Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

DRAFT
Regulatory
Document

RD–337

Design of New Nuclear Power Plants

Issued for Internal Review and External Stakeholder Consultation
October 2007

Draft release date: 18/10/07

Canada

CNSC REGULATORY DOCUMENTS

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

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

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

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

Draft Regulatory Document

RD–337

DESIGN OF NEW NUCLEAR POWER PLANTS

October 2007

About this Document

This draft regulatory document sets out the expectations of the Canadian Nuclear Safety Commission (CNSC) with respect to the design of new nuclear power plants. Given the importance and complexity of the subject matter, CNSC staff will hold an information session in the upcoming weeks to help our stakeholders better understand this document. Further details about this information session will be posted on the CNSC's Web site at www.nuclearsafety.gc.ca.

Comments

The CNSC invites interested persons to submit comments on this draft regulatory document by 14 January 2008.

Comments can be submitted electronically to consultation@cnsc-ccsn.gc.ca. To communicate in writing, please contact us at the postal address below.

Please note that any comments submitted, including names and affiliations, may be made public.

Document availability

This document is available in English or French on the CNSC Web site at www.nuclearsafety.gc.ca. To order a paper copy of the document in either official language, please contact:

Canadian Nuclear Safety Commission
Regulatory Framework Division
P.O. Box 1046, Station B
280 Slater Street
Ottawa, Ontario, CANADA, K1P 5S9
E-mail: consultation@cnsc-ccsn.gc.ca

Draft Regulatory Document

RD–337

DESIGN OF NEW NUCLEAR POWER PLANTS

Issued for Internal Review and
External Stakeholder Consultation by the
Canadian Nuclear Safety Commission
October 2007

TABLE OF CONTENTS

DESIGN OF NEW NUCLEAR POWER PLANTS

1.0 PURPOSE

The purpose of this regulatory document is to set out the expectations of the Canadian Nuclear Safety Commission (CNSC) with respect to the design of new nuclear power plants (NPPs).

2.0 SCOPE

This document sets out the criteria against which the CNSC will review new NPP designs, taking into account all design aspects of the NPP, promoting multiple levels of defence in the design, and ensuring adherence to high standards and consistency with modern international codes and standards. To the extent practicable, the criterion presented herein is technology neutral.

This document establishes:

1. Safety goals and objectives for the design;
2. Design principles to be utilized;
3. Requirements for the management of the design;
4. Design requirements for systems, structures, and components;
5. High level requirements for environmental protection, radiation protection, ageing, human factors, security, safeguards, transportation, accident and emergency response planning; and
6. Requirements for integrating safety analysis into the design.

3.0 RELEVANT LEGISLATION

The CNSC is the federal agency that regulates the use of nuclear energy and materials in Canada to protect health, safety, security, and the environment, and to respect Canada's international commitments on the peaceful use of nuclear energy. The *Nuclear Safety and Control Act* (NSCA) requires persons or organizations to be licensed by the CNSC for carrying out the activities referred to in Section 26 of the NSCA, unless otherwise exempted. The associated regulations stipulate prerequisites for CNSC licensing and the obligations of licensees.

The provisions of the NSCA and regulations that are relevant to this regulatory document include:

1. Subsection 24(4) of the NSCA prohibits the Commission from issuing, renewing, amending or replacing a licence, unless in the opinion of the Commission, the applicant is (*a*) qualified to carry on the activity that the licence authorize the licensee to carry on, and (*b*), in carrying out that activity, make adequate provision for the protection of the environment, the health and safety of persons and the maintenance of national security and measures required to implement international obligations to which Canada has agreed;
2. Subsection 24(5) of the NSCA authorizes the Commission to include in a licence any term or condition that the Commission considers necessary for the purposes of the NSCA.
3. Paragraph 3(1)(*i*) of the *General Nuclear Safety and Control Regulations* stipulates that an application for a licence shall contain, in addition to other information, "a description and the results of any test, analysis or calculation performed to substantiate the information included in the application";
4. Paragraph 5(*i*) of the *Class I Nuclear Facilities Regulations* stipulates that an application for a licence to construct a Class I nuclear facility shall contain, in addition to other information, information on "the effects on the environment and the health and safety of persons that may result from the construction, operation and decommissioning of the nuclear facility..";
5. Paragraph 6(*h*) of the *Class I Nuclear Facilities Regulations* stipulates that an application for a licence to operate a Class I nuclear facility shall contain, in addition to other information, information on "the effects on the environment and the health and safety of persons that may result from the operation and decommissioning of the nuclear facility…";
6. Paragraph 7(*f*) of the *Class I Nuclear Facilities Regulations* stipulates that an application for a licence to decommission a Class I nuclear facility shall contain, in addition to other information, information on "the effects on the environment and the health and safety of persons that may result from the decommissioning of the nuclear facility; and
7. Relevant sections of the *Nuclear Security Regulations* and *General Nuclear Safety and Control Regulations* that may pertain to the design of a nuclear power plant.

