss of life.
2. Persons intimate with the initial event have a low probability of injury or death.

To demonstrate that the above life safety objectives have been achieved, the design shall provide:

1. effective and reliable means of fire detection in all areas
2. effective and reliable means of emergency notification, including the nature of the emergency and protective actions to be taken
3. multiple and separate safe egress routes from any area
4. easily accessible exits
5. effective and reliable identification and illumination of egress routes and exits
6. sufficient exiting capacity for the number of workers (taking into account the emergency movement of crowds)
7. protection of workers from fires and fire by-products (i.e., combustion products, smoke, heat, etc.) during egress and in the areas of refuge
8. protection of workers performing plant control and mitigation functions during or following a fire

9. adequate supporting infrastructure (lighting, access, etc.) for workers to perform emergency response, plant control, and mitigation activities during or following a fire
10. sufficient structural integrity and stability of buildings and structures to ensure the safety of workers and emergency responders during and after a fire
11. protection of workers from the release or dispersion of hazardous substances, radioactive material, or nuclear material as a result of fire

Guidance

The *National Building Code of Canada* (NBCC) and the *National Fire Code of Canada* (NFCC) are objective-based national model codes. The provisions of the NBCC and NFCC 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 this regulatory document. Additional fire safety provisions are usually assessed and documented in the code compliance and fire hazard assessment, as required by CSA N293, *Fire protection for nuclear power plants*.

5.12.3 Environmental protection and nuclear safety

The design shall minimize the release and dispersion of hazardous substances or radioactive material to the environment, and shall minimize the impact of any releases or dispersions, including those resulting from fire.

Guidance

As indicated in section 7.12.2, the NBCC and the 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. 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.

5.13 Seismic qualification and design

The seismic qualification of all SSCs shall meet the requirements of Canadian national or equivalent standards.

The design shall include instrumentation for monitoring seismic activity at the site for the life of the plant.

5.13.1 Seismic design and classification

The design authority shall ensure that seismically qualified SSCs important to safety are qualified to a design-basis earthquake (DBE), and ensure that they are categorized accordingly. This shall apply to:

1. SSCs whose failure could directly or indirectly cause an accident leading to core damage
2. SSCs restricting the release of radioactive material to the environment
3. SSCs that assure the subcriticality of stored nuclear material
4. SSCs such as radioactive waste tanks containing radioactive material that, if released, would exceed regulatory dose limits

The design of these SSCs shall also meet the DBE criteria to maintain all essential attributes, such as pressure boundary integrity, leak-tightness, operability, and proper position in the event of a DBE.

The design shall ensure that no substantive damage to these SSCs will be caused by the failure of any other SSC under DBE conditions.

Seismic fragility levels shall be evaluated for SSCs important to safety by analysis or, where possible, by testing.

A beyond-design-basis earthquake (BDBE) shall be identified that meets the requirements for identification of DECs as described in section 7.3.4. SSCs credited to function during and after a BDBE shall be demonstrated to be capable of performing their intended function under the expected conditions. Such demonstration shall provide high confidence of low probability of failure (HCLPF) under BDBE conditions for these SSCs. This demonstration need not be seismic qualification by testing.

Guidance

The seismic design of a reactor facility 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, DBAs and DECs. In addition, beyond design load categories are considered for structural performance in DECs. 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. A DBE is defined as a part of the abnormal or extreme load category corresponding to DBA. BDBE load should be considered under DECs.

Seismic input motion, derived from the DBE, 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. The DBE is defined by multiplying the mean site specific uniform hazard spectrum with a probability of occurrence of 10-4/yr by a design factor, defined in the standard ASCE 43-05, Seismic Design Criteria for Structures, Systems and Components in Nuclear Facilities. The probability of occurrence of the defined DBE is therefore equivalent to the probability of DBAs. A minimum seismic input motion, consistent with national or international standards, should be considered in the design phase for the DBE. 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 should take 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, Design procedures for seismic qualification of nuclear power plants, clause 5.2.3.

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 recognized standards such as ASCE 43-05 and CSA N289.3. 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 categorized 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 the *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 is 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, *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, *Requirements for Safety-Related Structures for CANDU Nuclear Power Plants*

For all safety design categories in a reactor facility, ductility requirements should be in accordance with CSA-A23.3, Design of Concrete Structures for concrete structures and CSA S16, Design of Steel Structures for steel structures, assuming that the structures are ductile or type D. These ductility requirements should provide margins for the BDBE.

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, *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 the ASME Code.

For equipment qualified by testing, multi-axis, multi-frequency testing is acceptable for the DBE in accordance with the requirement of IEEE 344-2004 – *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*; 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 BDBE should utilize the methodology in Electrical Power Research Institute (EPRI) TR-103959, *Methodology for Developing Seismic Fragilities*, to determine if an HCLPF goal is met.

Seismic instrumentation design should follow CSA-N289.5, *Seismic Instrumentation Requirements for Nuclear Power Plants and Nuclear Facilities*, which itemizes the requirements for single and multiple 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. To support achievement of the safety goals, the acceptance criterion for BDBE should demonstrate that the plant HCLPF is at least 1.67 times the DBE.

Assessment and validation of margins for beyond-design-basis earthquakes 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 DBE 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 a BDBE up to 2 times the spectral accelerations of the DBE without major damage and while preserving its function. It includes the provisions to accommodate the structural displacements up to 2 times the displacements under DBE conditions.

Additional information

Additional information may be found in:

- American National Standards Institute (ANSI)/American Nuclear Society (ANS) Standard 2.26, *Categorization of Nuclear Facility Structures, Systems, and Components for Seismic Design*, La Grange Park, Illinois, reaffirmed 2010.
- American Society of Civil Engineers (ASCE), 04-98, *Seismic Analysis of Safety-Related Nuclear Structures*, Reston, Virginia, 2000.

- ASCE/Structural Engineering Institute, 43-05, *Seismic Design Criteria for Structures, Systems and Components in Nuclear Facilities*, Reston, Virginia, 2005.
- American Society of Mechanical Engineers (ASME), Boiler and Pressure Vessel Code Section III, Division 1- Subsection NE, *Rules for Construction of Nuclear Facility Components*, New York, 2010.
- CSA Group, N287 series on requirements for concrete containment structures for CANDU nuclear power plants.
- CSA Group, N289 series on seismic design and qualification of nuclear power plants.
- CSA Group, A23.3, *Design of Concrete Structures*, Toronto, Canada.
- CSA Group, S16, *Design of Steel Structures*, Toronto, Canada.
- CSA Group, N291, *Requirements for Safety-Related Structures for CANDU Nuclear Power Plants*, Toronto, Canada.
- Electric Power Research Institute, TR-103959, *Methodology for Developing Seismic Fragilities*, Palo Alto, California, 1994.
- European Standard, EN-15129, *Anti-seismic Devices*, European Committee for Standardization: Brussels, 2009.
- European Standard, EN-1337-3, *Structural Bearings – Elastomeric Bearings*, European Committee for Standardization: Brussels, 2000.
- European Standard, EN 1337-1, *Structural Bearings – General Design Rules*, European Committee for Standardization: Brussels, 2000.
- IEEE, 344, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*, Piscataway, New Jersey, 2004.
- NRC, *National Building Code of Canada*, Ottawa, Canada, 2010.
- U.S. NRC, Regulatory Guide 1.57, *Design Limits and Loading Combinations for Metal Primary Reactor Containment System Components*, Washington, D.C., 2007.
- U.S. NRC, Regulatory Guide 1.91, *Evaluations of Explosions Postulated to Occur on Transportation Routes Near Nuclear Power Plants*, Washington, D.C., 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, Washington, D.C., 2007.

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

In order to maintain the reactor facility within the boundaries of the design, the design shall be such that the SSCs important to safety can be calibrated, tested, maintained and repaired (or replaced), inspected, and monitored over the lifetime of the plant.

These activities shall be performed to standards commensurate with the importance of the respective safety functions of the SSCs, with no significant reduction in system availability or undue exposure of the site personnel to radiation.

SSCs that have shorter service lifetimes than the plant lifetime shall be identified and described in the design documentation.

In cases where SSCs important to safety cannot be designed to support the desirable testing, inspection, or monitoring schedules, one of the following approaches shall be taken:

1. Proven alternative methods, such as surveillance of reference items or use of verified and validated calculation methods, shall be specified.
2. Conservative safety margins shall be applied, or other appropriate precautions shall be taken, to compensate for possible unanticipated failures.

Details of alternate approaches to SSC monitoring shall be provided in the design documentation.

The design shall provide facilities for monitoring chemical conditions of fluids and of metallic and non-metallic materials. In addition, the means for adding or modifying the chemical constituents of fluid streams shall be specified.

The design shall identify the needs for related testing when specifying the commissioning requirements for the plant.

The design shall provide the means to gather baseline data in order to support maintenance-related testing, inspection and monitoring.

Guidance

While in-service testing, maintenance, repair, inspection and monitoring take place primarily during the operating phase of the plant's lifecycle, the reactor facility 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 to 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 that need to be carried out during the construction and commissioning phases should be identified, in order to provide 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 SSC 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, construction organization, 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 reactor facilities of similar or identical design and layout
- technologies and methodologies available for monitoring, inspection and testing, as well as for the repair, replacement 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 plant safety are acceptable.

Additional information

Additional information may be found in:

- ASME, Boiler and Pressure Vessel Code-2010, Section XI, *Rules for Inservice Inspection of Nuclear Power Plant Components*, New York, 2010.
- CNSC, RD-334, *Aging Management for Nuclear Power Plants*, Ottawa, Canada, 2011.
- CNSC, RD/GD-210, *Maintenance Programs for Nuclear Power Plants*, Ottawa, Canada, 2012.
- CSA Group, N287.7, *In-service Examination and Testing Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants*, Toronto, Canada.
- CSA Group, N285.4, *Periodic inspection of CANDU nuclear power plant components*, Toronto, Canada.
- CSA Group, N285.5, *Periodic inspection of CANDU nuclear power plant components*, Toronto, Canada.
- CSA Group, N291, *Requirements for Safety-Related Structures for CANDU Nuclear Power Plants*, Toronto, Canada.
- IAEA, Safety Guide NS-G-2.6, Maintenance, Surveillance and In-Service Inspection in Nuclear Power Plants, Vienna, 2002.

5.15 Civil structure

5.15.1 Design

The reactor facility design shall specify the required performance for the safety functions of the civil structures in operational states, DBAs and DECs.

Civil structures important to safety shall be designed and located so as to minimize the probabilities and effects of internal hazards such as fire, explosion, smoke, flooding, missile generation, pipe whip, jet impact, or release of fluid due to pipe breaks.

External hazards such as earthquakes, floods, high winds, tornadoes, tsunamis, and extreme meteorological conditions shall be considered in the design of civil structures.

Settlement analysis and evaluation of soil capacity shall include consideration of the effects of fluctuating ground water on the foundations, and identification and evaluation of potential liquefiable soil strata and slope failure.

Civil structures important to safety shall be designed to meet the serviceability, strength, and stability requirements for all possible load combinations under the categories of normal operation, AOO, DBA and DEC conditions, including external hazards. The serviceability considerations shall include, without being limited to, deflection, vibration, permanent deformation, cracking, and settlement.

The design specifications shall also define all loads and load combinations, with due consideration given to the probability of concurrence and loading time history.

Environmental effects shall be considered in the design of civil structures and the selection of construction materials. The choice of construction material shall be commensurate with the designed service life and potential life extension of the plant.

The plant safety assessment shall include structural analyses for all civil structures important to safety.

Guidance

The design authority should provide the design principles, design basis requirements and criteria, 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 are specified in section 7.4. Earthquake design input loads and impacts of malevolent acts, including large aircraft crash, can be found in sections 7.13 and 7.22, respectively.

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

- normal condition loads expected during the assumed design life of the reactor facility
- AOO loads (or severe environmental loads)
- DBA loads (or abnormal or 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 withstand, accommodate or avoid foundation settlement (total and differential), according to its performance requirements.

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

The design should include 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 views 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 hazards. 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 the 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 a common mat slab that is not separated from the other building foundation, the impact should be evaluated.

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

- N287.1, *General Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants*, for general requirements in documentation of design specification and design reports
- N287.2, *Material Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants*, for material
- N287.3, *Design Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants*, for design
- N287.4, *Construction, Fabrication and Installation Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants*, and N287.5, *Examination and Testing Requirements for Concrete Containment Structures for Nuclear Power Plants*, for containment construction and inspection
- N287.6, Pre-operational proof and leakage rate testing requirements for concrete containment structures for nuclear power plants, 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 equivalent standard. Stability of the containment vessel and appurtenances should be evaluated using ASME Code Case N-284-1, *Metal Containment Shell Buckling Design Methods*, Section III, Division 1, Class MC.

For other requirements on the design of containment structures, refer to section 8.6.2 of this regulatory document.

Safety-related structures

The safety-related structures other than the containment should be designed and constructed in accordance with CSA N291, *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 building
- containment shield building, if applicable
- other safety-related structures defined by the design
- turbine building (for boiling water reactor)

Additional information

Additional information may be found in:

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

5.15.2 Surveillance

The design shall enable implementation of periodic inspection programs for structures important to safety in order to verify that the as-constructed structures meet their functional and performance requirements.

The design shall also facilitate in-service monitoring for degradations that may compromise the intended design function of the structures. In particular, the design shall permit monitoring of foundation settling.

Pressure and leak testing shall be conducted on applicable structures to demonstrate that the respective design parameters comply with requirements.

The design shall facilitate routine inspection of sea, lake, and river flood defences and demonstrate fitness for service.

Guidance

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, *Pre- operational proof and leakage rate testing requirements for concrete containment structures for nuclear power plants,* and CSA N287.7, *In-service examination and testing requirements for concrete containment structures for CANDU nuclear power plants*.

Special design provisions should be made to accommodate in-service inspection and pressure testing of concrete containments (e.g., providing sufficient physical access, providing alternative means for identification of conditions that can lead to degradation in inaccessible areas, 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, such as a strain gauge, to monitor stress, strain and any deformation of the structures.

5.15.3 Lifting and handling of large loads

The lifting and handling of large and heavy loads, particularly those containing radioactive material, shall be considered in the reactor facility design. This shall include identification of the large loads, traversing routes and situations where they need to be lifted over areas of the plant that are critical to safety. The design of all cranes and lifting devices shall, therefore, incorporate large margins, appropriate interlocks, and other safety features to accommodate the lifting of large loads.

The drop of large loads lifted and handled in areas where there are systems and components that are important to safety shall be taken into account in the design. The potential load due to the large load drop shall be taken into account in the analysis of DBAs.

5.16 Construction and commissioning

SSCs important to safety shall be designed so that they can be manufactured, constructed, assembled, installed and erected in accordance with established processes that ensure that the design will achieve the required level of safety.

All plant systems shall be designed such that, to the greatest extent practicable, commissioning tests can be performed to confirm that design requirements have been achieved.

The design shall include provisions to facilitate the commissioning activities. In particular, the design of the I&C systems shall make provisions for start-up neutron sources and dedicated start-up instrumentation for conditions in which they are needed.

The design shall specify commissioning requirements including data to be recorded and retained. In particular, the design shall clearly identify any non-standard or special commissioning requirements, which shall be specified in design documentation.

Guidance

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 start-up 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 start-up 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, DBAs and DECs.

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 SSC 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 for 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 of that SSC.

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

Additional information

Additional information may be found in:

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

5.17 Aging and wear

The design shall take due account of the effects of aging and wear on SSCs. For SSCs important to safety, this shall include:

1. an assessment of design margins, taking into account all known aging and wear mechanisms and potential degradation in operational states, including the effects of testing and maintenance processes
2. provisions for monitoring, testing, sampling, and inspecting SSCs so as to assess aging mechanisms, verify predictions, and identify unanticipated behaviours or degradation that may occur during operation, as a result of aging and wear

Additional requirements are provided in RD-334, *Aging Management for Nuclear Power Plants*.

Guidance

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

5.18 Control of foreign material

The design shall provide for the detection, exclusion and removal of all foreign material and corrosion products that may have an impact on safety.

5.19 Transport and packaging for fuel and radioactive waste

The design shall incorporate appropriate features to facilitate the transport and handling of new fuel, irradiated fuel, and radioactive waste in accordance with the requirements of the Packaging and Transport of Nuclear Substances Regulations. Related considerations shall include facility access, as well as lifting and packaging capabilities.

5.20 Escape routes and means of communication

The design shall provide a sufficient number of safe escape routes that will be available in operational states, DBAs and DECs, including seismic events. These routes shall be identified with clear and durable signage, emergency lighting, ventilation and other building services essential to their safe use.

Escape routes shall be subject to the relevant Canadian requirements for radiation zoning, fire protection, industrial safety, and plant security, which include assurance of the ability to escape from containment regardless of the pressure in containment.

Suitable alarm systems and means of communication shall be available at all times to warn and instruct all persons in the plant and on the site.

The design shall ensure that diverse methods of communication are available within the reactor facility and in the immediate vicinity, as well as to offsite agencies, in accordance with the emergency response plan.

Additional information

Additional information may be found in:

- CSA Group, N293, Fire protection for nuclear power plants, Toronto, Canada.
- CNSC, G-225, Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills, Ottawa, Canada, 2001 or successor document.
- IAEA GS-R-2, Preparedness and Response for a Nuclear or Radiological Emergency, Vienna, 2002.
- NRC, National Building Code of Canada, Ottawa, Canada, 2010.
- NRC, *National Fire Code of Canada*, Ottawa, Canada, 2010.