4.0 SAFETY OBJECTIVES AND CONCEPTS

4.1 General Nuclear Safety Objective

As established by the International Atomic Energy Agency (IAEA), nuclear power plants shall be designed and operated so as to protect individuals, society and the environment from harm by establishing and maintaining in nuclear installations effective defences against radiological hazards.

This general nuclear safety objective is supported by two complementary safety objectives dealing with radiation protection and technical aspects. The technical objective is interdependent with administrative and procedural measures to ensure defence against hazards due to ionizing radiation.

4.1.1 Radiation Protection Objective

The radiation protection objective of the design shall provide that, in all operational states, radiation exposures within the NPP or due to any planned release of radioactive material from the NPP are kept below prescribed limits and as low as reasonably achievable (ALARA). The design shall provide for the mitigation of the radiological consequences of any accidents.

4.1.2 Technical Safety Objective

The technical safety objective of the NPP design shall provide for all practicable measures to prevent accidents in the NPP and to mitigate their consequences should they occur. It takes into account all possible accidents, including those of very low probability. Any radiological consequences would be minor and below prescribed limits and the likelihood of accidents with serious radiological consequences shall be extremely low.

4.2 Safety Analysis

To demonstrate that the safety objectives are met in the design of a nuclear power plant, a comprehensive safety analysis is carried out to identify all sources of exposure and to evaluate radiation doses that could be received by workers at the plant and by the public, as well as potential effects on the environment. The safety analysis examines:

1. All planned normal operational modes of the plant,
2. Plant performance in anticipated operational occurrences (AOOs),
3. Design basis accidents (DBAs), and
4. Beyond design basis accidents (BDBAs), including event sequences that may lead to a severe accident.

On the basis of this analysis, the capability of the design to withstand postulated initiating events and accidents can be established, the effectiveness of the items important to safety can be demonstrated, and requirements for emergency response can be established. The results of the safety analysis are fed back to the design.

4.3 Accident Mitigation and Management

Although measures are taken to control radiation exposure in operational states 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, there is a residual probability that an accident may happen. Measures are therefore taken to ensure that the radiological consequences are mitigated. Such measures include:

1. Engineered safety features;
2. On-site accident management procedures established by the operating organization; and
3. Off-site intervention measures established by appropriate authorities in order to mitigate radiation exposure if an accident has occurred.

The design shall apply the principle that plant states that could result in high radiation doses or radioactive releases are of very low probability of occurrence, and plant states with significant probability of occurrence have only minor or no potential radiological consequences.

4.4 Safety Goals

The NSCA and the safety objectives defined above provide the basis for dose acceptance criteria and safety goals.

4.4.1 Dose Acceptance Criteria

The following table indicates dose acceptance criteria for operational states and DBAs:

Dose Acceptance Criteria

AOOs	DBAs
0.5 mSv	20.0 mSv

4.4.2 Qualitative Safety Goals

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

1. Individual members of the public shall be provided a level of protection from the consequences of nuclear power plant operation such that there is no significant additional risk to the life and health of individuals; and
2. Societal risks to life and health from nuclear power plant operation shall be comparable to or less than the risks of generating electricity by viable competing technologies, and should not be a significant addition to other societal risks.

4.4.3 Quantitative Application of the Safety Goals

For practical application, quantitative safety goals are established to achieve the same intent as the qualitative safety goals. The quantitative safety goals include three frequency types:

1. Small release frequency (SRF);
2. Large release frequency (LRF); and
3. Core damage frequency.

4.4.3.1 Small Release Frequency (SRF)

The sum of frequencies of all event sequences that can lead to release to the environment of more than 10^{15} Bq of I_{131} should be less than 10^{-6} per plant year and shall not exceed 10^{-5} per plant year.

4.4.3.2 Large Release Frequency (LRF)

The sum of frequencies of all events sequences that can lead to release to the environment of more than 10^{14} Bq of Cs_{137} should be less than 10^{-7} per plant year and shall not exceed 10^{-6} per plant year.

4.4.3.3 Core Damage Frequency (CDF)

The sum of frequencies of all events sequences that can lead to significant core degradation should be less than 10^{-6} per plant year and shall not exceed 10^{-5} per plant year.

4.5 Safety Concepts

4.5.1 Defence-in-Depth

The concept of defence-in-depth is applied to all organizational, behavioural, and design related safety activities to ensure that they are subject to overlapping provisions, so that if a failure were to occur, it would be detected and compensated for, or corrected.

This concept is applied throughout the design of the NPP to provide a series of levels of defence aimed at preventing accidents, and ensuring appropriate protection in the event that prevention fails.

All levels of defence shall be available at all times, although some relaxations may be specified for the various operational modes other than power operation. The levels of defence are summarized in the following table.

Table 4.1—Levels of Defence in Depth

Level	Objective	Essential Means
1	Prevention of abnormal operation and of failures	Conservative design and high quality in construction and operation (e.g. for process system)
2	Control of abnormal operation and detection of failures	Control systems, and other surveillance features
3	Minimizing the consequences of accidents	Engineered safety features (e.g., safety systems) and emergency procedures
4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management (e.g. safety systems and mitigating systems)
5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

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

The plant shall be designed, constructed, maintained, and operated in accordance with appropriate quality levels and engineering practices, and application of the principles of redundancy, independence, separation and diversity. In the design, careful attention shall be paid to the selection of appropriate design codes and materials, to the procedures applied in the design, to equipment qualification, to safety analysis, and to the use of operational experience.

The aim of the second level of defence is to detect and respond to deviations from normal operational states in order to prevent failures of SSCs from escalating to accident conditions, and to return the plant to a state of normal operation.

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

The aim of the fourth level of defence is to control severe plant conditions, prevent accident progression, and mitigate the consequences of severe accidents to ensure that radioactive releases are kept as low as reasonably achievable. Most importantly, the plant design shall provide adequate protection of the confinement function. This protection may be achieved by a robust containment design, by complementary measures and procedures to prevent accident progression, and by accident management procedures.

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. This requires the provision of an adequately equipped emergency support centre, and plans for the on-site and off-site emergency response.

In keeping with the concept of defence-in-depth, the design shall describe structures, systems, and components (SSCs) for:

1. Process systems;
2. Control systems associated with the process systems;
3. Safety systems for coping with design basis accidents; and
4. Complementary design features for mitigating the consequences of beyond design basis accidents and severe accidents.

In addition, common support services such as electrical power, cooling water, and instrument air, shall be provided for these systems.

Consideration of Physical Barriers

An important aspect of the implementation of defence-in-depth is the provision in the design of a series of physical barriers to confine the radioactive material at specified locations. Such barriers may include the fuel matrix, the fuel cladding, the reactor coolant pressure boundary, the containment, and the exclusion zone.

4.5.2 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 can be controlled by the operator.

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

Safe operation depends upon personnel as well as on equipment. The OLCs shall therefore include:

1. Control system constraints and procedural constraints on important process variables;
2. Requirements for different operational states, including shutdowns;
3. Actions to be taken and limitations to be observed by operating personnel;
4. Principal requirements for surveillance and corrective or complementary actions; and

5. The limitations to be observed and the operational requirements that SSCs must be able to meet in order to perform their intended functions as assumed in the plant safety analysis report.

The basis on which the OLCs are derived shall be either included in the documentation, or available locally, to increase consciousness on the part of plant personnel of their application and observance.

5.0 SAFETY MANAGEMENT DURING DESIGN

5.1 General

The nuclear power plant design shall:

1. Meet Canadian regulatory requirements;
2. Be in accordance with the design specifications and confirmed by safety analysis;
3. Take account of current safety practices;
4. Fulfil the requirements of an effective quality assurance program; and
5. Incorporate only those design changes that have been properly considered;

The design shall be performed by technically qualified and appropriately trained staff at all levels, and with:

1. A clear division of responsibilities with corresponding lines of authority and communication;
2. Clear interfaces established between the groups engaged in different parts of the design, and between designers, utilities, suppliers, constructors, and contractors as appropriate;
3. Procedures that align with an established quality assurance program; and
4. A positive safety culture throughout all levels of the organization.

5.2 Design Authority

During the design phase, formal design authority typically lies with the organization that has overall responsibility for the design. Prior to plant start-up, this authority may 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 design authority shall retain overall responsibility.

The applicant shall ensure that during the development of the design, the design authority has:

1. Established a knowledge base of all relevant aspects of the plant design and maintained it up-to-date, while taking due account of experience and research findings;
2. Ensured that the knowledge of the design that is needed for the safe operation and maintenance of a plant is available;
3. Maintained design configuration control;
4. Reviewed, verified, approved (or rejected) and documented design changes to the plant;
5. Established and controlled the necessary interfaces with responsible designers or other suppliers engaged in design work;
6. Ensured that the necessary engineering and scientific skills and knowledge have been maintained, either by the design authority or by responsible designers or other sources (including any research programs that are needed to keep the knowledge up-to-date);
7. Ensured that the safety impact of individual design changes, or multiple changes that may have significant interdependencies, have been properly assessed and understood; and

5.3 Design Management

Design management shall ensure that:

1. SSCs important to safety meet the respective requirements;
2. Due account is taken of the human capabilities and limitations of personnel;
3. Adequate safety design information necessary for safe operation and maintenance of the plant and any subsequent plant modifications is preserved;
4. Operational limits and conditions for incorporation into the plant administrative and operational procedures are provided;
5. The plant is designed to facilitate maintenance throughout the life of the plant;
6. Account is taken of the results of the deterministic and probabilistic safety assessments;
7. Due consideration is given to the prevention of accidents and mitigation of their consequences;
8. The generation of radioactive waste is limited to minimum practicable levels, in terms of both activity and volume.

5.4 Proven Engineering Practices

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

If the identified standards and codes are found to be insufficient to ensure that SSC quality corresponds to the importance of the respective safety function to be performed, then they shall be supplemented or modified as necessary.

SSCs important to safety shall then be designed according to the standards and codes established for the design. These SSCs shall be of proven designs.