5.21 Human factors

The design shall include a human factors engineering program plan. Relevant and proven systematic analysis techniques shall be used to address human factors issues within the design process.

Human factors considerations:

1. reduce the likelihood of human error as far as reasonably achievable
2. provide means for identifying the occurrence of human error, and methods by which to recover from such an error
3. mitigate the consequences of error

The human factors engineering program shall also facilitate the interface between the operating personnel and the plant by promoting attention to plant layout and procedures, maintenance, inspection, training, and the application of ergonomic principles to the design of working areas and working environments.

Appropriate and clear distinction between the functions assigned to operating personnel and those assigned to automatic systems shall be facilitated by systematic consideration of human factors and the human-system interface. This consideration shall continue in an iterative way throughout the entire design process.

The human-system interfaces in the main control room, the secondary control room, the emergency support facilities, and in the plant shall provide operators with necessary and appropriate information in a usable format that is compatible with the necessary decision and action times.

Human factors verification and validation plans shall be established for all appropriate stages of the design process so as to confirm that the design adequately accommodates all necessary operator actions.

To assist in the establishment of design criteria for information display and controls, each operator shall be considered to have dual roles: that of a systems manager (including responsibility for accident management) and that of an equipment operator. Verification and validation activities shall be comprehensive, such that the design conforms to human factors design principles and meets usability requirements.

The design shall identify the type of information that facilitates an operator’s ability to readily:

1. assess the general state of the plant, whether in operational states, DBAs or DECs
2. confirm that the designed automatic safety actions are being carried out
3. determine the appropriate operator-initiated safety actions to be taken

The design shall provide the type of information that enables an equipment operator to identify the parameters associated with individual plant systems and equipment, and to confirm that the necessary safety actions can be initiated safely.

Design goals shall include promoting the success of operator action with due regard for the time available for response, the physical environment to be expected, and the associated psychological demands made on the operator.

The need for operator intervention on a short time scale shall be kept to a minimum. Where such intervention is necessary, the following conditions shall apply:

1. the information necessary for the operator to make the decision to act is presented simply and unambiguously
2. the operator has sufficient time to make a decision and to act
3. following an event, the physical environment is acceptable in the main control room or in the secondary control room, and in the access route to the secondary control room

Guidance

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 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 are 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 provided that established criteria pertaining to system complexity and importance to safety are met.

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 that they cover, considering the risk of the activities and the novelty of the design
- be 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 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 human-system interface technologies (e.g., displays and controls) that are new to reactor facility 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 facilities, 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 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 analyzed 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

Additional information may be found in:

- ANSI/ANS, 58.8-1994, *Time Response Design Criteria for Safety-Related Operator Actions*, La Grange Park, Illinois, reaffirmed 2008.
- CNSC, G-323, *Ensuring the Presence of Sufficient Qualified Staff at Class I Nuclear Facilities – Minimum Staff Complement*, Ottawa, Canada, 2007.
- CNSC, G-276, *Human Factors Engineering Program Plans*, Ottawa, Canada, 2003.
- CNSC, G-278, *Human Factors Verification and Validation Plans*, Ottawa, Canada, 2003.
- CNSC, P-119, *Policy on Human Factors*, Ottawa, Canada, 2000.
- CSA Group, N290.6, *Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of an Accident*, Toronto, Canada.
- CSA Group, N290.4, *Requirements for Reactor Control Systems of Nuclear Power Plants*, Toronto, Canada.
- IEC, 61839, *Nuclear Power Plants – Design of Control Rooms – Functional Analysis and Assessment*, Geneva, 2000.
- IEC, 60964, *Nuclear Power Plants – Control Rooms – Design*, Geneva, 2009.
- 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*, Piscataway, New Jersey 1998.
- IEEE, 1023, *IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations*, Piscataway, New Jersey, 2004.

- U.S. NRC, NUREG/CR-1278, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications- Final Report*, Piscataway, New Jersey , 2011.
- U.S. NRC, NUREG-0711, *Human Factors Engineering Program Review Model*, Washington, D.C., 2002.
- U.S. NRC, NUREG-0700, *Human System Interface Design Review Guidelines*, Washington, D.C., 2002.
- U.S. NRC, NUREG-6393, *Integrated System Validation: Methodology and Review Criteria*, Washington, D.C., 1997.
- U.S. NRC, NUREG-6684, *Advanced Alarm Systems: Revision of Guidance and Its Technical Basis*, Washington, D.C., 2000.
- U.S. NRC, NUREG/CR-6633, Advanced Information Systems Design: Technical Basis and Human Factors Review Guidelines, Washington, D.C., 2000.

5.22 Robustness against malevolent acts

The design shall provide physical features, such as protection against design-basis threats (DBTs), in accordance with the requirements of the Nuclear Security Regulations.

Guidance on 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 characterization
- 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.

5.22.1 Design principles

The design shall be such that the reactor facility and any other onsite facilities with potential to release large amounts of radioactive material or energy are protected against malevolent acts.

Threats from credible malevolent acts are referred to as design-basis threats (DBTs). More severe but unlikely threats are referred to as beyond-design-basis threats (BDBTs). Both types of threats shall be considered in the design.

Threats identified as DBTs shall have credible attributes and characteristics of potential insider or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage against which a physical protection system is designed and evaluated.

BDBTs are threats too unlikely to warrant incorporation into the design basis, but for which the consequences shall be assessed in order to establish means of mitigation to the extent practicable.

Consistent with the concept of defence in depth, the design shall provide multiple barriers for protection against malevolent acts, including physical protection systems, engineered safety provisions, and

measures for post-event management, as appropriate. The failure of a preceding barrier shall not compromise the integrity and effectiveness of subsequent barriers.

Guidance

The identification of vital areas involves the identification and location of SSCs that require protection, in order to prevent significant radioactive releases. The vital areas include 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, the DBT and BDBT sets of load cases should be selected. Each load case selected should be the worst case scenario for a given threat.

5.22.2 Design methods

The design authority shall develop a methodology for assessing the challenges imposed by DBTs and evaluating the capabilities for meeting these challenges (e.g., as identified in an initial threat and risk assessment). The methodology shall apply conservative design measures and sound engineering practices.

The plant design shall take into account the role of structures, pathways, equipment, and instrumentation in providing detection, delay, and response to threats.

Vital areas shall be identified and taken into account in the design and verification of robustness. For vital areas, the design shall allow enough delay for effective intervention by the onsite or offsite response force, taking structures, detection and assessment into account. These areas shall, to the extent practicable, be protected from inadvertent damage while performing defensive actions.

The design shall provide appropriate means for access control and detection, and for minimizing the number of access and egress points to protected areas. Such points shall include storm sewers, culverts, service piping, and cable routing that could be used to gain access to the facility.

The design shall also take into account the placement of civil utilities to minimize access requirements for such activities as repair and maintenance, in order to reduce threats to protected areas and vital areas.

The design authority shall also develop a methodology for assessing the challenges associated with BDBTs. This methodology shall be applied to determine the margins available for shutdown, fuel cooling and confinement of radioactivity. Significant degradation of engineering means may be permitted.

Guidance

Vital areas are designed using the tiered approach related to the threat level as described below.

For the loadings induced by DBT, the structural design methodology applies conservative design measures and sound engineering practices that meet codes and standards.

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

For the second-tier BDBT (extreme events), degradation of the containment barrier may be accepted; however, the degradation should be limited. The structures of vital areas should be designed for the second-tier BDBT that may exceed design code limits but must stay 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 should 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 may 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, in the absence of adequate design measures, local damage associated with the impact of a missile into the wall could result in scabbing of concrete from the rear face. Ultimately, it could 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. Adequate design measures should be provided to meet the acceptance criteria set out in section 7.22.3.

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

5.22.3 Acceptance criteria

All safety system functions and capabilities shall continue to be available for DBTs.

The design shall provide for the ongoing availability of fundamental safety functions during BDBTs; these provisions will depend on the severity of the threat.

For more severe events, there shall be a safe shutdown path that comprises at least one means for each of the following:

1. reactor shutdown
2. fuel cooling
3. retention of radioactivity from the reactor

There shall be sufficient structural integrity to protect important systems. Two such success paths shall be identified where practical.

For extreme events, there shall be at least one means of reactor shutdown and core cooling. Degradation of the containment barrier may allow the release of radioactive material; however, the degradation shall be limited. In these cases, the response shall include onsite and offsite emergency measures.

Guidance

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

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

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

Further detailed guidance on structural analysis of containment structures is given in Appendix A.

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

Additional information

Additional information may be found in:

- ACI, Standard 349, Code Requirements for Nuclear Safety-Related Concrete Structures and Commentary, Farmington Hills, Michigan, 2007.
- ASCE, Ed. 2, Design of Blast-Resistant Buildings in Petrochemical Facilities, Reston, Virginia, 2010.
- ASCE, 58, Manual and Reports on Engineering Practice, Structural Analysis and Design of Nuclear Plant Facilities, Reston, Virginia, 1980.

- Communications Security Establishment, TRA-1, Harmonized Threat and Risk Assessment (TRA) Methodology, Ottawa, Canada, 2007.
- CNSC, RD-321, Criteria for Physical Protection Systems and Devices at High-Security Sites, Ottawa, Canada, 2010.
- CNSC, RD-363, Nuclear Security Officer Medical, Physical, and Psychological Fitness, Ottawa, Canada, 2008.
- CNSC, G-274, Security Programs for Category I or II Nuclear Material or Certain Nuclear Facilities, Ottawa, Canada, 2003.
- CNSC, RD-346, Site Evaluation for New Nuclear Power Plants, Ottawa, Canada, 2008.
- CNSC, G-208, Transportation Security Plans for Category I, II or III Nuclear Material, Ottawa, Canada, 2003.
- CSA Group, N291, Requirements for Safety-Related Structures for CANDU Nuclear Power Plants, Ottawa, Canada.
- 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, Vienna, 2002.
- IAEA, TECDOC-1276, Handbook on the Physical Protection of Nuclear Materials and Facilities, 2002.
- IAEA, INFCIRC-225, Rev.5, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, Vienna, 2011.
- NEI, 07-13, Methodology for Performing Aircraft Impact Assessments for New Plant Designs, Washington, D.C., 2011.
- Unified Facilities Criteria, 3-340-02, Structures to Resist the Effects of Accidental Explosions, Washington, D.C., 2008.
- United Kingdom Atomic Energy Authority, Guidelines for the Design and Assessment of Concrete Structures Subjected to Impact, Oxfordshire, United Kingdom, 1990.

5.22.4 Cyber security

The design of computer-based I&C systems important to safety shall provide a cyber security defensive architecture.

Computer-based I&C systems and components important to safety shall be protected from cyber attacks in order to maintain confidentiality, integrity and availability.

A cyber security program shall be developed, implemented and maintained so as to achieve the security required in each phase of the computer-based I&C systems' lifecycle.

Cyber security features shall not adversely affect the functions or performance of SSCs important to safety.

Guidance

The security of computer-based I&C systems is designed to provide a secure operational 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 a high level of 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 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

A site specific program should include the following elements:

- defensive strategy
- asset identification and security controls
- roles and responsibilities
- policies and procedures
- awareness and training
- configuration management
- information protection
- coordination with other security programs
- incident reporting and recovery plan
- program maintenance

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 for 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 by 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 that, if compromised, would adversely affect safety functions
- cyber attacks should include either physical or logical threats (with either malicious or non-malicious intent), originating from inside and outside of the perimeter of the system's facility
- computer-based systems and components should include computer hardware, software, firmware, and interfaces
- both autonomous and non-autonomous computer-based systems or components subject to cyber security should be protected

- computer-based systems and components for the functions of emergency preparedness systems, 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, and should meet the following expectations:

- 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 set point adjustments and calibration adjustments should be limited
- 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 safety systems
- safety systems should be designed such that virus protection software is not required
- dedicated communication of plant data between the plant and the emergency support facilities (either onsite or offsite) should be provided using secure protocols

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 or function, or of the complete set of applied controls for safety systems, should consider the following:

- implementation should not adversely 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 a 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 made for periodic and post-maintenance verification, to confirm that the security features are properly configured and operating.

Additional information

Additional information may be found in:

- IAEA, Nuclear Security Series No. 17, *Computer Security at Nuclear Facilities*, Vienna, 2011.

- IEEE, 7-4.3.2, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*, Piscataway, New Jersey, 2010.
- IEC, 61513, *Nuclear Power Plant -Implementation and Control Important to Safety - General Requirements for Systems*, Geneva, 2011.
- NEI, 08-09, rev.6, *Cyber Security Plan for Nuclear Power Reactors*, Washington, D.C., 2010.
- NEI, 10-04, rev.2, *Identifying Systems and Assets Subject to the Cyber Security Rules*, Washington, D.C., 2012.
- U.S. NRC, Regulatory Guide 5.71, *Cyber Security Programs for Nuclear Facilities*, Washington, D.C., 2010.

5.22.5 Prescribed information

Prescribed information to be encompassed by the physical security protection system for the reactor facility shall be identified; it shall be complete and in compliance with section 21(1) of the General Nuclear Safety and Control Regulations.

5.23 Safeguards

Reactor facilities are subject to the obligations arising from Canada's international agreements, and to requirements pertaining to safeguards and non-proliferation.

The design and the design process shall ensure compliance with the obligations arising from the safeguards agreement between Canada and the IAEA. These features allow for the permanent installation of safeguards equipment and the provision of services required for the ongoing operation of that equipment.

Guidance

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.

Safeguards considerations should be integrated during the early design phase of a new reactor facility. This approach is a well-established practice in the Canadian nuclear industry and 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 equipment.

Additional information

Additional information may be found in:

- CNSC, RD-336, Accounting and Reporting of Nuclear Material, Ottawa, Canada, 2010.
- CNSC, GD-336, Guidance for Accounting and Reporting of Nuclear Material, Ottawa, Canada, 2010.

5.24 Decommissioning

Future plant decommissioning and dismantling activities shall be taken into account, such that:

1. materials are selected for the construction and fabrication of plant components and structures with the purpose of minimizing eventual quantities of radioactive waste and assisting decontamination
2. plant layout is designed to facilitate access for decommissioning or dismantling activities, including for plants with multiple units at a site, in periods when some units are operating and some are under decommissioning
3. consideration is given to the future potential requirements for storage of radioactive waste generated as a result of new facilities being built, or existing facilities being expanded

Guidance

Future plant decommissioning and dismantling activities considered at the design phase 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 reactor facilities 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

Additional information may be found in:

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

5.25 Provision for extended shutdown

Provision shall be made in the design to meet the needs arising in long shutdown periods, such as the needs for maintaining the conditions of the nuclear fuel, the coolant or the moderator; for the inspection, periodic testing and maintenance of the relevant SSCs of the facility; and for providing physical protection. Special consideration shall be given to long-lived neutron poisons, which may affect the restarting of the reactor

5.26 Provision for utilization and modification

Special precautions shall be taken in the design in relation to the utilization and modification of the reactor facility to ensure that the configuration of the reactor facility is known at all times, and that the safety case is valid for that configuration.

The safety case shall be made with consideration of utilization of equipment included in the reactor facility as it can:

- cause hazards directly if it fails
- cause hazards indirectly by affecting the safe operation of the reactor
- increase the hazard due to an initiating event by its consequent failure and the effects on the event sequence

Every proposed utilization or modification of equipment (e.g., experimental devices) included in the reactor facility that may have a major significance for safety shall be designed in accordance with the same principles as applied to the reactor facility. In particular, all experimental devices using the reactor shall be designed to standards equivalent to those applied to the reactor itself, and shall be fully compatible in terms of the materials used, the structural integrity and the provision for radiation protection. Further requirements for the design of experimental devices are in section 8.1.1.

Where experimental devices penetrate the reactor boundaries, they shall be designed to preserve the means of confinement and shielding of the reactor. Safety systems for experimental devices shall be designed to protect both the device and the reactor.

The safety case shall also be made with consideration of utilization or modification of equipment that is not part of the reactor facility (e.g., independent adjacent facilities making use of heat, steam or power produced by the reactor facility).

6. System-specific requirements

6.1 Reactor core

The design shall provide the following safety functions under normal operation and transient and accident conditions:

- prevention of unacceptable transients and instabilities
- prevention of progression of AOOs to DBAs
- reactor shutdown, as necessary
- safe shutdown state of the reactor

Reactor core parameters and their limits shall be specified. The design shall consider all foreseeable reactor core configurations for normal operation.

The reactor core, including the fuel elements, reactivity control mechanisms, reflectors, fuel channel and structural parts, shall be designed so that the reactor can be shut down, cooled and held subcritical with an adequate margin in operational states, DBAs and DECs.

The design of the reactor core shall incorporate safety margins as part of defence in depth to ensure that the permissible design limits, taking into account engineering tolerances and uncertainties associated with reactor behaviour under accident conditions, are not exceeded.

The anticipated upper limit of possible deformation or other changes due to irradiation conditions shall be evaluated. These evaluations shall be supported by data from experiments, and from experience with irradiation. The design shall provide protection against those deformations, or any other changes to reactor structures that have the potential to adversely affect the behaviour of the core or associated systems.

Appropriate neutronic, thermal-hydraulic, mechanical, material, chemical and irradiation-related considerations associated with the reactor as a whole shall be taken into account in the design of fuel elements and assemblies, reflectors and other core components.