Where a new design, feature or engineering practice is introduced, adequate safety shall be proven by a combination of supporting research and development programs and examination of relevant experience from similar applications.

New designs shall be tested before being brought into service, and shall be monitored in service to verify that the expected behaviour is achieved. An adequate qualification program shall be established to verify that the new design meets all applicable safety requirements.

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

5.5 Operational Experience and Safety Research

The design shall take into account the operational experience that has been gained in the nuclear industry, and the results of relevant research programs.

5.5.1 Safety Assessment

Safety assessment is a systematic process that is carried out throughout the design process to ensure that all the relevant safety requirements are met by the proposed (or actual) design of the plant. This includes the requirements set by the operating organization and the regulators. The basis for the safety assessment shall be data derived from the safety analysis, previous operational experience, results of supporting research and proven engineering practice

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

The operating organization shall ensure that an independent peer review of the safety assessment is performed by individuals or groups separate from those carrying out the design, before the design is submitted to the regulatory body.

The safety assessment documentation shall be made readily accessible, and shall be clear, concise, and presented in a logical and understandable format.

The safety assessment documentation shall identify the important aspects of operation, maintenance, and management required for safety, and shall be maintained in a living suite of documents to reflect changes in design as the plant evolves.

5.5.2 Quality Assurance

A quality assurance program shall be prepared that describes the overall arrangements for the management, performance and assessment of the plant design. Implementation of this program shall be in accordance with the requirements of the applicable standards and codes. CSA standard CAN3-N286.2, *Design Quality Assurance for Nuclear Plants*, may be used as a program to support more detailed plans for each SSC so that the quality of the design and the selected components is ensured at all times.

Design, including subsequent changes or safety improvements, shall be carried out in accordance with established procedures that call on appropriate engineering standards and codes, and shall incorporate applicable requirements and design bases. Design interfaces shall be identified and controlled.

The adequacy of 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. Verification, validation, and approval shall be completed before implementation of the detailed design.

5.5.3 Documentation

In addition to the design documentation, documents shall be prepared to demonstrate that the requirements of this document are met. The support documents shall be clear, concise, and in a logical and understandable format, and shall include, without being limited to, the following information:

1. Design description;
2. System classifications;
3. Plant states;
4. Operating limits and conditions (OLCs);
5. Design requirements;
6. Identification and categorization of initiating events;
7. Derived acceptance criteria;

8. Deterministic safety analysis;
9. Probabilistic safety assessment (PSA); and
10. All other hazards analyses.

6.0 SAFETY REQUIREMENTS

6.1 Requirements for Defence-in-Depth

The design shall incorporate defence-in-depth, and shall therefore provide:

1. Confidence that plant failures and deviations from normal operations are minimized and accidents prevented by incorporating safety margins in the design of SSCs;
2. For control of plant behaviour during and following a postulated initiating event (PIE) using both inherent and engineered features—uncontrolled transients shall be minimized or excluded by design to the extent possible;
3. Safety systems that minimize consequences of DBAs—the need for operator actions in the early phase of DBAs shall be minimized by automatic activation of safety systems; and
4. Equipment and procedures to manage accidents and mitigate their consequences as far as practicable.

To ensure that the overall safety concept of defence-in-depth is maintained, the design shall also provide multiple physical barriers to the uncontrolled release of radioactive materials to the environment. The design shall prevent as much as practicable:

1. Challenges to the integrity of physical barriers;
2. Failure of a barrier when challenged; and
3. Failure of a barrier as a consequence of failure of another barrier.

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

6.2 Safety Functions

The 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; and
3. Facilitate the management of the plant in and following any design basis accident, and in accident conditions beyond the design basis accidents.

The following fundamental safety functions shall be in place to support normal operation during and following any PIE and, to the extent practicable, in response to BDBAs:

1. Control of reactivity;
2. Removal of heat from the core;
3. Confinement of radioactive material;
4. Control of operational discharges and hazardous substances, as well as limitation of accidental releases; and
5. Monitoring of safety critical parameters to guide operator actions.

Where practicable, these safety functions shall be performed by multiple means.

6.3 Accident Prevention and Plant Safety Characteristics

Inherently safe features for accident prevention shall be considered in the design of NPPs

In order to minimize the sensitivity of the plant design to PIEs, the expected response to any PIE shall include those of the following characteristics that can be reasonably achieved:

1. A response to a PIE produces no significant safety related effect, or produces only a change in the plant towards a safe condition, either by inherent characteristics or by the control systems;
2. Following a PIE, the plant is rendered safe by passive safety features, or by the action of control systems;
3. Following a PIE, the plant is rendered safe by the action of safety systems; or
4. Following a PIE, the plant is rendered safe by specified procedural actions.

It shall be demonstrated that the relative merits of inherent safety design features and engineering design features have been considered in the design of the NPP.

6.4 Radiation Protection and Acceptance Criteria

To achieve the safety objective (discussed in Section 4.1), all actual and potential sources of radiation shall be identified, and provision made to ensure that sources are kept under strict technical and administrative control.

The design shall be such that radiation doses to the public and to site personnel are as low as reasonably achievable. In all non-accident operational states, including maintenance and decommissioning, doses shall not exceed the limits prescribed in the *Radiation Protection Regulations*.

Prevention and mitigation of radiation exposures resulting from design basis accidents and beyond design basis accidents shall be incorporated into the design. There shall be design provisions to ensure that potential radiation doses to the public and to site personnel do not exceed acceptable limits.

Plant states that could potentially result in high radiation doses or radioactive releases shall be restricted to a very low likelihood of occurrence, and the potential radiological consequences of plant states with a significant likelihood shall be minor.

The overall risk to the public from all plant states shall be judged against the safety goals.

6.5 Exclusion Zone

The design shall include adequate provisions for an appropriate exclusion zone. The appropriateness of the exclusion zone is based on several factors, including (without being limited to):

1. Evacuation needs;
2. Land usage needs;
3. Security requirements; and
4. Environmental factors.

6.6 Facility Layout

The design of the facility layout considers the following factors:

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. Escape routes;
5. Limiting access to authorized personal;
6. Movement of hazardous substances, nuclear materials, and radioactive materials;
7. Movement of authorized and unauthorized personal; and
8. 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 shall therefore reflect a deliberate assessment of options, demonstrating that an optimized plant layout configuration has been sought.

7.0 GENERAL DESIGN REQUIREMENTS

The general design requirements comprise, at a minimum, the following information:

1. Safety classifications;
2. Design basis, including design rules and limits;
3. Design for reliability;
4. General SSC requirements, such as equipment qualification, instrumentation and control, etc.;
5. Operational activity needs, such as ageing, material control, transport, etc.;
6. Administrative and procedural needs, such as security, safeguards, human factors, etc.; and
7. Any other information necessary to support a comprehensive NPP design.

7.1 Classification of Systems by Relative Importance to Safety

All systems or items shall be identified and classified as either important or not important to safety.

Systems and items important to safety shall be further classified in order of importance, as follows:

1. Safety systems;
2. Complementary design features;
3. Safety support systems; and
4. Others systems and items whose failure may lead to safety concerns (e.g., process and control systems).

The criteria for determining safety importance shall be based on:

1. Safety function(s) to be performed;
2. The consequence of failure;
3. The probability that the system or item will be called upon to perform the safety function; and
4. The time following a PIE at which it will be called upon to operate, and the expected duration of operation.

Detailed design requirements for the systems and items important to safety shall be consistent with other applicable requirements.

Appropriately designed interfaces between structures, systems, and components of different classes shall be provided to prevent the potential of a system or item of less importance to safety from adversely affecting the function or reliability of one of greater importance.

7.2 Plant Design Envelope

A plant design envelope shall be established that comprises design capabilities for all credible plant states considered in the design, including normal operating, AOO, DBA, and BDBA states.

7.2.1 Design Basis

The design shall identify the necessary capabilities of the plant to cope with a specific range of operational states and design basis accidents (DBAs), within the established requirements.

Conservative design measures and sound engineering practices shall be applied in accordance with modern standards and codes, and shall be adhered to in the design basis for normal operation and DBAs.

The engineering design rules shall be identified for all SSCs. These design rules shall comply with the applicable modern standards and codes.

A set of design limits shall be specified for all systems and components, and for plant states, including normal operation and DBAs. The design limits shall be consistent with modern standards and codes applicable to pressure boundaries.

Those parts of structures, systems, and components that form the pressure boundaries of the safety systems shall be classified, designed, fabricated, erected, inspected, and tested in accordance with modern standards and codes.

Pressure retaining components whose failure will affect nuclear safety shall be designed to permit inspection of their pressure boundaries throughout the component design life. Any limitation on inspection must be augmented by other means to detect leakage and degradation of the component.

7.2.2 Identification of Plant States

Plant states shall be grouped into the following four categories:

1. *Normal Operating State*—operation within specified operational limits and conditions;

2. *Anticipated Operational Occurrence (AOO)*—An operational process deviating from normal operation that is expected to occur once or several times during the operating lifetime of the NPP but which, in view of the appropriate design provisions, does not cause any significant damage to items important to safety nor lead to accident conditions;
3. *Design Basis Accident (DBA)*—Accident conditions against which an NPP is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.; and
4. *Beyond Design Basis Accident (BDBA)*—Accident conditions less frequent and more severe than a design basis accident. A BDBA may or may not involve core degradation.

Classification of plant state shall also take into consideration experience and other guidance, such as the classifications used for existing reactors.

Acceptance criteria shall be assigned to each category, taking into account the requirements that frequent PIEs shall have only minor or no radiological consequences, and those events that may result in severe consequences shall be of extremely low probability.

7.2.2.1 Normal Operation

The plant shall be designed to operate safely within a defined range of parameters, with an assumed availability of a minimum set of specified support features for safety systems.

The design 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 (where appropriate), and maintenance. Safety system unavailability shall be minimized under these conditions.