The reactor core and associated structures and cooling systems shall:

1. withstand static and dynamic loading, including thermal expansion and contraction
2. withstand vibration (such as flow-induced and acoustic vibration)
3. ensure chemical compatibility, including service-related contaminants
4. meet thermal material limits
5. meet radiation damage limits

The design of the reactor core shall be such that:

- the maximum degree of positive reactivity and maximum rate of increase by insertion in operational states and DBAs are limited by a combination of the inherent neutronic characteristics of the core, its thermal-hydraulic characteristics, and the capabilities of the control system and means of shutdown, so that no resultant failure of the reactor pressure boundary will occur, cooling capability will be maintained, and no damage will occur to the reactor core
- power oscillations can be reliably and readily detected and controlled
- specified design limits are not exceeded during normal operation, AOOs and DBAs

- prompt criticality is avoided in any postulated accident unless it is demonstrated (e.g. experimentally, operating experience) that the resulting energy deposition does not result in damage to fuel or the reactor coolant boundary

The reactor core design shall include provisions for a guaranteed shutdown state as described in section 7.11.

The shutdown margin for all shutdown states shall be such that the core will remain subcritical for any credible changes in the core configuration and reactivity addition.

If operator intervention is required to keep the reactor in a shutdown state, the feasibility, timeliness, and effectiveness of such intervention shall be demonstrated.

The core design shall include provisions for monitoring, surveillance, inspections, tests, analyses and commissioning programs, as well as periodic verification and testing programs to ensure that the reactor facility performs as designed and meets the acceptance criteria.

Guidance on nuclear design

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

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.

The design of the reactor core and associated coolant and fuel systems 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. The design should define the measurements to be made, including start-up 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, DBAs and DECs

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 DBAs and DECs.

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:

- 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 the fuel reload cycle, or during on-power fuelling (depending upon the reactor design, reactivity device configurations, and load-follow transients)
  - special problems (such as power spikes due to densification), possible asymmetries, and misaligned reactivity devices
- 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 set points 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 start-up confirmatory tests and the required periodic 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 for 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.

Design power distributions should be broken down into the following components:

- 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 DBAs and DECs. The design limits, along with related uncertainties, operating limits, instrument requirements, and set points, should be incorporated into OLCs.

Reactivity coefficients

The design should establish and characterize the bounding reference values for reactivity coefficients. These reference values should be conservative.

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, DBAs and DECs. 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 and experimental checks of the coefficient in operating reactors
- any required checks of the coefficient in the start-up 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
- 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

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.

It is recognized that reactivity coefficients of the design are important in determining the reactor behavior and safety characteristics. This document does not have specific requirements on the sign or magnitude of the reactivity coefficients including the power coefficient of reactivity. Instead, this document requires a number of design provisions related to the nuclear design to ensure that the design is acceptable for reactor control, stability and plant safety. If a reactor design has a positive power coefficient of reactivity for any operating state, the design authority should demonstrate that operation with a positive power coefficient is acceptable, 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 start-up 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 significantly reduces the probability of a failure to shut down.

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 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.

A validation or verification method can be proven either by meeting accepted verification and validation standards, or by established practice, or some combination of these. New method(s) are "proven" by performing a number of acceptance and demonstration tests that show that the method(s) meets pre-defined criteria.

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, including 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

Additional information may be found in:

- CSA Group, N286.7.1, Guideline for the application of N286.7-99, Quality assurance of analytical, scientific, and design computer programs for nuclear power plants, Toronto, Canada.
- CSA Group, N286.7, Quality Assurance of Analytical, Scientific, and Design Computer Programs for Nuclear Power Plants, Toronto, Canada.
- CSA Group, N290.4, Requirements for reactor control systems of nuclear power plants, Toronto, Canada.
- CSA Group, CAN3-N290.1, Requirements for the Shutdown Systems of CANDU Nuclear Power Plants, Toronto, Canada.
- IAEA, NS-G-2.5, Core Management and Fuel Handling for Nuclear Power Plants, Vienna, 2002.
- IAEA, NS-G-1.12, Design of the Reactor Core for Nuclear Power Plants, Vienna, 2005.
- U.S. NRC, Regulatory Guide 1.77, Assumptions Used for Evaluating a Control Rod Ejection Accident for Pressurized Water Reactors, Washington, D.C., 1974.
- U.S. NRC, Regulatory Guide 1.203, *Transient and Accident Analysis Methods*, Washington, D.C., 2005.

Guidance on 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 where a significant fraction of the fuel is replaced or shuffled during fuelling, the design should provide for diagnostic tests at startup. These tests should verify that the core parameters are within their allowed range.

Guidance on mechanical design of reactor internals

The reactor internals classified as core support structures according to the ASME *Boiler and Pressure Vessel Code* (BPVC), Section III, Division 1, NG-1121, *Core Support Structures*, should be designed, fabricated, and examined in accordance with the provisions of ASME BPVC Section III Division 1, subsection NG.

Those reactor internals not classified as ASME BPVC Code, Section III, Division 1, *Core Support Structures* should be classified as internal structures in accordance with ASME Code, Section III, Division 1, 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 the ASME Code, Section III, Division 1, Subsection NG- 3000, and be 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, components and supports, 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 of a high safety class 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.

6.1.1 Fuel elements, assemblies and design

Fuel assembly design shall include all components in the assembly, such as the fuel matrix, cladding, spacers, support plates, movable rods inside the assembly, etc. The fuel assembly design shall also identify all interfacing systems.

Fuel assemblies and the associated components shall be designed to withstand the anticipated irradiation and environmental conditions in the reactor core, and all processes of deterioration that can occur in operational states. The fuel shall remain suitable for continued use after AOOs. At the design stage, consideration shall be given to long-term storage of irradiated fuel assemblies after discharge from the reactor.

Fuel design limits shall be established to include, at a minimum, limits on fuel power or temperature, limits on fuel burnup, and limits on the leakage of fission products in the reactor cooling system. The design limits shall reflect the importance of preserving the fuel matrix and cladding, as these are first and second barriers to fission product release, respectively.

The design shall account for all known degradation mechanisms, with allowance being made for uncertainties in data, calculations, and fuel fabrication.

Fuel assemblies shall be designed to permit adequate inspection of their structures and components prior to and following irradiation.

In DBAs, the fuel assembly and its component parts shall remain in position with no distortion that would prevent effective post-accident core cooling or interfere with the actions of reactivity control devices or mechanisms. The design shall specify the acceptance criteria necessary to meet these requirements in DBAs.

The requirements for reactor and fuel assembly design shall apply in the event of changes in fuel management strategy, or in operating conditions, over the lifetime of the plant.

Fuel design and design limits shall reflect a verified and auditable knowledge base. The fuel shall be qualified for operation, either through experience with the same type of fuel in other reactors, or through a program of experimental testing and analysis, to ensure that fuel assembly requirements are met.

Analyses shall be performed to show that the intended irradiation conditions and limits in the reactor core (such as fission density, total fissions at the end of lifetime and neutron fluence) are acceptable and will not lead to undue deformation or swelling of the fuel elements. The anticipated upper limit of possible deformation or other changes shall be evaluated. These analyses shall be supported by data from experiments and from experience with irradiation.

There shall be provisions in the design to monitor the integrity of the fuel.

Guidance

The fuel design and qualification should provide assurance that the reactor core design requirements in section 8.1 are met.

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, and related analyses. The fuel design criteria and other design considerations are discussed below.

Fuel damage

Fuel damage criteria should be established for all known damage mechanisms in operational states (normal operation and AOOs). The damage criteria should ensure that fuel dimensions remain 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 burnup 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 insertability.

Fuel rod failure

Fuel rod failure applies to operational states, DBAs and DECs. 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 could occur during DBAs and DECs, and are accounted for in the safety analysis.

Assessment methods should be stated for fuel failure mechanisms, reactor loading and power manoeuvring limitations, and fuel duty, leading to an acceptably low probability of failure. 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 should be provided for all damage mechanisms in DBAs and DECs. 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 fission product release. The criteria should include cladding embrittlement, fuel rod ballooning, structural deformation and, in CANDU, beryllium braze penetration.

Other 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)

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).

Reactor core thermal hydraulic design

The thermal hydraulic 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, as required by REGDOC-2.4.1, Deterministic Safety Analysis.

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, 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.

Additional information

Additional information may be found in:

- ANSI/ANS, 57.5, Light Water Reactor Fuel Assembly Mechanical Design and Evaluation, La Grange Park, Illinois, 1996.
- CNSC, G-144, Trip Parameter Acceptance Criteria for the Safety Analysis of CANDU Nuclear Power Plants, Ottawa, Canada, 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, Washington, D.C., 2007.

6.1.2 Control systems

The design shall provide the means for detecting and controlling reactivity, and levels and distributions of neutron flux. This shall apply to neutron flux in all regions of the core during normal operation (including after shutdown and during and after refuelling states), and during AOOs.

The reactor core control system shall detect and intercept deviations from normal operation with the goal of preventing AOOs from escalating to accident conditions.

Adequate means shall be provided to maintain both bulk and spatial power distributions within a predetermined range.

The control system shall limit the positive reactivity insertion rate to a level required to control reactivity changes and power manoeuvring.

The control system, combined with the inherent characteristics of the reactor and the selected operating limits and conditions, shall minimize the need for shutdown action.

The control system and the inherent reactor characteristics shall keep all critical reactor parameters within the specified limits for a wide range of AOOs.

In the design of the reactivity control devices, due account shall be taken of wear-out and of the effects of irradiation, such as burnup, changes in physical properties and production of gas.

Guidance

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 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), including 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 lifecycle 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 the 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 that 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

6.2 Reactor coolant system

The design shall provide the reactor coolant system (RCS) and its associated components and auxiliary systems with sufficient margin to ensure that the appropriate design limits of the reactor coolant pressure boundary are not exceeded in operational states or DBAs.

The design shall ensure that the operation of pressure relief devices will not lead to significant radioactive releases from the plant, even in DBAs. The RCS shall be fitted with isolation devices to limit any loss of radioactive coolant outside containment.

The material used in the fabrication of the component parts shall be selected so as to minimize corrosion and activation of the material.

Operating conditions in which components of the pressure boundary could exhibit brittle behaviour shall be avoided.

The design shall take into account all conditions of the boundary material in normal operation (including maintenance and testing), AOOs, DBAs and DECs, as well as expected end-of-life properties affected by aging mechanisms, the rate of deterioration, and the initial state of the components.

The design of the moving components contained inside the reactor coolant pressure boundary, such as pump impellers and valve parts, shall minimize the likelihood of failure and associated consequential damage to other items of the reactor coolant system. This shall apply to operational states and DBAs, with allowance for deterioration that may occur in service.

The design shall provide a system capable of detecting and monitoring leakage from the reactor coolant system.

Guidance

The design should have adequate provisions with regard to RCS 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 RCS and reactor auxiliary systems should meet – or contribute to meeting – the following objectives:

- maintain sufficient reactor coolant inventory for core cooling both during 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, DBAs and DECs 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 thermal hydraulic 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 RCS and reactor auxiliary systems:

Pressurizer

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

- volume and capability to accommodate load changes, and to accommodate secondary side transients without the need for pressure relief for the containment to the extent practicable
- capability to withstand thermal shock, particularly in spray nozzles and connections to the main RCS circuit
- control of pressure, such as via heaters, sprays, coolers or steam bleeding

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

Additional information may be found in:

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

6.2.1 In-service pressure boundary inspection

The components of the reactor coolant pressure boundary shall be designed, manufactured, and arranged in a manner that permits adequate inspections and tests of the boundary, support structures and components throughout the lifetime of the plant.

The design shall also facilitate surveillance in order to determine the metallurgical conditions of materials for which metallurgical changes are anticipated.

6.2.2 Reactor coolant system inventory

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. This requirement shall extend to the provision of adequate capacity (flow rate and storage volumes) in the systems performing this function.

The inventory in the RCS and its associated systems shall be sufficient to support cool down from hot operating conditions to zero-power cold conditions without the need for transfer from any other systems.

If necessary for operational states and DBAs, the design shall provide means of monitoring reactor core coolant inventory.

Means of estimating the core coolant inventory in DECs shall be provided, to the extent practicable.

Guidance

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.

6.2.3 Reactor coolant system cleanup

The design shall provide for adequate monitoring and removal of impurities and radioactive substances from the reactor coolant, including activated corrosion products and fission products leaking from the fuel. The safety limit for activity in the reactor coolant shall be defined.

6.2.4 Removal of residual heat from reactor core

The design shall provide a means (i.e., backup) of removing residual heat from the reactor for all conditions of the RCS. The backup shall be independent of the configuration in use.

The means of removing residual heat shall meet reliability requirements on the assumptions of a single failure and the loss of offsite power, by incorporating suitable redundancy, diversity, and independence. Interconnections and isolation capabilities shall have a degree of reliability that is commensurate with system design requirements.

Heat removal shall be at a rate that prevents the specified design limits of the fuel and the reactor coolant pressure boundary from being exceeded.

If a residual heat removal system is required when the RCS is hot and pressurized, the design shall ensure that it can be initiated at the normal operating conditions of the RCS.

6.3 Steam supply system

6.3.1 Steam lines

The steam piping up to and including the turbine generator governor valves and, where applicable, the steam generators shall allow sufficient margin to ensure that the appropriate design limits of the pressure boundary are not exceeded in operational states and DBAs. This provision shall take into account the operation of control and safety systems.

The main steam isolation valves (MSIVs) shall be installed in each of the steam lines leading to the turbine, and located as close as practicable to the containment structure.

Where MSIVs are credited with preventing steam flow into containment, they shall be capable of closing under the conditions for which they are credited.

Where MSIVs provide a containment barrier, they shall meet the containment requirements that apply to those conditions for which they are credited.

The MSIVs shall be inspectable and testable.

Steam lines up to and including the first isolation valve and, where applicable, steam generators shall be qualified to withstand a DBE.

6.3.2 Stream and feedwater system piping and vessels

All piping and vessels shall be typically separated from electrical and control systems, to the extent practicable.

The auxiliary feedwater, steam generator pressure control, and other auxiliary systems shall prevent the escalation of AOOs to DBAs or DECs.

6.3.3 Turbine generators

The design shall provide over-speed protection systems for the turbine generators to minimize the probability of turbine disk failure leading to generation of missiles.

The design shall be such as to minimize the potential for any missiles from a turbine break-up striking the containment, or striking other SSCs important to safety.

Guidance

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)
- the design should consider the potential impacts of any missiles that may result from a turbine break-up striking the SSCs important to safety; the selection of the axes orientation of the turbine generator should minimize such potential

Additional information

Additional information may be found in:

- U.S. NRC, 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, Washington, D.C., 2007.

6.4 Means of shutdown

The design shall provide means of reactor shutdown capable of reducing reactor power to a low value, and maintaining that power for the required duration, when the reactor power control system and the inherent characteristics are insufficient or incapable of maintaining reactor power within the requirements of the OLCs.

The design shall include two separate, independent, and diverse means of shutting down the reactor.

At least one means of shutdown shall be independently capable of quickly rendering the nuclear reactor subcritical from normal operation in AOOs and DBAs, by an adequate margin, on the assumption of a single failure. For this means of shutdown, a transient recriticality may be permitted in exceptional circumstances if the specified fuel and component limits are not exceeded.

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.

No single failure in the shutdown system shall prevent the system from fulfilling its safety function when required.

Means shall be provided to ensure that there is a capability to shut down the reactor in DECs, and to maintain the reactor subcritical even for the most limiting conditions of the reactor core, including severe degradation of the reactor core.

Redundancy shall be provided in the fast-acting means of shutdown if, in the event that the credited means of reactivity control fails during any AOO or DBA, inherent core characteristics are unable to maintain the reactor within specified limits.

While resetting the means of shutdown, the maximum amount of positive reactivity and the maximum rate of reactivity increase shall be within the capacity of the reactor control system.

To improve reliability, stored energy shall be used in shutdown actuation.

The effectiveness of the means of shutdown (i.e., speed of action and shutdown margin) shall be such that specified limits are not exceeded, and the possibility of recriticality or reactivity excursion following a PIE is minimized.

Guidance

For the two means of shutting down the reactor to be independent of each other, they do 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 this regulatory document, “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. In that case, only one fast-acting means of shutdown would be required.

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 that may impair a rod-based shutdown means. The fuel design should ensure that this does not occur in operational states and DBAs.

The most reactive conditions of the core required for the analysis normally include 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 loss of coolant accident (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 extent of the damage 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.

6.4.1 Reactor trip parameters

The design authority shall specify derived acceptance criteria for reactor trip parameter effectiveness for all AOOs and DBAs, and shall perform a safety analysis to demonstrate the effectiveness of the means of shutdown.

Trip parameters shall take into account the effects of SSC aging on effectiveness.

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.

There shall be no gap in trip coverage within the OLCs for any operating condition (such as power, temperature), taking into account plant aging. This shall be ensured by the provision of additional trip parameters if necessary. A different level of effectiveness may be acceptable for the additional trip parameters.

The extent of trip coverage provided by all available parameters shall be documented for the entire spectrum of failures for each set of PIEs.

An assessment of the accuracy and the potential failure modes of the trip parameters shall be provided in the design documentation.

Guidance

The effectiveness of trip parameters should be assessed through safety analysis performed in accordance with REGDOC-2.4.1, Deterministic Safety Analysis.

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 REGDOC-2.4.1, Deterministic Safety Analysis, 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 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.

Guidance on applying the requirements for number and diversity of trip parameters is given in REGDOC-2.4.1, Deterministic Safety Analysis.

REGDOC-2.4.1 also provides the minimum expectations for the number of trip parameters.

A manual reactor trip can be considered equivalent to a trip parameter, if the requirements for crediting operator action from the main control room are met (see section 8.10.4) and the reliability of manual shutdown meets the reliability requirements for an automatic trip.

6.4.2 Reliability

The design shall permit ongoing demonstration that each means of shutdown is being operated and maintained in a manner that ensures continued adherence to reliability and effectiveness requirements.

Periodic testing of the systems and their components shall be scheduled at a frequency commensurate with applicable requirements.

Guidance

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 should be included.

The reliability of the shutdown function should be such that the cumulative frequency of failure to shut down on demand is less than 10-5 failures per demand, and the contribution of all sequences involving failure to shut down to the large release frequency of the safety goals is less than 10-7/yr. This considers the likelihood of the initiating event and recognizes that the two shutdown means may not be completely independent.

Section 7.6.2 requires that the shutdown function be 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.

6.4.3 Monitoring and operator action

Once automatic shutdown is initiated, it shall be impossible for an operator to prevent its actuation.

The need for manual shutdown actuation shall be minimized.

The means for manual actuation and for monitoring shutdown status shall be provided in the main control room and secondary control room.

6.5 Emergency core cooling system

Where required, nuclear reactor facilities shall be equipped with an emergency core cooling system (ECCS). The function of this safety system is to transfer heat from the reactor core following a loss of reactor coolant that exceeds makeup capability. All equipment required for correct operation of the ECCS shall be considered part of the system or its safety support system(s).

Systems that supply electrical power or cooling water to equipment used in the operation of the ECCS shall be classified as safety support systems, and shall be subject to all relevant requirements and expectations.

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.

The ECCS shall meet the following criteria for all DBAs involving loss of coolant:

1. All fuel assemblies and components in the reactor shall be kept in a configuration such that continued removal of the residual heat produced by the fuel can be maintained.
2. A continued cooling flow (recovery flow) shall be supplied to prevent further damage to the fuel after adequate cooling of the fuel is re-established by the ECCS.

The ECCS recovery flow path shall be such that impediment to the recovery of coolant following a loss of coolant accident by debris or other material is avoided.

The design shall ensure that maintenance and reliability testing can be carried out without a reduction in the effectiveness of the system below the OLCs, if the testing is conducted when ECCS availability is required.

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.

All ECCS components that may contain radioactive material shall be located inside containment or in an extension of containment.

ECCS piping in an extension of containment that may contain radioactivity from the reactor core shall be subject to the following requirements:

1. As a piping extension to containment, it meets the requirements for metal penetrations of containment.
2. All piping and components of the ECCS recovery flow path piping that are open to the containment atmosphere are designed for a pressure greater than the containment design pressure.
3. All ECCS recovery flow paths are housed in a confinement structure that prevents leakage of radioactivity to the environment and to adjacent structures.
4. This housing includes detection capability for leakage of radioactivity, and the capability to either return the radioactivity to the flow path, or to collect the radioactivity and store or process it in a system designed for this purpose.

Intermediate or secondary cooling piping loops shall have leak detection, whether the ECCS recovery system is inside or outside of containment, with the leak detection being such that upon detection of radioactivity from the ECCS recovery flow, the loops can be isolated as per the requirements for containment isolation.

Inadvertent operation of all or part of the ECCS shall have no detrimental effect on plant safety.

Guidance

The design authority should describe any reactivity control function performed by the ECCS, together with necessary limits and conditions. For example, PWRs often credit soluble boron in the ECCS accumulators and storage tanks, to supplement control rod insertion for long term reactivity control.

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 requires that the ECCS be 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 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 this regulatory document, “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.

6.6 Containment and means of confinement

Confinement is a fundamental safety function, and a means to achieve this safety function shall be provided for any reactor facility.

The confinement shall be designed to ensure that a release of radioactive material following an accident involving disruption of the core is within acceptable limits. The confinement shall include physical barriers designed to prevent or mitigate an unplanned release of radioactive material to the environment during normal operation, AOOs, DBAs and, to the extent practicable, BDBAs.

To achieve confinement, the means of confinement shall require:

- control of the pressure and temperature
- isolation of the confinement boundary
- leak-tightness of the confinement boundary
- a controlled point of release (which is usually elevated)
- control of combustible sources
- reduction of the concentration of free radioactive material in the confinement boundary
- protection against external events
- radiation shielding

Considering factors such as reactor power, safety characteristics, safety design features and any other relevant factors detailed in section 4.4.1 of this document, the graded approach may be applied to the means of confinement.

The design basis and the various modes of operation of an engineered safety feature shall be defined. The extent to which confinement is automated and the conditions for which its manual overriding is warranted shall be identified. The following features shall be incorporated into the design of confinement:

- The barriers shall be designed with suitable margins for the highest calculated pressure and temperature loads expected in DBA and selected BDBA conditions.

- The acceptable release rate under DBA and selected BDBA conditions shall be determined with account taken of the source term and other parameters such as filtration, the point of release, environmental conditions, and the pressure and temperature under DBA and selected BDBA conditions.

6.6.1 Containment

Where required, each nuclear reactor facility shall be installed within a containment structure, so as to minimize the release of radioactive materials to the environment during operational states and DBAs.

Containment shall also assist in mitigating the consequences of DECs. In particular, the containment and its safety features shall be able to perform their credited functions during DBAs and DECs, including melting of the reactor core. To the extent practicable, these functions shall be available for events more severe than DECs.

The containment shall be a safety system and may include complementary design features. Both the containment system and the complementary design features shall be subject to the respective design requirements provided in this regulatory document.

The design shall include a clearly defined continuous leak-tight containment envelope, the boundaries of which are defined for all conditions that could exist in the operation or maintenance of the reactor, or following an accident.

All piping that is part of the main or backup reactor coolant systems shall be entirely within the main containment structure, or in an extension to the containment structure.

The containment design shall incorporate systems in order to assist in controlling internal pressure and the release of radioactive material to the environment, following an accident.

The containment shall include at least the following subsystems:

1. the containment structure and related components
2. equipment required to isolate the containment envelope and maintain its completeness and continuity following an accident
3. equipment required to reduce the pressure and temperature of the containment and reduce the concentration of free radioactive material within the containment envelope
4. equipment required for limiting the release of radioactive material from the containment envelope following an accident

When the containment design includes the use of compressed air or non-condensable gas systems in response to a DBA, the autonomy of the compressed air system shall be demonstrated.

In the event of a loss of compressed air, containment isolation valves shall fail in their safe state.

The design authority shall identify where and when the containment boundary is credited for providing shielding for people and equipment.

Guidance

The design should establish acceptance criteria for inspection, testing 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, leakage from air-operated valves) should be considered in calculating containment pressure loads.

Additional information:

Additional information may be found in:

- CSA Group, N287.3, Design Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, Toronto, Canada.
- CSA Group, N290.0/N290.3, package, General requirements for safety systems of nuclear power plants and Requirements for the containment system of nuclear power plants, Toronto, Canada.

6.6.2 Strength of the containment structure

The strength of the containment structure shall provide sufficient margins of safety based on potential internal overpressures, underpressures, temperatures, dynamic effects such as missile generation, and reaction-forces anticipated to result in the event of DBAs. Strength margins shall be applied to access openings, penetrations, and isolation valves, and to the containment heat removal system.

The margins shall reflect:

1. effects of other potential energy sources, such as possible chemical reactions and radiolytic reactions
2. limited experience and experimental data available for defining accident phenomena and containment responses
3. conservatism of the calculation model and input parameters

The positive and negative design pressures within each part of the containment boundary shall include the highest and lowest pressures that could be generated in the respective parts as a result of any DBA.

The containment structure shall protect systems and equipment important to safety in order to preserve the safety functions of the plant.

The design shall support the maintenance of full functionality following a DBE for all the parts of the containment system credited in the safety analysis.

The seismic design of the concrete containment structure shall have an elastic response when subjected to seismic ground motions. The special detailing of reinforcement shall allow the structure to possess ductility and energy-absorbing capacity, which permits inelastic deformation without failure.

Guidance

Section 8.6.12 indicates that, in addition to the specific requirements for DBAs, consideration is given to severe accidents, 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.

6.6.3 Capability for pressure tests

The containment structure shall be subject to pressure testing at a specified pressure in order to demonstrate structural integrity. Testing shall be conducted before plant operation commences and at appropriate intervals throughout the plant's lifetime.

6.6.4 Leakage

Leakage rate limits

The safety leakage rate limit shall ensure that:

1. normal operation release limits are met
2. AOOs and DBAs will not result in exceeding dose acceptance criteria

The design leakage rate limit shall be:

1. below the safety leakage rate limit
2. as low as is practicably attainable
3. consistent with state-of-the-art design practices

Test acceptance leakage rate limits

A test acceptance leakage rate shall provide the maximum rate acceptable under actual measurement tests. Test acceptance leakage rate limits shall be established for the entire containment system, and for individual components that can contribute significantly to leakage.

The containment structure and the equipment and components affecting the leak tightness of the containment system shall be designed to allow leak rate testing:

1. for commissioning, at the containment design pressure
2. over the service lifetime of the reactor, in accordance with applicable codes and standards

The design shall provide ready and reliable detection of any significant breach of the containment envelope.

Guidance

A modern containment should be able to achieve a leakage rate of 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.

Additional information

Additional information may be found in:

- CSA Group, N287.7, In-service Examination and Testing Requirements for Concrete Containment Structures for CANDU Nuclear Power Plants, Toronto, Canada.
- CSA Group, N287.6, Pre-operational proof and leakage rate testing requirements for concrete containment structures for nuclear power plants, Toronto, Canada.

6.6.5 Containment penetrations

The number of penetrations through the containment shall be kept to a minimum.

All containment penetrations shall be subject to the same design requirements as the containment structure itself, and shall be protected from reaction forces stemming from pipe movement or accidental loads, such as those due to missiles generated by external or internal events, jet impact, and pipe whip.

All penetrations shall be designed to allow for periodic inspection and testing.

If resilient seals such as elastomeric seals, electrical cable penetrations, or expansion bellows are used with penetrations, they shall have the capacity for leak testing at the containment design pressure. To demonstrate continued integrity over the lifetime of the plant, this capacity shall support testing that is independent of determining the leak rate of the containment as a whole.

Guidance

Keeping the number of penetrations through the containment to a minimum should consider the need for separation and redundancy, and be consistent with modern designs.

6.6.6 Containment isolation

Each line of the reactor coolant pressure boundary that penetrates the containment, or that is connected directly to the containment atmosphere, shall be automatically and reliably sealed. This requirement is essential to maintaining the leak tightness of the containment in the event of an accident, and preventing radioactive releases to the environment that exceed prescribed limits.

Automatic isolation valves shall be positioned to provide the greatest safety upon loss of actuating power.

Piping systems that penetrate the containment system shall have isolation devices with redundancy, reliability, and performance capabilities that reflect the importance of isolating the various types of piping systems. Alternative types of isolation may be used where justification is provided.

Where manual isolation valves are used, they shall be readily accessible and have locking or continuous monitoring capability.

Reactor coolant system auxiliaries that penetrate containment

Each auxiliary line that is connected to the reactor coolant pressure boundary, and that penetrates the containment structure, shall include two isolation valves in series. The valves shall be normally arranged with one inside and one outside the containment structure.

Where the valves provide isolation of the heat transport system during normal operation, both valves shall be normally in the closed position.

Systems directly connected to the reactor coolant system that may be open during normal operation shall be subject to the same isolation requirements as the normally closed system, with the exception that manual isolating valves inside the containment structure will not be used. At least one of the two isolation valves shall be either automatic or powered, and operable from the main and secondary control rooms.

For any piping outside of containment that could contain radioactivity from the reactor core, the following requirements shall apply:

1. The design parameters shall be the same as those for a piping extension to containment, and are subject to the requirements for metal penetrations of containment.
2. All piping and components that are open to the containment atmosphere shall be designed for a pressure greater than the containment design pressure.
3. The piping and components shall be housed in a confinement structure that prevents leakage of radioactivity to the environment and to adjacent structures.
4. This housing shall include detection capability for leakage of radioactivity, and the capability to deal safely with the leakage.

Systems connected to containment atmosphere

Each line that connects directly to the containment atmosphere, that penetrates the containment structure and that is not part of a closed system shall be provided with two isolation barriers that meet the following requirements:

1. two automatic isolation valves in series for lines that may be open to the containment atmosphere
2. two closed isolation valves in series for lines that are normally closed to the containment atmosphere

3. the line up to and including the second valve is part of the containment envelope

Closed systems

All closed piping service systems shall have at least one single isolation valve on each line penetrating the containment, with the valve being located outside of, but as close as practicable to, the containment structure.

Where failure of a closed loop is assumed to be a PIE or the result of a PIE, the isolations appropriate to the system shall apply.

Closed piping service systems, whether inside or outside the containment structure, that form part of the containment envelope, require no further isolation if:

1. they meet the applicable service piping standards and codes
2. they can be continuously monitored for leaks

6.6.7 Containment airlocks

Personnel access to the containment shall take place through airlocks equipped with doors that are interlocked to ensure that at least one of the doors is closed during operational states, DBAs and DECs.

Where provision is made for entry of personnel for surveillance or maintenance purposes during normal operation, the design shall specify provisions for personnel safety, including emergency egress. This requirement shall also apply to equipment air locks.

Guidance

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

6.6.8 Internal structures of the containment

The design shall provide for ample flow routes between separate compartments inside the containment. The openings between compartments shall be large enough to prevent significant pressure differentials, which may cause damage to load-bearing and safety systems during AOOs, DBAs and DECs.

The design of internal structures shall consider the hydrogen control strategy, and assist in the effectiveness of that strategy.

Guidance

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, DBAs and DECs (including consideration of hydrogen). In particular, the analyses of a large LOCA, main steamline break and DBE 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

Additional information may be found in:

- CSA Group, N291, Requirements for Safety-Related Structures for CANDU Nuclear Power Plants, Toronto, Canada.

6.6.9 Containment pressure and energy management

The design shall enable heat removal and pressure reduction in the reactor containment in operational states, DBAs and DECs. Systems designed for this purpose shall be treated as part of the containment system, and are capable of:

1. minimizing the pressure-assisted release of fission products to the environment
2. preserving containment integrity
3. preserving required leak tightness

Guidance

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

Pressure and energy management 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.

6.6.10 Control and cleanup of the containment atmosphere

The design shall provide systems to control the release of fission products, hydrogen, oxygen, and other substances into the reactor containment, as necessary, to:

1. reduce the amount of fission products that might be released to the environment during an accident
2. prevent deflagration or detonation that could jeopardize the integrity or leak tightness of the containment

The design shall also:

1. provide isolation of all sources of compressed air and other non-condensable gases into the containment atmosphere following an accident
2. ensure that, in the case of ingress of non-condensable gas resulting from a PIE, containment pressure will not exceed the design limit
3. provide isolation of compressed air sources to prevent any bypass of containment

6.6.11 Coverings, coatings and materials

The coverings and coatings for components and structures within the containment shall be carefully selected, and their methods of application shall be specified to ensure fulfillment of their safety functions. The primary objective of this requirement is to minimize interference with other safety functions or accident mitigation systems in the event of deterioration of coverings and coatings. In addition, the choice of materials inside containment shall take into account the impact on post-accident containment conditions, including fission product behaviour, acidity, equipment fouling, radiolysis, fires, and other factors that may affect containment performance and integrity, and fission product release.

Coverings and coatings shall also be selected considering the need for their removal and replacement to permit access to components for maintenance and inspection.

Guidance

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.

6.6.12 Design extension conditions

Following onset of core damage, the containment boundary shall be capable of contributing to the reduction of radioactivity releases to allow sufficient time for the implementation of offsite emergency procedures.

Damage to the containment structure shall be limited to prevent uncontrolled releases of radioactivity, and to maintain the integrity of structures that support internal components.

The ability of the containment system to withstand loads associated with design extension conditions (DECs) shall be demonstrated in design documentation, and shall include the following considerations:

1. various heat sources, including residual heat, metal-water reactions, combustion of gases, and standing flames
2. pressure control
3. control of combustible gases
4. sources of non-condensable gases
5. control of radioactive material leakage
6. effectiveness of isolation devices
7. functionality and leak tightness of airlocks and containment penetrations
8. effects of the accident on the integrity and functionality of internal structures

The design authority shall demonstrate that complementary design features have been incorporated that will:

1. prevent a containment melt-through or failure due to the thermal impact of the core debris
2. facilitate cooling of the core debris
3. minimize generation of non-condensable gases and radioactive products
4. preclude unfiltered and uncontrolled release from containment

Guidance

Provisions for DECs vary greatly between designs. The claimed functionality and analysis should be supported by adequate evidence.

The containment leakage rate in DECs with core damage should 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.

The design should minimize generation of combustible, non-condensable gases from corium-concrete interaction.

Containment venting design should take into account such factors as:

- ignition of flammable gases
- generation of non-condensable 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.

6.7 Heat transfer to an ultimate heat sink

The design shall include systems for transferring residual heat from SSCs important to safety to an ultimate heat sink. This overall function shall be subject to very high levels of reliability during operational states, DBAs and DECs. All systems that contribute to the transport of heat by conveying heat, providing power, or supplying fluids to the heat transport systems shall therefore be designed in accordance with the importance of their contribution to the function of heat transfer as a whole.

Natural phenomena and human induced events shall be taken into account in the design of heat transfer systems, and in the choice of diversity and redundancy, both in the ultimate heat sinks and in the storage systems from which fluids for heat transfer are supplied.

The design shall extend the capability to transfer residual heat from the core to an ultimate heat sink so that, in the event of a severe accident considered as a DEC:

1. acceptable conditions can be maintained in SSCs needed for mitigation of severe accidents
2. radioactive materials can be confined
3. releases to the environment can be limited

Guidance

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, DBAs and DECs.