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

1. Limits important to safety;
2. Control system and procedural constraints;
3. Requirements for maintenance, testing, and inspection of the plant to ensure that structures, systems and components function as intended, taking the ALARA principle into consideration; and
4. Clearly defined operating configurations, such as start-up, power production, shut down, 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 operational limits and conditions (OLCs) under which the plant will be authorized to operate.

7.2.2.2 Anticipated Operational Occurrence

The design shall include provisions such that releases to the public following an AOO do not exceed the dose acceptance criteria, as indicated in the table in Section 4.4.1, "Dose Acceptance Criteria."

The design shall include provisions such that all structures, systems and components (SSCs) shall remain fit for continued service following an AOO.

The design shall be such that the response of the plant to a wide range of AOOs will allow safe operation or shutdown, if necessary, without the necessity of invoking provisions beyond defence-in-depth Level 1, or at the most extreme, Level 2.

When operator intervention is required, equipment shall be placed at the most suitable location to ensure its immediate availability, allowing for safe and timely access.

7.2.2.3 Design Basis Accident

A set of design basis accidents shall be specified for the purpose of setting the boundary conditions according to which the SSCs important to safety are designed.

The design shall be such that releases to the public following a DBA do not exceed the dose acceptance criteria.

Provision shall be made to initiate the necessary actions of safety systems automatically where prompt and reliable action is necessary in response to a PIE. This requirement will prevent progression to a more severe condition that may threaten the next barrier.

Provision shall also be made to support timely detection of, and manual response to conditions where prompt action is not necessary, including 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 the 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 ensure its availability when needed, and to allow safe and timely worker access.

7.2.2.4 Beyond Design Basis Accident

The design shall identify credible BDBA scenarios, based on experience, engineering judgment, and the results of analysis and research. This shall include events leading to core degradation (severe accidents), particularly those events that challenge the containment.

Complementary design features shall be provided to minimize the likelihood of the identified BDBA scenarios, and mitigate their consequences.

Complementary design features shall include design or procedural considerations, or both, and shall be based on a combination of phenomenological models, engineering judgments, and probabilistic methods.

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

The complementary design features, together with the design basis plant capabilities form the plant design envelope.

Demonstration of the ability to meet the safety goals shall include BDBAs.

The design shall specify a radiological and combustible gas accident source term for use in the design of the complementary design features. This source term shall be referred to as the reference source term, and shall be based on a representative severe core damage accident.

7.2.2.5 Severe Accident

The design shall be balanced such that no particular event or design feature makes a disproportionately large or significantly uncertain contribution to the frequency of severe accidents.

The design shall identify the various potential barriers in the system at which point potential core degradation can be halted.

The design shall consider these potential barriers early in the design process, and shall consider features that can be incorporated into the design to halt their effects. All options considered, and the basis on which they were accepted or rejected, shall be documented.

Complementary design features for BDBAs shall also be assessed for their effectiveness in responding to severe accidents.

The design shall identify the equipment to be used in management of severe accidents. Environmental, fire, and seismic assessments shall demonstrate to a reasonable level of confidence that such equipment will perform as intended in the case of a severe accident.

Particular attention shall be placed on prevention of potential containment bypass in scenarios involving core degradation.

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 requirement applies to any system for which it can be shown with a reasonable degree of assurance that it will be able to function in the expected environmental conditions.

In the case of multi-unit plants, the use of available support from other units shall be relied upon only if it can be established that the safe operation of the other units is not compromised.

It shall be demonstrated that the containment will maintain its role as a leak tight barrier for a period of at least 24 hours following the onset of core damage. After this period, the containment must prevent uncontrolled releases of radioactivity.

Symptom based severe accident management guidelines (SAMG) shall be established, taking into account the plant design features and the understanding of accident progression and associated phenomena.

7.2.3 Postulated Initiating Events

Postulated initiating events (PIEs) are capable of leading to AOO or accident conditions, and shall include credible failures or malfunctions of SSC, operator errors, as well as common cause internal and external hazards.

The design shall identify PIEs based on design and operational experience, regulatory requirements, and the results of deterministic and probabilistic analyses.

7.2.3.1 Internal Hazards

Structures, systems, and components important to safety shall be designed and located so as to minimize the probability and effects of 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.

Some external events may initiate internal fires or floods and may lead to the generation of missiles. Such interaction of external and internal events shall also be considered in the design, where appropriate.

Where two fluid systems operating at different pressures are interconnected, an assumption shall be made that a single failure (the initiating event) will occur. Either the systems shall both withstand the higher pressure, or provision shall be made to preclude the design pressure of the system operating at the lower pressure from being exceeded,.

7.2.3.2 External Hazards

The design shall consider all natural and human-induced external events with which significant radiological risk may be associated. A combination of deterministic and probabilistic methods shall be used to select a subset of external events that the plant is designed to withstand, and from which the design basis events are determined.

Applicable natural external hazards include such events as earthquakes, floods, high winds, tornadoes, tsunami, and extreme meteorological conditions. Applicable human induced external events include those identified in site characterization, such as plane crashes, ship collisions, and terrorist activities.

7.2.3.3 Site Related Characteristics

Various interactions between the plant and the environment, such as population, meteorology, hydrology, geology and seismology, shall be taken into account in determining the design basis of a nuclear power plant.