6.8 Emergency heat removal system

The design shall include an emergency heat removal system (EHRS) which provides for removal of residual heat in order to meet fuel design limits and reactor coolant boundary condition limits.

If the design of the plant is such that the EHRS is required to mitigate the consequences of a DBA, then the EHRS shall be designed as a safety system. There shall be reasonable confidence that the EHRS will function during DECs, if required.

Correct operation of the EHRS equipment following an accident shall not be dependent on power supplies from the electrical grid or from the turbine generators associated with any reactor unit that is located on the same site as the reactor involved in the accident.

Where water is required for the EHRS, it shall come from a source that is independent of normal supplies.

The design shall support maintenance and reliability testing without a reduction in system effectiveness below what is required by the OLCs.

As far as practicable, inadvertent operation of the EHRS, or of part of the EHRS, shall not have a detrimental effect on plant safety.

If the fire water supply or system components are interconnected with the EHRS, operation of one shall not impair operation of the other.

Guidance

The emergency heat removal system is to provide a path to the ultimate heat sink, in the case that normal heat removal capabilities are not available. The purpose of this system is to prevent events 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 in DBAs or DECs. 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 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 provided by a separate pumped supply or by a secondary depressurization and gravity feed. The water supply should meet the requirements of a safety system.

6.9 Electrical power systems

The design shall specify the required functions and performance characteristics of each electrical power system that provides normal, standby, emergency and alternate power supplies to ensure:

1. sufficient capacity to support the safety functions of the connected loads in operational states, DBAs and DECs
2. availability and reliability is commensurate with the safety significance of the connected loads

The requirements of both the standby and emergency power systems may be met by a single system.

Electrical power systems shall be designed to include the various modes of interaction between offsite power and onsite power. In addition, design provisions shall be established for coping with grid disturbances, including conditions caused by solar flare (coronal mass ejection) events.

The design shall specify:

1. environmental and electromagnetic conditions to which electrical equipment and cables may be subjected
2. limits on electromagnetic emissions conducted or radiated from electrical equipment

The electrical power systems shall include appropriate protection, control, monitoring and testing facilities.

Guidance

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 alternating current (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 lightning surges

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

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 provided 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 sufficient to have only one offsite power connection, although this should be justified.

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 offsite 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

Additional information may be found in:

- CSA Group, N290.5, *Requirements for electrical power and instrument air systems of CANDU nuclear power plants,* Toronto, Canada (note**:** CSA N290.5 is a CANDU specific document which particularly addresses the two group design philosophy).
- IAEA, NS-G-1.8, *Design of Emergency Power Systems of Nuclear Power Plants*, Vienna, 2004.
- IEEE, 1050, *Guide for Instrumentation and Control Equipment Grounding in Generating Stations*, Piscataway, New Jersey 1996.
- IEEE, C62.23, *IEEE Application Guide for Surge Protection of Electric Generating Plants*, Piscataway, New Jersey, 1995.
- IEEE, 141, *IEEE Recommended Practice for Electric Power Distribution for Industrial Plants*, Piscataway, New Jersey, 1993.
- IEEE, 242, *IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems*, Piscataway, New Jersey, 2001.
- IEEE, 308, *IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations*, Piscataway, New Jersey, 2001.
- IEEE, 387, *IEEE Standard Criteria for Diesel-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations*, Piscataway, New Jersey, 1995.
- IEEE, 279, *IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations*, Piscataway, New Jersey, 1971.
- IEEE, 665, *IEEE Standard for Generating Station Grounding*, Piscataway, New Jersey, reaffirmed 2001.

6.9.1 Standby and emergency power systems

The standby and emergency power systems shall have sufficient capacity and reliability, for a specified mission time, and in the presence of a single failure to provide the necessary power to:

1. maintain the plant in a safe shutdown state and ensure nuclear safety in DBAs and DECs
2. support severe accident management actions

Dedicated onsite fuel storage facilities shall have a sufficient quantity of fuel to operate standby and emergency power sources while supplying connected loads.

The PPS to the electrical power systems shall be from offsite power or the main generator.

The design shall:

1. identify all events for which actuation of standby and emergency power sources is required
2. specify the required start-up time and safety load energization times for standby and emergency power sources such that they are available in a time commensurate with the safety function of the connected loads
3. specify conditions for electrical protection to trip standby and emergency power sources to protect equipment from significant failure
4. minimize challenges to standby and emergency power supplies as a result of an electrical system disturbance or transient condition
5. specify requirements for standby and emergency power supplies including all support auxiliaries and fuel supplies

The design of the emergency power system shall take into account common-cause failures involving loss of normal power supply and standby power supply (if applicable). The emergency power system shall be electrically independent, physically separate and diverse from normal power supply and standby power system (if applicable).

The standby and emergency power sources shall:

1. preferably be initiated automatically
2. be capable of being periodically tested under load conditions representing full load demand and full mission time

Guidance

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 onsite storage.

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

6.9.2 DC and uninterruptible power systems

The design of the direct current (DC) power systems and uninterruptible AC power systems (if applicable) shall specify operating mission times when performing the intended safety functions of the connected loads and meet the capacity requirements of section 7.10.

The design shall include provisions for periodic testing for DC power and uninterruptible AC power supplies to confirm their capability.

Guidance

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.

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

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 an 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.

6.9.3 Alternate AC power supply

The electrical power system design shall include provisions for mitigating the complete loss of onsite and offsite AC power. This is accomplished by the use of onsite portable, transportable or fixed power sources or offsite portable or transportable power sources, or a combination of these.

The alternate AC power source shall be available and located at or nearby the reactor facility, and shall:

1. be connectable to but not normally connected to the offsite or onsite standby and emergency AC power systems
2. have minimum potential for common mode failure with offsite power or the onsite standby and emergency AC power sources
3. be available in a timely manner after the onset of a station blackout
4. have sufficient capacity and reliability for operation of all systems required for coping with station blackout and for the time required to bring and maintain the plant in a safe shutdown state

The design shall include provision for periodic capacity testing of the alternate power supply to confirm its capability to cope with a station blackout event.

Guidance

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 station blackout (SBO) condition.

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

6.10 Control facilities

6.10.1 Main control room

The design shall provide for a main control room (MCR) from which the plant can be safely operated, and from which measures can be taken to maintain the plant in a safe state or to bring it back into such a state after the onset of AOOs, DBAs or DECs.

The design shall identify events both internal and external to the MCR that may pose a direct threat to its continued operation, and shall provide practicable measures to minimize the effects of these events.

The safety functions that can be initiated by automatic control logic in response to an accident shall be capable of being initiated manually from the MCR.

The layout of the controls and instrumentation, and the mode and format used to present information, shall provide operating personnel with an adequate overall picture of the status and performance of the plant and provide the necessary information to support operator actions.

The design of the MCR shall be such that appropriate lighting levels and thermal environment are maintained, and noise levels shall be minimized in accordance with applicable standards and codes.

The design of the MCR shall take ergonomic factors into account to provide both physical and visual accessibility to controls and displays, without adverse impact on health and comfort. This includes hardwired display panels as well as computerized displays, with the aim of making these displays as user-friendly as possible.

Cabling for the I&C equipment in the MCR shall be arranged such that a fire in the secondary control room (SCR) cannot disable the equipment in the MCR.

The design shall provide visual and, if appropriate, audible indications of plant conditions and processes that have deviated from normal operation and that could affect safety.

The design shall also allow for the display of information needed to monitor the effects of the automatic actions of all control, safety, and safety support systems.

The MCR shall be provided with secure communication channels to the emergency support facilities and to offsite emergency response organizations, and to allow for extended operating periods.

Guidance

There should be sufficient displays in the MCR to monitor all safety functions.

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

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

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 DBAs or DECs, release of radioactive material, fire, or explosive or toxic gases.

The manual initiation of safety functions 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.

Habitability assessments should be conducted for all control facilities. The minimum duration of habitability should be sufficient to fulfill the required safety function in each facility. Criteria for control room habitability should be established.

6.10.1.1 Safety parameter display system

The MCR shall contain a safety parameter display system (SPDS) that presents sufficient information on safety-critical parameters for the diagnosis and mitigation of DBAs and DECs.

The SPDS shall have the following capabilities:

1. display safety-critical parameters within the full range expected in operational states, DBAs and DECs
2. track data trends
3. indicate when process or safety limits are being approached or exceeded
4. display the status of safety systems

The SPDS shall be designed and installed such that the same information is made available in a secure manner to the emergency response facility.

The SPDS shall be integrated and harmonized with the overall control room human-system interface design.

Guidance

The primary function of the 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 relate to functions such as:

- 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 shown 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.

6.10.2 Secondary control room

The design shall provide an SCR that is physically and electrically separate from the MCR, and from which the plant can be placed and kept in a safe shutdown state when the ability to perform essential safety functions from the MCR is lost.

The design shall identify all events that may pose a direct threat to the continued operation of the MCR and the SCR. The design of the MCR and the SCR shall be such that no event can simultaneously affect both control rooms to the extent that the essential safety functions cannot be performed.

For any PIE, at least one control room shall be habitable and accessible by means of a qualified route.

Instrumentation, control equipment, and displays shall be available in the SCR so that the essential safety functions can be performed, essential plant variables can be monitored, and operator actions are supported.

Safety functions initiated by automatic control logic in response to an accident shall also be capable of being initiated manually from the SCR.

The design of the SCR shall ensure that appropriate lighting levels and thermal environment are maintained, and noise levels align with applicable standards and codes.

Ergonomic factors shall apply to the design of the SCR to ensure physical and visual accessibility to controls and displays, without adverse impact on health and comfort. These shall include hardwired display panels as well as computerized displays that are as user-friendly as possible.

Cabling for the I&C equipment in the SCR shall be such that a fire in the MCR cannot disable the equipment in the SCR.

The SCR shall be equipped with an SPDS similar to that in the MCR. At a minimum, this display system shall provide the information required to facilitate placing and keeping the plant in a safe shutdown state when the MCR is uninhabitable.

The SCR shall be provided with secure communication channels to the emergency response facility and to offsite emergency response organizations.

The SCR shall allow for extended operating periods.

Guidance

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.

There should be adequate routes through which, under emergency conditions, the operation staff from one control room can safely leave and reach another control room.

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

6.10.3 Emergency support facilities

The design shall provide for onsite emergency support facilities that are separate from the plant control rooms for use by the technical support staff and emergency support staff in the event of an emergency.

The emergency support facilities shall consist of a technical support centre (TSC) and an onsite emergency response facility (ERF). The technical support centre and the emergency response facility can be located in one place or separated.

The emergency support facilities shall provide equipment, facilities, and communication means for trained staff to manage, control and coordinate any emergency response and to provide technical support to operations, emergency response organizations, and severe accident management evaluation.

The emergency support facilities design shall ensure that appropriate lighting levels and thermal environment are maintained, and that noise levels are minimized in accordance with applicable standards and codes.

The emergency support facilities shall include secure means of communication with the MCR, SCR, and other important points in the plant, and with onsite and offsite emergency response organizations.

The design shall ensure that the emergency support facilities:

1. include provisions to protect occupants over protracted periods from the hazards resulting from DBAs and DECs
2. are equipped with adequate facilities to allow extended operating periods

The emergency response facility shall include a SPDS similar to those in the MCR and in the SCR.

Information about the radiological conditions in the plant and its immediate surroundings, and about meteorological conditions in the vicinity of the plant, shall be accessible from the ERF.

Guidance

The design provides emergency support facilities which include a technical support center and an onsite emergency response facility.

The TSC will provide the following functions:

- provide technical support and plant management to plant operation personnel during emergency conditions
- handle peripheral duties and communication not directly related to reactor manipulations in order to relieve the burden of reactor operators during emergency conditions
- prevent congestion in the control rooms
- perform emergency support functions until the emergency response facility is functional

To facilitate the above functions, the TSC should be located as close as possible to control rooms of sufficient size to accommodate the technical support staff.

Equipment should be provided to gather, store, and display data needed in the TSC to analyze plant conditions.

The TSC should have a complete and up-to-date repository of plant records to aid the technical analysis and evaluation of emergency conditions.

Equipment should be provided in the emergency response facility for the acquisition, display, and evaluation of all radiological, meteorological, and plant system data required to determine offsite protective measures.

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

The emergency response facility data system should be designed to achieve an appropriate level of reliability.

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

If the TSC and emergency response facility are located in one place, then they should be physically separate from the control rooms with adequate distance to ensure the capability of carrying out their functions.

In the case of plants with multiple units at a site, the emergency support facilities should be demonstrated to be adequate to respond to common-cause events in multiple units.

6.10.4 Credit for operator action

If operator action is required for actuation of any safety system or safety support system equipment, all of the following requirements shall apply:

1. there are clear, well-defined, validated, and readily available operating procedures that identify the necessary actions
2. there is instrumentation in the control rooms to provide clear and unambiguous indication of the necessity for operator action
3. following indication of the necessity for operator action inside the control rooms, there are at least 30 minutes available before the operator action is required
4. following indication of the necessity for operator action outside the control rooms, there is a minimum of 1 hour available before the operator action is required

For automatically initiated safety systems and control logic actions, the design shall facilitate backup manual initiation from inside the appropriate control room.

Guidance

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

The available time before operator action can be credited should be counted from the receipt of an unambiguous indication of a potential accident (typically an alarm) and include diagnostic time.

The time available to perform the actions should be based on the analysis of the plant response to AOOs and DBAs, using realistic assumptions. The time required for operator action should be based on a human factors engineering 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 this regulatory document, 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 of 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.

Where justified, alternative action times may be used. The alternative action times should make due allowance for the complexity of the action to be taken, and the time needed for activities such as diagnosing the event and accessing the field location.

Additional information

Additional information may be found in:

- ANSI/ANS, 58.8, Time Response Design Criteria for Safety Related Operator Actions, La Grange Park, Illinois, 2008.
- CSA Group, N290.4, Requirements for Reactor Control Systems of Nuclear Power Plants, Toronto, Canada.
- CNSC, G-225, Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills, Ottawa, Canada, 2001, or successor document.
- IEC, 60964, Nuclear Power Plants - Control Rooms – Design, Geneva, 2009.

- IEC, 60965, Nuclear Power Plants - Control Rooms - Supplementary Control Points for Reactor Shutdown Without Access to the Main Control Room, Geneva, 2009.
- NEI 99-03, Control Room Habitability Assessment Guidance, Washington, D.C., 2001.
- U.S. NRC, NUREG-0696, Functional Criteria for Emergency Response Facilities, Washington, D.C., 1981.
- U.S. NRC, Regulatory Guide 1.196, Control Room Habitability at Light-Water Nuclear Power Reactors, Washington, D.C., 2003.

6.11 Waste treatment and control

The design shall include provisions to treat liquid and gaseous effluents in a manner that will keep the quantities and concentrations of discharged contaminants within prescribed limits, and that will support application of the ALARA principle.

The design of the reactor facility shall minimize the generation of radioactive and hazardous waste. The design shall also include adequate provision for the safe onsite handling and storage of radioactive and hazardous wastes, for a period of time consistent with options for offsite management or disposal.

Additional information

Additional information may be found in:

- CNSC, P-290, *Managing Radioactive Waste*, Ottawa, Canada, 2004.

6.11.1 Control of liquid releases to the environment

To ensure that emissions and concentrations remain within prescribed limits, the design shall include suitable means for controlling liquid releases to the environment in a manner that conforms to the ALARA principle.

This shall include a liquid waste management system of sufficient capacity to collect, hold, mix, pump, test, treat, and sample liquid waste before discharge, taking expected waste and accidental spills or discharges into account.

6.11.2 Control of airborne material within the plant

The design shall include gaseous waste management systems capable of:

1. controlling all gaseous contaminants so as to conform to the ALARA principle and ensure that concentrations remain within prescribed limits
2. collecting all potentially active gases, vapours, and airborne particulates for monitoring
3. passing all potentially active gases, vapours, and airborne particulates through pre-filters, absolute filters, charcoal filters, or high efficiency particulate air filters where applicable
4. delaying releases of potential sources of noble gases by way of an off-gas system of sufficient capacity

The design shall provide a ventilation system with an appropriate filtration system capable of:

1. preventing unacceptable dispersion of all airborne contaminants within the plant
2. reducing the concentration of airborne radioactive substances to levels compatible with the need for access to each particular area

3. keeping the level of airborne radioactive substances in the plant below prescribed limits, applying the ALARA principle in normal operation
4. ventilating rooms containing inert or noxious gases without impairing the capability to control radioactive releases

Guidance

Radiological zones may be established in the reactor facility 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 higher contamination. Recirculation of air within one zone or room may be permitted.

6.11.3 Control of gaseous releases to the environment

The ventilation system shall include filtration that will:

1. control the release of gaseous contaminants and hazardous substances to the environment
2. ensure conformation to the ALARA principle
3. maintain airborne contaminants within prescribed limits

The filtration system shall reliably achieve the necessary retention factors under the expected prevailing conditions, and shall be designed in a manner that facilitates appropriate efficiency testing.

Guidance

A gaseous waste management system is designed to collect all active or potentially active gases, vapours, or airborne particulates that may occur, in order to monitor and filter the effluent before it is released to the atmosphere. The filter units should be placed in a fully enclosed room with concrete walls and floors thick enough to protect station personnel from radiation. Monitors should be 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 should also be monitored and filtered before discharge to the atmosphere.

Additional information

Additional information may be found in:

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

6.12 Fuel handling and storage

There shall be barriers to prevent the insertion of incorrect, defective or damaged fuel into the reactor.

There shall be provisions to prevent contamination of the fuel and the reactor.

The design shall meet the requirements found in CNSC RD-327, *Nuclear Criticality Safety*.

Guidance

The design should provide the basis for the fuel handling and storage systems. The design should include 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 criticality safety requirements are provided in CNSC RD-327, *Nuclear Criticality Safety*. Comprehensive guidance on criticality safety and complete technical reference is provided in CNSC 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

Additional information may be found in:

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

6.12.1 Handling and storage of non-irradiated fuel

The design of the fuel handling and storage systems for non-irradiated fuel shall:

1. ensure nuclear criticality safety
2. permit appropriate maintenance, periodic inspection, and testing of components important to safety
3. permit inspection of non-irradiated fuel
4. prevent loss of or damage to the fuel
5. meet Canada's safeguards requirements for recording and reporting accountancy data, and for monitoring flows and inventories related to non-irradiated fuel containing fissile material

6.12.2 Handling and storage of irradiated fuel

The design of the handling and storage systems for irradiated fuel shall:

1. ensure nuclear criticality safety
2. permit adequate heat removal in operational states, DBAs and DECs
3. permit inspection of irradiated fuel
4. permit periodic inspection and testing of components important to safety
5. prevent the dropping of irradiated fuel in transit
6. prevent unacceptable handling stresses on fuel elements or fuel assemblies
7. prevent the inadvertent dropping of heavy objects and equipment on fuel assemblies
8. permit inspection and safe storage of suspect or damaged fuel elements or fuel assemblies
9. provide proper means for radiation protection
10. permit adequate identification of individual fuel modules
11. facilitate maintenance and decommissioning of the fuel storage and handling facilities

12. facilitate decontamination of fuel handling and storage areas and equipment when necessary
13. ensure implementation of adequate operating and accounting procedures to prevent loss of fuel
14. include measures to prevent a direct threat or sabotage to irradiated fuel
15. meet Canada's safeguards requirements for recording and reporting accountancy data, and for monitoring flows and inventories related to irradiated fuel containing fissile material

A design for a water pool used for fuel storage shall include provisions for:

1. controlling the chemistry and activity of any water in which irradiated fuel is handled or stored
2. monitoring and controlling the water level in the fuel storage pool
3. detecting leakage
4. preventing the pool from emptying in the event of a pipe break
5. sufficient space to accommodate the entire reactor core inventory at all times

The design of irradiated fuel storage pools shall include means for preventing the uncovering of fuel in the pool in operational states, DBAs and DECs.

The design for a water pool used for fuel storage shall include provisions for DECs by:

1. ensuring that boiling in the pool does not result in structural damage
2. providing temporary connections to enable the refill of the pool using temporary supplies
3. providing temporary connections to heat removal systems for power and cooling water
4. providing hydrogen mitigation in the spent fuel pool area
5. ensuring that severe accident management actions related to the spent fuel pool can be carried out

Guidance

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. Hydrogen mitigation in the spent fuel pool area may not be necessary if draining of the pool beyond make-up capability can be precluded.

6.12.3 Detection of failed fuel

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.

Guidance

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

6.13 Radiation protection

The design and layout of the plant shall make suitable provision to minimize exposure and contamination from all sources. This shall include the adequate design of SSCs to:

1. control access to the plant
2. minimize exposure during maintenance and inspection
3. provide shielding from direct and scattered radiation

4. provide ventilation and filtering to control airborne radioactive materials
5. limit the activation of corrosion products by proper specification of materials
6. minimize the spread of active material
7. monitor radiation levels
8. provide suitable decontamination facilities

Guidance

The reactor facility 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

Additional information may be found in:

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

6.13.1 Design for radiation protection

The shielding design shall prevent radiation levels in operating areas from exceeding the prescribed limits. This shall include provision of appropriate permanent layout and shielding of SSCs containing radioactive materials, and the use of temporary shielding for maintenance and inspection work.

To minimize radiation exposure, the plant layout shall provide for efficient operation, inspection, maintenance, and replacement. In addition, the design shall limit the amount of activated material and its build-up.

The design shall account for frequently occupied locations, and support the need for human access to locations and equipment.

Access routes shall be shielded where needed.

The design shall enable operator access for actions credited for post-accident conditions.

Adequate protection shall be provided against exposure to radiation and radioactive contamination during DBAs and DECs for those parts of the facility to which access is required.

Guidance

Shielding should be designed based on the zone delineation described in section 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 reactor facility.

6.13.2 Access and movement control

The plant layout and procedures shall control access to radiation areas and areas of potential contamination.

The design shall minimize the movement of radioactive materials and the spread of contamination, and provide appropriate decontamination facilities for personnel.

Guidance

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.

6.13.3 Radiation monitoring

Equipment shall be provided to ensure that there is adequate radiation monitoring in operational states, DBAs and DECs.

Stationary alarming dose rate meters shall be provided:

1. for monitoring the local radiation dose rate at places routinely occupied by operating personnel
2. where the changes in radiation levels may be such that access may be limited for periods of time
3. to indicate, automatically and in real time, the general radiation level at appropriate locations in operational states, DBAs and DECs
4. to give sufficient information in the control room or at the appropriate control location for operational states, DBAs and DECs, to enable plant personnel to initiate corrective actions when necessary

Monitors shall be provided for measuring the activity of radioactive substances in the atmosphere:

1. for areas routinely occupied by personnel
2. for areas where the levels of activity of airborne radioactive materials may, on occasion, be expected to necessitate protective measures
3. to give an indication in the control room, or in other appropriate locations, of when a high concentration of radionuclides is detected

Facilities shall be provided for monitoring individual doses to and contamination of personnel.

Stationary equipment and laboratory facilities shall be provided to determine the concentration of selected radionuclides in fluid process systems as appropriate, and in gas and liquid samples taken from plant systems or the environment.

Stationary equipment shall be provided for monitoring the effluents prior to or during discharge to the environment.

6.13.4 Sources of radiation

The design shall provide for:

1. appropriate disposal of radioactive materials, either to onsite storage or through removal from the site
2. reduction in the quantity and concentration of radioactive materials produced
3. control of dispersal within the plant
4. control of releases to the environment
5. decontamination facilities for equipment, and for handling any radioactive waste arising from decontamination activities
6. minimization of radioactive waste generation

6.13.5 Monitoring environmental impact

The design shall provide the means for monitoring radiological and hazardous releases to the environment in the vicinity of the plant, with particular reference to:

1. pathways to the human population, including the food chain
2. the radiological impact, if any, on local ecosystems
3. the possible accumulation of radioactive and hazardous materials in the environment
4. the possibility of any unauthorized discharge routes

Guidance

Additional guidance can be found in CSA N288.4, *Environmental Monitoring Programs at Class I Nuclear Facilities and Uranium Mines and Mills*.

6.14 Secondary side cooling system

When a steam supply system is installed, the system design shall meet the applicable requirements in section 8.3.

When a steam supply system is not installed, the system shall meet the applicable requirements set out in section 8.2.

6.15 Auxiliary systems

The failure of any auxiliary system, irrespective of its importance to safety, shall not be able to jeopardize the safety of the reactor facility.

Adequate measures shall be taken to prevent the release of radioactive material to the environment in the event of the failure of an auxiliary system containing radioactive material.

7. Safety analysis

7.1 General

A safety analysis of the plant design shall include hazard analysis, deterministic safety analysis, and probabilistic safety assessment (PSA) techniques. The safety analysis shall demonstrate achievement of all levels of defence in depth, and confirm that the design is capable of meeting the applicable expectations, dose acceptance criteria and safety goals.

Radioactive sources other than the reactor core, such as the spent fuel pool and fuel handling systems, shall be considered. Impacts for multiple units at a site, if applicable, shall be included.

The first step of the safety analysis shall be to identify PIEs using a systematic methodology, such as failure modes and effects analysis. Both direct and indirect events shall be considered in PIE identification. Requirements and guidance for identification of PIEs is given in section 7.4 of this document.

7.2 Analysis objectives

The safety analysis shall be iterative with the design process, and result in two reports: a preliminary safety analysis report, and a final safety analysis report.

The preliminary safety analysis shall assist in the establishment of the design-basis requirements for the items important to safety, and demonstrate whether the plant design meets applicable requirements.

The final safety analysis shall:

1. reflect the as-built plant
2. account for postulated aging effects on SSCs important to safety
3. demonstrate that the design can withstand and effectively respond to identified PIEs
4. demonstrate the effectiveness of the safety systems and safety support systems
5. derive the OLCs for the plant, including:
    a. operational limits and set points important to safety
    b. allowable operating configurations, and constraints for operational procedures
6. establish requirements for emergency response and accident management
7. determine post-accident environmental conditions, including radiation fields and worker doses, to confirm that operators are able to carry out the actions credited in the analysis
8. demonstrate that the design incorporates sufficient safety margins
9. confirm that the dose and derived acceptance criteria are met for all AOOs and DBAs
10. demonstrate that all safety goals have been met

Guidance

The *Class I Nuclear Facilities Regulations* require a preliminary safety analysis report demonstrating the adequacy of the reactor facility design to be submitted in support of an application for a licence to construct a Class I nuclear facility. A final safety analysis report demonstrating the adequacy of the design is required for an application for a licence to operate a Class I nuclear facility.

7.3 Hazard analysis

Hazard analysis shall collect and evaluate information about the reactor facility to identify the associated hazards and determine those that are significant and must be addressed. A hazard analysis shall demonstrate the ability of the design to effectively respond to credible common-cause events.

As discussed in section 9.1, the first step of the hazard analysis is to identify PIEs. For each common-cause PIE, the hazard analysis shall identify:

1. applicable acceptance criteria (i.e., the success path criteria)
2. the hazardous materials in the plant and at the plant site
3. all qualified mitigating SSCs credited during and following the event; all non-qualified safety or safety support systems are assumed to fail, except in cases where their continued operation would result in more severe consequences
4. operator actions and operating procedures for the event
5. plant or operating procedure parameters for which the event is limiting

The hazard analysis shall confirm that:

1. the plant design incorporates sufficient diversity and separation to cope with credible common-cause events
2. credited SSCs are qualified to survive and function during and following credible common-cause events, as applicable
3. the following criteria are met:
   a. the plant can be brought to a safe shutdown state
   b. the integrity of the fuel in the reactor core can be maintained
   c. the integrity of the reactor coolant pressure boundary and containment can be maintained
   d. safety-critical parameters can be monitored by the operator

The hazard analysis report shall include the findings of the analysis and the basis for those findings. This report shall also:

1. include a general description of the physical characteristics of the plant that outlines the prevention and protection systems to be provided
2. include the list of safe shutdown equipment
3. define and describe the characteristics associated with hazards for all areas that contain hazardous materials
4. describe the performance criteria for detection systems, alarm systems, and mitigation systems, including requirements such as seismic or environmental qualification
5. describe the control and operating room areas and the protection systems provided for these areas, including additional facilities for maintenance and operating personnel
6. describe the operator actions and operating procedures of importance to the given analysis
7. identify the plant parameters for which the event is limiting
8. explain the inspection, testing, and maintenance parameters needed to protect system integrity

9. define the emergency planning and coordination requirements for effective mitigation, including any necessary measures to compensate for the failure or inoperability of any active or passive protection system or feature

Guidance

The objective of the hazard analysis is to determine the adequacy of protection of the reactor facility 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 facilities) should be adequately protected against relevant internal and external hazards.

The hazard 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 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 hazard analysis should demonstrate that the design incorporates sufficient safety margins.

Additional information

Additional information may be found in:

- CNSC, RD-346, Site Evaluation for New Nuclear Power Plants, Ottawa, Canada, 2008.
- CNSC, RD/GD-369, Licence Application Guide: Licence to Construct a Nuclear Power Plant, Ottawa, Canada, 2011.
- CSA Group, N293, Fire protection for nuclear power plants, Toronto, Canada, 2012.
- CSA Group, N289.4, Testing procedures for seismic qualification of nuclear power plants, Toronto, Canada.
- IAEA, NS-G-3.3, Evaluation of Seismic Hazards for Nuclear Power Plants, Vienna, 2002.
- IAEA, NS-G-1.5, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Vienna, 2003.
- IAEA, NS-G-3.1, External Human Induced Events in Site Evaluation for Nuclear Power Plants, Vienna, 2002.
- IAEA, NS-G-3.5, Flood Hazard for Nuclear Power Plants on Coastal and River Sites, Vienna, 2003.
- IAEA, NS-G-3.4, Meteorological Events in Site Evaluation for Nuclear Power Plants, Vienna, 2003.
- IAEA, SSG-18, Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations, Vienna, 2011.
- IAEA, NS-G-1.7, Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants, Vienna, 2004.

- IAEA, NS-G-1.11, Protection Against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, Vienna, 2004.
- IAEA, NS-G-1.6, Seismic Design and Qualification for Nuclear Power Plants, Vienna, 2003.
- IAEA, SSG-9, Seismic Hazards in Site Evaluation for Nuclear Installations, 2 Vienna, 2010.

7.4 Deterministic safety analysis

The deterministic safety analysis shall be conducted in accordance with the requirements specified in CNSC regulatory document REGDOC-2.4.1, *Deterministic Safety Analysis*.

Additional information

Additional information may be found in:

- CNSC, REGDOC-2.4.1, *Deterministic Safety Analysis,* Ottawa, Canada, 2014.
- CNSC, RD/GD-369, *Licence Application Guide: Licence to Construct a Nuclear Power Plant*, Ottawa, Canada, 2011.
- CSA Group, N286.7.1, *Guideline for the Application of N286.7-99, Quality Assurance of Analytical, Scientific, and Design Computer Programs for Nuclear Power Plants*, Toronto, Canada.
- CSA Group, N286.7, *Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants*, Toronto, Canada.
- IAEA, SSG-2, *Deterministic Safety Analysis for Nuclear Power Plants*, Vienna, 2009.
- IAEA NS-G-1.2, Safety Assessment and Verification for Nuclear Power Plants, Vienna, 2001.

7.5 Probabilistic safety assessment

The probabilistic safety assessment shall be conducted in accordance with the requirements specified in CNSC REGDOC-2.4.2, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*.

Additional information

Additional information may be found in:

- ASME/ANS, RA-Sa-2009, Standard for Level 1/Large Early Release Frequency PRA for Nuclear Power Plant Applications, La Grange, Illinois, 2009.
- CNSC RD/GD-369, Licence Application Guide: Licence to Construct a Nuclear Power Plant, Ottawa, Canada, 2011.
- CNSC, REGDOC-2.4.2, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, Ottawa, Canada, 2014.
- IAEA, SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 2010.
- IAEA, SSG-4, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 2010.
- IAEA, Safety Series No. 50-P-10, Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 1995.
- IAEA Safety Reports Series No. 25, Review of Probabilistic Safety Assessments by Regulatory Bodies, Vienna, 2002.
- IAEA, Safety Series No. 50-P-7, Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 1995.
- IAEA, Safety Report Series No.10, Treatment of Internal Fires in Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 1998.

8. Environmental protection and mitigation

8.1 Design for environmental protection

The design shall make adequate provision to protect the environment and to mitigate the impact of the reactor facility on the environment. A review of the design shall confirm that this provision has been made.

A systematic approach shall be used to assess the potential biophysical environmental effects of the reactor facility on the environment, and the effects of the environment on the reactor facility.

Guidance

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

8.2 Release of nuclear and hazardous substances

The design shall demonstrate through process, monitoring, control, prevention, and mitigation measures that the releases of nuclear and hazardous substances will conform to the ALARA principle.

The lifecycle assessment shall identify various sources of nuclear and hazardous substances in design, operation, and decommissioning, along with their possible environmental impacts on human and non-human biota.

Some of the factors that shall be considered include:

1. resource requirements for the reactor facility such as fuel, energy, and water
2. depletion of ground and surface water resources
3. contamination of air, soil and water resources
4. nuclear and hazardous substances used
5. types of waste generated – gaseous, liquid and solid
6. quantities of waste generated
7. impact of cooling water intake on entrainment and impingement
8. impact of water output on the thermal regime of the receiving environment

Technological options shall be considered in establishing design objectives for controlling and monitoring releases during start-up, normal operation, shutdown, and potential abnormal and emergency situations. Appropriate limits shall be included in the plant OLCs.

Pollution prevention principles shall be applied when considering the technological design options for cooling water systems, in order to minimize adverse environmental impact.

Guidance

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 this regulatory document should include an initial estimate of the total inventory of all radioactive and hazardous materials that 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, chloro-fluoro-carbons, volatile organic compounds, nitrogen oxides, 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, and temperature), their management and the wastes created should be accounted for.

Pollution prevention principles should be applied through an assessment of various technological options, in order to identify the technology and techniques that are BATEA. The technological option selected for the design of cooling water systems should minimize the impact on the environment to the extent practicable given nuclear safety requirements. The economically achievable assessment of a technology option is not determined on the basis of a specific project, but rather at the industry level. Technical feasibility of an option depends upon site-specific conditions, taking into account environmental risk and socio-economic factors. The technology option of choice should be the one that best balances costs with environmental benefits resulting from application of a structured process of options analysis (e.g. cost-benefit analysis, multi-criteria decision analysis). It should include an assessment of:

- the age of equipment and facilities involved
- how the option is designed, built, maintained, operated and decommissioned
- the process employed
- the engineering aspects of the application of various types of control techniques
- process changes
- technological advances or changes in scientific knowledge and understanding
- cost of achieving the environmental benefits or reducing the environmental impacts
- socioeconomic factors
- time limits for installation of new and existing plants
- other environmental impacts (including energy requirements)
- other such factors as deemed appropriate by the regulator

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

Additional information

Additional information may be found in:

- CNSC, G-296, Developing Environmental Protection Policies, Programs and Procedures at Class I Nuclear Facilities and Uranium Mines and Mills, Ottawa, Canada, 2006.
- CNSC, REGDOC-2.9.1, Environmental Protection: Policies, Programs and Procedures, Ottawa, Canada, 2013.
- CNSC P-223, Protection of the Environment, Ottawa, Canada, 2001.
- CNSC, REGDOC-2.9.1, *Environmental Protection: Policies, Programs and Procedures*, Ottawa, Canada, 2017.
- CSA N288.5, Effluent Monitoring Programs at Class I Nuclear, 2011
- CSA N288.9, Guidance for Design of fish Impingement and Entrainment Program at Class I Nuclear Facilities, 2018
- CSA N288.6 Environmental Risk Assessment at Class I Nuclear Facilities, 2012
- CSA N288.7, Groundwater Protection Program at Class I Nuclear Facilities and Uranium Mines and Mills, 2015

9. Alternative approaches

The requirements in this regulatory document are intended to be technology neutral for water-cooled reactor designs. It is recognized that specific technologies may use alternative approaches.