The design shall take into account the availability of off-site services upon which the safety of the plant and protection of the public may depend, such as the electricity supply and fire fighting services.

7.2.3.4 Combinations of Events

Where combinations of randomly occurring individual events could credibly lead to AOOs or accident conditions, they shall be considered in the design. Such combinations shall be identified early in the design phase and shall be confirmed by PSA techniques.

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

7.3 Design for Reliability

A systematic approach shall be followed to identify the structures, systems, and components (SSCs) that are necessary to fulfill the safety functions following a PIE. It is expected that this approach will identify the need for reactor shutdown, emergency core cooling, containment, emergency heat removal and power systems, and any other emergency system.

SSCs important to safety shall be capable of withstanding all identified PIEs with sufficient quality and reliability to meet the safety goals. A reliability analysis shall be prepared for each of these systems.

Where possible, testing shall be used to demonstrate that these reliability requirements will be met during operation.

The safety systems and their support systems shall be designed to ensure that the probability of system failure on demand from all causes is lower than 10^{-3}.

The reliability model for each system shall use realistic failure criteria and best estimate failure rates, considering, in particular, the system as built and the real demand on the system from PIEs.

7.3.1 Mission Time

The mission times for all SSCs shall be defined.

7.3.2 Common Cause Failures

The design shall consider the potential for common cause failures of items important to safety to determine where the principles of diversity, separation, and independence should be applied to achieve the necessary reliability.

There shall be sufficient physical separation between the support services for safety systems, safety support systems, and process systems. This applies to equipment, as well as the routing of:

1. Electric cables for power and control of equipment,
2. Piping for service water for cooling of fuel and process equipment, and
3. Tubing and piping for compressed air or hydraulic drives for control equipment.

Where the requisite physical separation is not possible, support services may share physical space. In such cases, the reasons for the lack of requisite separation shall be stated and a justification for space sharing arrangement provided.

Where this is necessary, services for the safety and other important process systems may be arranged in a manner that incorporates the following considerations:

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

Protection against common cause events shall be provided where sufficient physical separation among individual services or groups of services does not exist.

All credible common cause events shall be considered, and the effectiveness, of physical separation and the protective measures provided, in meeting the acceptance criteria shall be demonstrated.

7.3.3 Single Failure Criterion

All safety systems and their safety support systems shall meet the single failure criterion.

The single failure criterion requires that each safety group perform all safety functions required for a PIE in the presence of:

1. Any single component failure;
2. All failures caused by that single failure;
3. All identifiable but non-detectable failures, including those in the non-tested components; and
4. All failures and spurious system actions that cause or are caused by the PIE requiring the safety functions.

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

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. Exemptions may apply to passive components.

In addition to passive failures, unintended action shall be considered as one mode of failure of a safety group.

The design shall demonstrate that each safety group can perform the required safety functions under the worst permissible systems configuration, taking into account such considerations as maintenance, testing, inspection and repair, and allowable equipment outage times.

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

Exemptions for passive components shall apply only to those that are designed, manufactured, inspected, and maintained in service, and that remain unaffected by the PIE. This exemption shall be justified analytically, taking account of loads and environmental conditions, 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 active components if they must change state following a PIE.

7.3.4 Fail-Safe Design

The principle of fail-safe design shall be incorporated into the design of SSCs important to safety for the plant. To the greatest extent practicable, plant systems shall be designed to pass into a safe state with no necessity for any action to be initiated if a system or component fails.

Foreseeable faults that could lead to a less safe plant state shall be identified and, as necessary, avoidance measures or appropriate protective features shall be provided.

7.3.5 Equipment Outages

The design shall allow online maintenance and testing of systems important to safety. For online maintenance and testing, the design shall have adequate redundancy, effectiveness, and reliability.

The time allowed for each equipment outage and the respective response actions shall be considered in the design.

7.3.6 Shared Systems

In cases where sharing of process and safety functions is permitted, the following rules shall be satisfied:

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 must be shown that all essential safety functions of the system are unaffected if it is required to mitigate the PIE;
3. The system must be designed to the standards of the system of higher importance with respect to safety;
4. If the process function is used intermittently, then it must be demonstrated by testing after each use that the safety function is available and will meet requirements; and
5. The requirements for sharing of instrumentation must be met.

7.3.6.1 Shared Instrumentation for Safety Systems

At least one of the shutdown systems shall not partake in any sharing of instrumentation.

There shall be no sharing of instrumentation between the safety systems. Where justified, sharing between a safety system and a non-safety (process or control) system may be permitted.

The reliability and effectiveness of a safety system shall not be impaired by normal operation, by partial or complete failure in the other safety or non-safety systems, or by any cross-link generated by the proposed sharing. This includes sharing that is indicated as a result of close proximity between systems, or as a result of human factors considerations, such as errors in operation, calibration, or maintenance.

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

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

There shall be no sharing of neutronic instrumentation between a shutdown system and a non-safety system.