The CNSC will consider alternative approaches to the requirements in this document where:

1. the alternative approach would result in an equivalent or superior level of safety
2. the application of the requirements in this document conflicts with other rules or requirements
3. the application of the requirements in this document would not serve the underlying purpose, or is not necessary to achieve the underlying purpose

Any alternative approach shall demonstrate equivalence to the outcomes associated with the use of the requirements set out in this regulatory document.

Appendix A: Structural Analysis of Containment Structures

This appendix provides further detailed guidance on acceptance criteria related to structural analysis of containment structures for robustness against malevolent acts in support of section 7.22.

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:

1. damage to the internal structures and to the containment due to extensive deformations of the containment building
2. shock damage to fragile components directly attached to the containment wall
3. induced vibration
4. structural integrity of the reserve water tank (e.g., CANDU design)
5. 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

Element type	Controlling stress	Design-basis threat	Beyond-design-basis threat		
			Shear ductility, μ_a	Flexure Support rotation in degrees[1,2], θ_a	
			Tier 1, 2	Tier 1	Tier 2
Beams	Flexure Shear: concrete only concrete + stirrups stirrups only compression	Essentially elastic behaviour [4]	 1.3 1.6 3.0 1.3	2	3
Slabs	Flexure Shear: concrete only concrete + stirrups stirrups only compression	Essentially elastic behaviour [4]	 1.3 1.6 3.0 1.3	4	6
Beam-columns, walls and slabs in compression	Flex ure She ar	Essentially elastic behaviour [4]	 1.3 [3]	2	3
Shear walls, diaphragms	Flexure Shear – In-plane Diaphragms	Essentially elastic behaviour [4]	 3 1.5	1.5	2

1. Transverse reinforcements are required for support rotations greater than 2 degrees.
2. These rotation criteria (in degrees) are, in general, consistent with those in TM 5-1300, *Structures to Resist the Effects of Accidental Explosions* – figure 2 illustrates the rotation angle.

3. For additional detailed criteria, see section F.3.8 of ACI-349, *Code Requirements for Nuclear Safety-related Concrete Structures and Commentary*
4. Essentially elastic behaviour means elastic structural analysis using design strain acceptance criteria of 1% for reinforcement in tension and 0.35% for concrete in compression.

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, *Requirements for Safety-Related Structures for CANDU Nuclear Power Plants*, respectively.

Figure 2: Reactor building under soft missile impact: global behaviour – support rotation

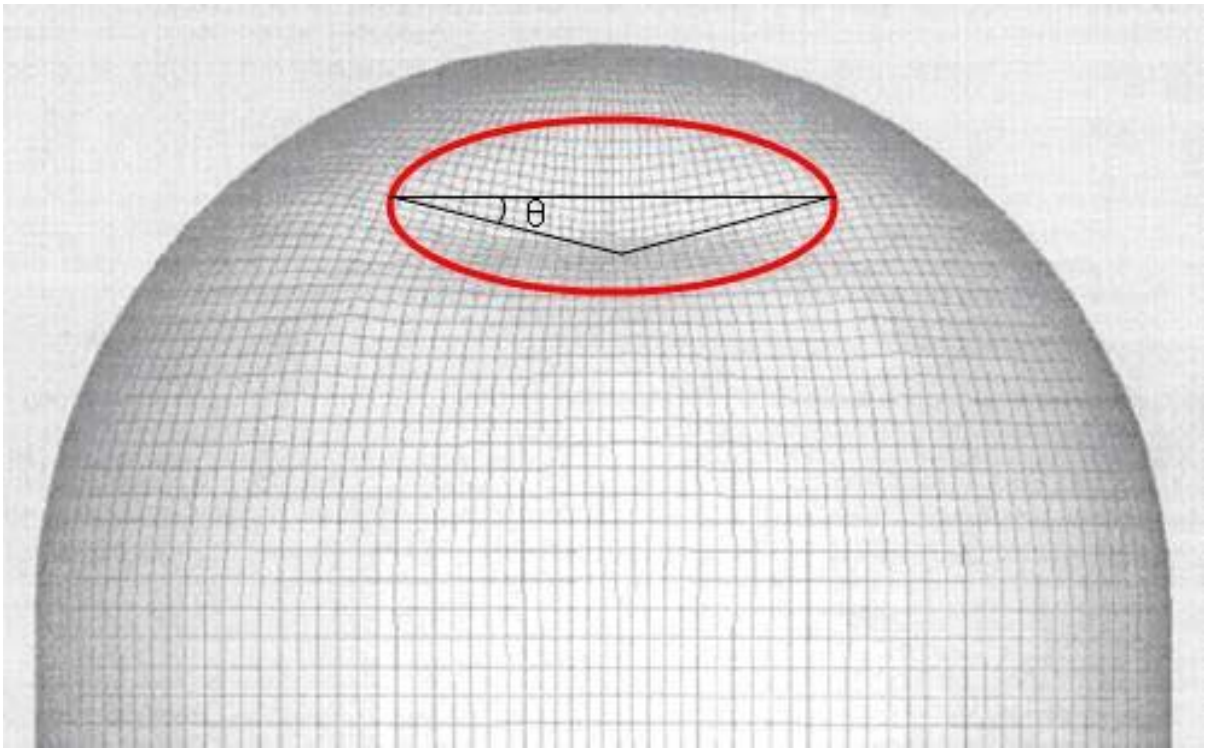


Table 2: Structural acceptance criteria - allowable strains for steel

Material	Strain measure	Allowable value design-basis threats	Allowable value for first-tier beyond-design-basis threats
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

*TF = triaxiality factor

Conservatively, TF can be taken as equal to 2.

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

Where σ1, σ2 and σ3 are principal stresses and σe is effective or equivalent stress.

The values in table 1 and table 2 are maximum values under the loading condition. For reinforced concrete, the maximum compression strain for DBTs is 0.0035.

For first-tier BDBTs, this strain is 0.005.

The strains are not provided in table 2 for second-tier BDBTs, but can be deduced from support rotations given in table 1.

Appendix B: Experimental Devices

This appendix is applicable when the reactor core employs experimental devices such as loops for fuel and material testing, irradiation sites or beam tubes.

The reactor behaviour under normal operation, transient and accident conditions shall be analyzed, including experimental devices. Any safety impact of any failure of experimental devices on the reactor core or that of any failure of the reactor core on the experimental devices shall be addressed.

A design basis shall be established for each experimental device associated with the reactor facility. The radioactive inventory of the experimental device, as well as the potential for the generation or release of energy, shall be taken into consideration.

Sufficient negative reactivity shall be available in the reactivity control devices so that the reactor can be brought to subcritical condition and maintained subcritical in normal operation and in accident conditions, with account taken of the experimental arrangements with the highest positive reactivity contribution. In the design of reactivity control devices, account shall be taken of aging and the effects of irradiation, such as burnup, changes in physical properties and the production of gas.

If safety devices are interconnected with the safety system, they shall be designed to maintain the quality of the safety system. The possibility of deleterious interactions with the safety system shall be assessed.

Trip parameters shall take into account the effects of experimental devices when employed in the reactor.

Where necessary for the safety of the reactor and the safety of the experiment, the design shall provide appropriate monitoring of the parameters for experiments in the main control room and shall include specific safety features, if necessary, for the reactor systems, experimental devices and any other related facility.

Requirements and limiting conditions for safe operation shall be prepared for experimental devices and incorporated into OLCs.

The maximum rate of addition of positive reactivity allowed by an experiment when employed shall be specified and shall be limited to values justified.

The preliminary decommissioning plan for the reactor facility shall include the decommissioning of any experimental device.

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 conditions
ECCS	emergency core cooling system
EHRS	emergency heat removal system
EQ	environmental qualification
GSS	guaranteed shutdown state
HCLPF	high confidence of 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
NPP	nuclear power plant

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

Glossary

For definitions of terms used in this document, see REGDOC-3.6, *Glossary of CNSC Terminology*, which includes terms and definitions used in the *Nuclear Safety and Control Act* and the regulations made under it, and in CNSC regulatory documents and other publications. REGDOC-3.6 is provided for reference and information.

The following terms are either new terms being defined, or include revisions to the current definition for that term. Following public consultation, the final terms and definitions will be submitted for inclusion in the next version of REGDOC-3.6, *Glossary of CNSC Terminology*.

References

The CNSC may include references to information on best practices and standards such as those published by CSA Group. With the permission of the publisher, CSA Group, all nuclear-related CSA standards may be viewed at no cost through the CNSC Web page "How to gain free access to all nuclear-related CSA standards."

1. Canadian Nuclear Safety Commission (CNSC), RD-336, *Accounting and Reporting of Nuclear Material*, Ottawa, Canada, 2010.

2. CNSC, RD-334, *Aging Management for Nuclear Power Plants*, Ottawa, Canada, 2011.

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

4. CNSC, RD-321, *Criteria for Physical Protection Systems and Devices at High-Security Sites*, Ottawa, Canada, 2010.

5. CNSC, G 219, *Decommissioning Planning for Licensed Activities*, Ottawa, Canada, 2000.

6. CNSC, G-296, *Developing Environmental Protection Policies, Programs and Procedures at Class I Nuclear Facilities and Uranium Mines and Mills*, Ottawa, Canada, 2006.

7. CNSC, G-225, *Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills, Ottawa, Canada*, 2001 or successor document.

8. CNSC, G-323, *Ensuring the Presence of Sufficient Qualified Staff at Class I Nuclear Facilities – Minimum Staff Complement*, Ottawa, Canada, 2007.

9. CNSC, REGDOC-2.9.1, *Environmental Protection: Policies, Programs and Procedures*, Ottawa, Canada, 2013.

10. CNSC, GD-336, *Guidance for Accounting and Reporting of Nuclear Material*, Ottawa, Canada, 2010.

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

12. CNSC, G-276, *Human Factors Engineering Program Plans*, Ottawa, Canada, 2003.

13. CNSC, G-278, *Human Factors Verification and Validation Plans*, Ottawa, Canada, 2003.

14. CNSC, G-129, rev. 1, *Keeping Radiation Exposures and Doses "As Low as Reasonably Achievable (ALARA)*", Ottawa, Canada, 2004.

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

16. CNSC, RD/GD-210, *Maintenance Programs for Nuclear Power Plants*, Ottawa, Canada, 2012.

17. CNSC, P-290, *Managing Radioactive Waste*, Ottawa, Canada, 2004.

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

19. CNSC, RD-363, *Nuclear Security Officer Medical, Physical, and Psychological Fitness*, Ottawa, Canada, 2008

20. CNSC, REGDOC-2.4.2, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*, Ottawa, Canada, 2014.

21. CNSC, P-119, *Policy on Human Factors*, Ottawa, Canada, 2000.

22. CNSC, P-223, *Protection of the Environment*, Ottawa, Canada, 2001.

23. CNSC, RD/GD-98, *Reliability Programs for Nuclear Power Plants*, Ottawa, Canada, 2012.

24. CNSC, REGDOC-2.4.1, *Deterministic Safety Analysis*, Ottawa, Canada, 2014.

25. CNSC, G-274, *Security Programs for Category I or II Nuclear Material or Certain Nuclear Facilities*, Ottawa, Canada, 2003.

26. CNSC, REGDOC-2.3.2, *Accident Management: Severe Accident Management Programs for Nuclear Reactors*, Ottawa, Canada, 2013.

27. CNSC, RD-346, *Site Evaluation for New Nuclear Power Plants*, Ottawa, Canada, 2008.

28. CNSC, G-208, *Transportation Security Plans for Category I, II or III Nuclear Material*, Ottawa, Canada, 2003.

29. CNSC, G-144, *Trip Parameter Acceptance Criteria for the Safety Analysis of CANDU Nuclear Power Plants*, Ottawa, Canada, 2006.

Additional Information

The CNSC may recommend additional information on best practices and standards such as those published by CSA Group. With the permission of the publisher, CSA Group, all nuclear-related CSA standards may be viewed at no cost through the CNSC webpage "How to gain free access to all nuclear-related CSA standards."

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

CSA Group

1. CSA Group, N287 series on concrete containment structures.
2. CSA Group, N294, *Decommissioning of facilities containing nuclear substances*, Toronto, Canada.
3. CSA Group, A23.3, *Design of Concrete Structures*, Toronto, Canada.
4. CSA Group, S16, *Design of Steel Structures*, Toronto, Canada.
5. CSA Group, N290.13, *Environmental Qualification of Equipment for CANDU Nuclear Power Plants*, Toronto, Canada.
6. CSA Group, N285.0/N285.6 Series, *General requirements for pressure-retaining systems and components in CANDU nuclear power plants/Material Standards for reactor components for CANDU nuclear power plants*, Toronto, Canada.
7. CSA Group, N286.7.1, *Guideline for the application of N286.7-99, Quality assurance of analytical, scientific, and design computer programs for nuclear power plants*, Toronto, Canada.
8. CSA Group, N288.2, *Guidelines for Calculating Radiation Doses to the Public from a Release of Airborne Radioactive Material under Hypothetical Accident Conditions in Nuclear Reactors*, Toronto, Canada.
9. CSA Group, N288.4, *Environmental monitoring programs at Class I nuclear facilities and uranium mines and mills*, Toronto, Canada.
10. CSA Group, N293, *Fire protection for nuclear power plants*, Toronto, Canada.
11. CSA Group, N290.0/N290.3 PACKAGE, *General requirements for safety systems of nuclear power plants* and *Requirements for the containment system of nuclear power plants*, Toronto, Canada.
12. CSA Group, N292.3, *Management of Low and Intermediate-level Radioactive Waste*, Toronto, Canada.
13. CSA Group, N286, *Management system requirements for nuclear power plants*, Toronto, Canada.

14. CSA Group, N285.4, *Periodic inspection of CANDU nuclear power plant components*, Toronto, Canada.

15. CSA Group, N285.5, *Periodic inspection of CANDU nuclear power plant components*, Toronto, Canada.

16. CSA Group, N290.14, *Qualification of Pre-developed Software for Use in Safety Related Instrumentation and Control Applications in Nuclear Power Plants*, Toronto, Canada.

17. CSA Group, N286.7, *Quality Assurance of Analytical, Scientific, and Design Computer Programs for Nuclear Power Plants*, Toronto, Canada.

18. CSA Group, N290.1, *Requirements for the Shutdown Systems of CANDU Nuclear Power Plants*, Toronto, Canada.

19. CSA Group, N290.4, *Requirements for reactor control systems of nuclear power plants*, Toronto, Canada, 2011.

20. CSA Group, N290.5, *Requirements for Electrical Power and Instrument Air Systems of CANDU Nuclear Power Plants*, Toronto, Canada.

21. CSA Group, N290.6, *Requirements for monitoring and display of nuclear power plant safety functions in the event of an accident*, Toronto, Canada.

22. CSA Group, N290.15, *Requirements for the safe operating envelope of nuclear power plants*, Toronto, Canada.

23. CSA Group, N291, *Requirements for Safety-Related Structures for CANDU Nuclear Power Plants*, Toronto, Canada.

24. CSA Group, N289 series on seismic design and qualification of nuclear power plants.

International Atomic Energy Agency

1. International Atomic Energy Association (IAEA), Safety Series No. 50-P-1, Application of the Single Failure Criterion, Vienna, 1990.

2. IAEA, Safety Reports Series No. 46, Assessment of Defence in Depth for Nuclear Power Plants, Vienna, 2005.

3. IAEA, NS-G-2.9, Commissioning for Nuclear Power Plants, Vienna, 2003.

4. IAEA, Nuclear Security Series No. 17, Computer Security at Nuclear Facilities, Vienna, 2011.

5. IAEA, NS-G-2.5, Core Management and Fuel Handling for Nuclear Power Plants, Vienna, 2002.

6. IAEA, WS-G-2.1, Decommissioning of Nuclear Power Plants and Research Reactors Safety Guide, Vienna, 1999.

7. IAEA, INSAG-10, Defence in Depth in Nuclear Safety, Vienna, 1996.

8. IAEA, NS-G-1.8, Design of Emergency Power Systems of Nuclear Power Plants, Vienna, 2004.

9. IAEA, NS-G-1.4, Design of Fuel Handling and Storage Systems in Nuclear Power Plants Safety Guide, Vienna, 2003.

10. IAEA, TECDOC-1657, Design Lessons Drawn from the Decommissioning of Nuclear Facilities, Vienna, 2011.

11. IAEA, NS-G-1.10, Design of Reactor Containment Systems for Nuclear Power Plants, Vienna, 2004.

12. IAEA, NS-G-1.9, Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants, Vienna, 2004.

13. IAEA, NS-G-1.12, Design of the Reactor Core for Nuclear Power Plants, Vienna, 2005.

14. IAEA, SSG-2, Deterministic Safety Analysis for Nuclear Power Plants, Vienna, 2009.

15. SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 2010.

16. IAEA, SSG-4, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 2010.

17. IAEA, Safety Reports Series No. 3, Equipment Qualification in Operational Nuclear Power Plants: Upgrading, Preserving and Reviewing, Vienna, 1998.

18. IAEA, NS-G-1.5, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Vienna, 2003.

19. IAEA, NS-G-3.1, External Human Induced Events in Site Evaluation for Nuclear Power Plants, Vienna, 2002.

20. IAEA, NS-G-3.3, Evaluation of Seismic Hazards for Nuclear Power Plants, Vienna, 2002.

21. IAEA, NS-G-2.1, Fire Safety in Operation of Nuclear Power Plants, Vienna, 2000.

22. IAEA, NS-G-3.5, Flood Hazard for Nuclear Power Plants on Coastal and River Sites, Vienna, 2003.

23. IAEA, TECDOC-967, Rev.1, Guidance and Considerations for the Implementation of INFCIRC/225/Rev.4, The Physical Protection of Nuclear Material and Nuclear Facilities, Vienna, 2002.

24. IAEA, TECDOC-1276, Handbook on the Physical Protection of Nuclear Materials and Facilities, Vienna, 2002.

25. IAEA, Safety Series No. 50-P-10, Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 1995.

26. IAEA, NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, Vienna, 2002.

27. IAEA, INSAG-19, Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life, Vienna, 2003.

28. IAEA, NS-G-2.6, Maintenance, Surveillance and In-Service Inspection in Nuclear Power Plants, Vienna, 2002.

29. IAEA, GS-R-3, The Management System for Facilities and Activities, Vienna, 2006.

30. IAEA, GS-G-3.5, The Management System for Nuclear Installations, Vienna, 2009.

31. IAEA, GS-G-3.3, The Management System for the Processing, Handling and Storage of Radioactive Waste Safety Guide, Vienna, 2008.

32. IAEA, NS-G-3.4, Meteorological Events in Site Evaluation for Nuclear Power Plants, Vienna, 2003.

33. IAEA, SSG-18, Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations, Vienna, 2011.

34. IAEA, INFCIRC-225, Rev.5, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, Vienna, 2011.

35. IAEA, RS-G-1.1, Occupational Radiation Protection, Vienna, 1999.

36. IAEA, NS-G-2.2, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, Vienna, 2000.

37. IAEA, Safety Report Series No. 8, Preparation of Fire Hazard Analysis for Nuclear Power Plants, Vienna, 1998.

38. IAEA, GS-R-2, Preparedness and Response for a Nuclear or Radiological Emergency, Vienna, 2002.

39. IAEA, NS-G-1.7, Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants, Vienna, 2004.

40. IAEA, NS-G-1.11, Protection Against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, Vienna, 2004.

41. IAEA, NS-G-1.13, Radiation Protection Aspects of Design for Nuclear Power Plants, Vienna, 2005.

42. IAEA, Safety Reports Series No. 25, Review of Probabilistic Safety Assessments by Regulatory Bodies, Vienna, 2002.

43. IAEA, NS-G-1.2, Safety Assessment and Verification for Nuclear Power Plants, Vienna, 2001.

44. IAEA, General Safety Requirements Part 4, Safety Assessment for Facilities and Activities, Vienna, 2009.

45. IAEA, Safety Series No. 110, The Safety of Nuclear Installations, Vienna, 1993.

46. IAEA, SSR 2/2, Safety of Nuclear Power Plants: Commissioning and Operation, Vienna, 2011.

47. IAEA, SSR 2/1, Safety of Nuclear Power Plants: Design, Vienna, 2012 (revision of NS-R-1).

48. IAEA, NS-G-1.6, Seismic Design and Qualification for Nuclear Power Plants, Vienna, 2003.

49. IAEA, SSG-9, Seismic Hazards in Site Evaluation for Nuclear Installations, Vienna, 2010.

50. IAEA, NS-G-2.15, Severe Accident Management Programmes for Nuclear Power Plants, Vienna, 2009.

51. IAEA, NS-G-1.1, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, Vienna, 2000.

52. IAEA, NS-G-2.11, A System for the Feedback of Experience from Events in Nuclear Installations, Vienna, 2006.

53. IAEA, Safety Series No. 50-P-7, Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants, Vienna, 1995.

United States Nuclear Regulatory Commission

1. United States Nuclear Regulatory Commission (U.S. NRC), NUREG-6684, Advanced Alarm Systems: Revision of Guidance and Its Technical Basis, Washington, D.C., 2000.

2. U.S. NRC, NUREG/CR-6633, Advanced Information Systems Design: Technical Basis and Human Factors Review Guidelines, Washington, D.C., 2000.

3. NUREG/CR-6486, Assessment of Modular Construction for Safety-Related Structures at Advanced Nuclear Power Plants, Washington, D.C., 1997.

4. U.S. NRC, Regulatory Guide 1.77, Assumptions Used for Evaluating a Control Rod Ejection Accident for Pressurized Water Reactors, Washington, D.C., 1974.

5. U.S. NRC, Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, Washington, D.C., 2010.

6. U.S. NRC, NUREG 1852, Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire, Washington, D.C., 2007.

7. U.S. NRC, Regulatory Guide 1.76, Design Basis Tornado and Tornado Missiles for Nuclear Power Plants, Washington, D.C., 2007.

8. U.S. NRC, Regulatory Guide 1.57, Design Limits and Loading Combinations for Metal Primary Reactor Containment System Components, Washington, D.C., 2007.

9. U.S. NRC, NUREG/CR-7007, Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, Washington, D.C., 2010.

10. U.S. NRC, Regulatory Guide 1.91, Evaluations of Explosions Postulated to occur on Transportation Routes near Nuclear Power Plants, Washington, D.C., 1978.

11. U.S. NRC, NUREG/CR-6850, EPRI 1011989, Fire Probabilistic Risk Assessment Methods Enhancements, Washington, D.C., 2010.

12. U.S. NRC, Regulatory Guide 1.189, Fire Protection for Operating Nuclear Power Plants, Washington, D.C., 2009.

13. U.S. NRC, NUREG-0696, Functional Criteria for Emergency Response Facilities, Washington, D.C., 1981.

14. 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, Washington, D.C., 2007.

15. U.S. NRC, NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications-Final Report, Washington, D.C., 2011.

16. U.S. NRC, NUREG-0711 Rev.2, Human Factors Engineering Program Review Model, Washington, D.C., 2004.

17. U.S. NRC, NUREG-0700 Rev.2, Human-System Interface Design Review Guidelines, Washington, D.C., 2002.

18. U.S. NRC, NUREG-6393, Integrated System Validation: Methodology and Review Criteria, Washington, D.C., 1997.

19. U.S. NRC, NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, Washington, D.C., 1994.

20. U.S. NRC, 10 CFR Part 50, Appendix B, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants, Washington, D.C., 2007.

21. U.S. NRC, NUREG-0800, section 3.8.1, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Concrete Containment, Washington, D.C., 2007.

22. U.S. NRC, 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, Washington, D.C., 2010.

23. U.S. NRC, NUREG-0800, chapter 8, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Electric Power, Washington, D.C., 2007.

24. U.S. NRC, 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, Washington, D.C., 2007.

25. U.S. NRC, 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, Washington, D.C., 2009.

26. U.S. NRC, NUREG-0800, chapter 18, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants – Human Factors Engineering, Washington, D.C., 2007.

27. U.S. NRC, 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, Washington, D.C., 2007.

28. U.S. NRC, 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, Washington, D.C., 2010.

29. 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, Washington, D.C., 2007.

30. U.S. NRC, 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, Washington, D.C., 2007.

31. U.S. NRC, Regulatory Guide 1.203, Transient and Accident Analysis Methods, Washington, D.C., 2005.

Other

1. American Concrete Institute, 349-06, Code Requirements for Nuclear Safety-Related Concrete Structures and Commentary, Farmington Hills, Michigan, 2007.

2. American National Standards Institute (ANSI)/American Nuclear Society (ANS), 57.1, American National Standard Design Requirements for Light Water Reactor Fuel Handling System, La Grange Park, Illinois, 1992.

3. ANSI/ANS, 57.5, Light Water Reactor Fuel Assembly Mechanical Design and Evaluation, La Grange Park, Illinois, 1996.

4. ANSI/ANS, 58.8-1994, Time Response Design Criteria for Safety-Related Operator Actions, La Grange Park, Illinois, reaffirmed 2008.

5. ANS, 2.26, Categorization of Nuclear Facility Structures, Systems, and Components for Seismic Design, La Grange Park, Illinois, reaffirmed 2010.

6. ANS, 2.3, Estimating Tornado, Hurricane, and Extreme Straight Line Wind Characteristics at Nuclear Facility Sites, La Grange Park, Illinois, 2011.

7. American Society of Civil Engineers (ASCE), Design of Blast-Resistant Buildings in Petrochemical Facilities, Reston, Virginia, 2010.

8. ASCE, 58, ASCE Manual Reports on Engineering Practice, Structural Analysis and Design of Nuclear Plant Facilities, Structural Analysis and Design of Nuclear Plant Facilities, Reston, Virginia, 1980.

9. ASCE, 04-98, Seismic Analysis for Safety-Related Nuclear Structures, Reston, Virginia, 2000.

10. ASCE/Structural Engineering Institute, 43-05, Seismic Design Criteria for Structures, Systems and Components in Nuclear Facilities, Reston, Virginia, 2005.

11. American Society of Mechanical Engineers (ASME), ASME Boiler and Pressure Vessel Code, New York, 2010.

12. ASME, QME-1-2002, Qualification of Active Mechanical Equipment Used in Nuclear Power Plants, New York, 2002.

13. ASME, NQA-1-2008, Quality Assurance Requirements for Nuclear Facility Applications, New York, 2008.

14. ASME, ASME/ANS RA-Sa-2009, Standard for Level 1/Large Early Release Frequency PRA for Nuclear Power Plant Applications, New York, 2009.

15. Communications Security Establishment, TRA-1, Harmonized Threat and Risk Assessment (TRA) Methodology, Ottawa, Canada, 2007.

16. Electric Power Research Institute (EPRI), TR-103959, Methodology for Developing Seismic Fragilities, Palto Alto, California, 1994.

17. EPRI, Technical Report, Rev.1, Nuclear Power Plant Equipment Qualification Reference Manual, Palto Alto, California, 2010.

18. European Standard, EN 15129, Anti-seismic Devices, European Committee for Standardization, Brussels, 2009.

19. European Standard, EN 1337-3, Structural Bearings – Elastomeric Bearings, European Committee for Standardization, Brussels, 2000.

20. European Standard, EN 1337-1, Structural Bearings – General Design Rules, European Committee for Standardization, Brussels, 2000.

21. International Electrotechnical Commission (IEC), 60964, Nuclear Power Plants - Control Rooms – Design, Geneva, 2009

22. IEC, 60965, Nuclear Power Plants - Control Rooms - Supplementary Control Points for Reactor Shutdown Without Access to the Main Control Room, Geneva, 2009.

23. IEC, 61839, Nuclear Power Plants – Design of Control Rooms – Functional Analysis and Assessment, Geneva, 2000.

24. IEC, 60780, Ed. 2.0, Nuclear Power Plants - Electrical Equipment of the Safety System – Qualification, Geneva, 1998.

25. IEC, 61226, Ed. 3.0, Nuclear Power Plants – Instrumentation and Control Important to Safety – Classification of Instrumentation and Control Functions, Geneva, 2009.

26. IEC, 61513, Nuclear Power Plants – Instrumentation and Control Important to Safety, Gener*al Requirements for Systems*, Geneva, 2011.

27. IEC, 60987, Nuclear Power Plants – Instrumentation and Control Important to Safety – Hardware Design Requirements for Computer-Based Systems, Geneva, 2007.

28. IEC, 62385, Nuclear Power Plants – Instrumentation and Control Important to Safety – Methods for Assessing the Performance of Safety System Instrument Channels, Geneva, 2007.

29. IEC, 60880, Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems Performing Category A Functions, Geneva, 2006.

30. IEC, 62138, Ed. 1.0, Nuclear Power Plants – Instrumentation and Control Important for Safety – Software Aspects for Computer-Based Systems Performing Category B or C Functions, Geneva, 2004.

31. IEC, 60671, Nuclear Power Plants – Instrumentation and Control Systems Important Safety – Surveillance Testing, Geneva, 2007.

32. Institute of Electrical and Electronics Engineers (IEEE), 379-1988, Application of the Single- Failure Criterion to Nuclear Power Generating Station Safety Systems, Piscataway, New Jersey, 1988.

33. IEEE, C62.23-1995, IEEE Application Guide for Surge Protection of Electric Generating Plants, Piscataway, New Jersey, 1995.

34. 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, Piscataway, New Jersey, 1998.

35. IEEE, 1023, IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations, Piscataway, New Jersey, 2004.

36. IEEE,1050-1996, Guide for Instrumentation and Control Equipment Grounding in Generating Stations, Piscataway, New Jersey, 1996.

37. IEEE, 141, IEEE Recommended Practice for Electric Power Distribution for Industrial Plants, Piscataway, New Jersey, 1993.

38. IEEE, 242, IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems, Piscataway, New Jersey, 2001.

39. IEEE, 344, IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, Piscataway, New Jersey, 2004.

40. IEEE, 497, IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations, Piscataway, New Jersey, 2010.

41. IEEE, 308 IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations, Piscataway, New Jersey, 2001.

42. IEEE, 7-4.3.2, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, Piscataway, New Jersey, 2010.

43. IEEE, 279, IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations, Piscataway, New Jersey, 1971.

44. IEEE, 665-1995, IEEE Standard for Generating Station Grounding, Piscataway, New Jersey, reaffirmed 2001.

45. IEEE, 627, IEEE Standard for Qualification of Equipment Used in Nuclear Facilities, Piscataway, New Jersey, 2010.

46. IEEE, 323, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, Piscataway, New Jersey, 2003.

47. IEEE, 387, IEEE Standard Criteria for Diesel-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations, Piscataway, New Jersey, 1995.

48. IEEE, 603, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, Piscataway, New Jersey, 2009.

49. International Organization for Standardization (ISO), ISO 9001:2008, Quality Management Systems – Requirements, Geneva, 2008.

50. Nuclear Energy Agency (NEA), No.6924, Applying Decommissioning Experience to the Design and Operation of New Nuclear Power Plants, Organization for Economic Cooperation and Development: Paris, 2010.

51. NEA, No.6833, Decommissioning Considerations for New Nuclear Power Plants,

52. Organization for Economic Cooperation and Development: Paris, 2010.

53. Nuclear Energy Institute (NEI), NEI 08-09 Rev.6, Cyber Security Plan for Nuclear Power Reactors, Washington, D.C., 2010.

54. NEI, 00-01, Guidance for Post Fire Safe Shutdown Circuit Analysis, Washington, D.C., 2005.

55. NEI, 99-03, Rev.0, Control Room Habitability Assessment Guidance, Washington, D.C., 2001.

56. NEI, 04-02, Rev. 1, Guidance for Implementing a Risk-Informed, Performance-Based Fire Protection Program under 10 CFR 50.48(c), Washington, D.C., 2005.

57. NEI, 07-13, Methodology for Performing Aircraft Impact Assessments for New Plant Designs, Washington, D.C., 2011.

58. National Fire Protection Association (NFPA), Fire Protection Handbook, Quincy, Massachusetts, 2008.

59. NFPA, 805, Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants, Quincy, Massachusetts, 2010.

60. NFPA, 804, Standard for Fire Protection for Advanced Light Water Reactor Electric Generating Plants, Quincy, Massachusetts, 2010.

61. Nuclear Information and Records Management Association/ANSI, 1.0, Standard Configuration Management, Washington, D.C., 2007.

62. National Research Council (NRC), National Building Code of Canada, Ottawa, Canada, 2010.

63. NRC, National Fire Code of Canada, Ottawa, Canada, 2010.

64. Society of Fire Protection Engineers, Society of Fire Protection Engineers Handbook of Fire Protection Engineering, Bethesda, Maryland, 2008.

65. Unified Facilities Criteria, 3-340-02, Structures to Resist the Effects of Accidental Explosions, Washington, D.C., 2008.

66. United Kingdom Atomic Energy Authority, Guidelines for the Design and Assessment of Concrete Structures Subjected to Impact, Oxfordshire, United Kingdom, 1990.

CNSC Regulatory Document Series

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

CNSC regulatory documents are classified under the following categories and series:

1.0 Regulated facilities and activities

Series 1.1 Reactor facilities
1.2 Class IB facilities
1.3 Uranium mines and mills
1.4 Class II facilities
1.5 Certification of prescribed equipment
1.6 Nuclear substances and radiation devices

2.0 Safety and control areas

Series 2.1 Management system
2.2 Human performance management
2.3 Operating performance
2.4 Safety analysis
2.5 Physical design
2.6 Fitness for service
2.7 Radiation protection
2.8 Conventional health and safety
2.9 Environmental protection
2.10 Emergency management and fire protection
2.11 Waste management
2.12 Security
2.13 Safeguards and non-proliferation
2.14 Packaging and transport

3.0 Other regulatory areas

Series 3.1 Reporting requirements
3.2 Public and Indigenous engagement
3.3 Financial guarantees
3.4 Commission proceedings
3.5 CNSC processes and practices
3.6 Glossary of CNSC terminology

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