Sharing of instrumentation between a safety system and a non-safety system shall meet the following requirements:

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 sensing device shall be electrically isolated to ensure that failures cannot be propagated from one system to the other; and
3. Isolation devices between systems of different safety importance shall always be associated with the system of higher importance.

7.3.6.2 Sharing of SSCs between Reactors

Structures, systems, and components important to safety shall generally not be shared between two or more reactors in nuclear power plants. In exceptional cases, when structures, systems, and components are shared between two or more reactors, such sharing shall exclude safety systems and turbine generator buildings containing high pressure steam and feedwater systems. In addition, it shall be demonstrated that:

1. All safety requirements are met for all reactors during normal operation, maintenance, design basis accidents, and common mode events; and
2. In the event of an accident involving one of the reactors, an orderly shutdown, cooling down, and removal of residual heat is achievable for the other reactor(s).

In the case of an NPP being built adjacent to an operating plant, for which sharing of structures, systems and components (SSCs) important to safety between NPPs has been justified, the availability of the SSCs and their capacity to meet all safety requirements shall be demonstrated during the construction phase.

7.4 Equipment Environmental Qualification

The design shall include the development and implementation of an equipment environmental qualification program that meets modern standards and codes.

Equipment environmental qualification shall ensure that the following functions can be carried out in post-accident conditions:

1. Safely shut down the reactor and maintain it in the safe shutdown condition during and following DBAs;
2. Remove residual and decay heat from the reactor after shutdown, during and following DBAs;

3. Limit the potential for release of radioactive materials from the plant, and ensure that the resulting dose to the public from DBAs is within prescribed limits and;
4. Provide post-accident monitoring 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 PSA and safety analysis, shall be used to determine the envelope of environmental conditions.

Equipment qualification shall also include consideration of any unusual environmental conditions that can reasonably be anticipated and could arise from specific operational states, such as periodic testing of the containment leak rate.

Equipment that is credited to operate during BDBA and severe accident states shall be assessed for its capacity to perform its intended function under the expected environmental conditions. A justifiable extrapolation of equipment behaviour, based on design specifications, environmental qualification testing, or other considerations, may be used to provide assurance of operability.

7.5 Instrumentation and Control

7.5.1 General Requirements

Instrumentation shall be provided to monitor plant variables and systems over the respective ranges for normal operation, AOOs, DBAs, and BDBAs, in order to ensure that adequate information can be obtained on the plant status.

Instrumentation shall be provided for measuring all the main variables that can affect the fission process, the integrity of the reactor core, the reactor cooling systems, and the containment, and for obtaining any information on the plant 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 required to do so.

The design shall include a capacity for the trending and automatic recording of measurements of any derived parameters 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 the required variables within specified operational ranges.

The design shall be such as to minimize the likelihood of operator action defeating the effectiveness of the safety and control systems in normal operations and expected operational occurrences, without negating correct operator actions following a design basis accident.

System control interlocks shall be designed to minimize the likelihood of inadvertent manual or automatic overriding, and to provide for situations when overriding interlocks are required 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.

7.5.2 Use of Computer-Based Systems or Equipment

Appropriate standards and codes for the development, testing and maintenance of computer hardware and software shall be established for systems or equipment important to safety that are controlled by computer. These standards and codes shall be implemented throughout the life cycle of the system or equipment, particularly during the software development cycle.

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

If software provided by a third-party vendor is used in systems or equipment important to safety, then it shall be demonstrated that the software—and any subsequent release of the software—has been developed, inspected, and tested in accordance with standards of a category commensurate with the safety function provided by the system or equipment.

The software development process, including control, testing, and commissioning of design changes shall be systematically documented and reviewable. An independent assessment of the software development process shall be undertaken.

Where a function important to safety is computer-based:

1. Functions not essential to safety shall be separate from and shown not to impact the safety function;
2. The safety function shall normally be executed in processors separate from software that implements other functions, such as control, monitoring and display;
3. The general requirements for diversity apply to computer-based systems that perform similar safety functions—in particular, the software in the first shutdown system and the software in the second shutdown system shall be diverse. The choice of type of diversity shall be justified;

4. The design shall incorporate fail-safe and fault tolerance features, and it shall be shown that the additional complexity ensuing from these features results in an overall gain in safety;
5. The design shall provide protection against physical attack, intentional and non-intentional intrusion, fraud, and viruses; and
6. The design shall provide for effective detection, location and diagnosis of failures in order to facilitate timely repair or replacement of equipment or software.

7.6 Safety Support Systems

Safety support systems provide services such as electrical, compressed air, and water to systems important to safety. The safety support systems shall ensure that the fundamental safety functions are available in all operational states, including normal, AOO, DBA and, to the extent practicable, BDBA states.

Where normal services are provided from external sources, back up services shall also be available on the site.

Emergency support systems shall be available to cope with the possibility of loss of normal service and, where applicable, concurrent loss of the back up service.

Normal, back up, and emergency sources of safety support systems shall have:

1. Sufficient capacity to meet the load requirements of the systems that perform the fundamental safety functions; and
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 back up systems;
2. Be qualified to the same level as the equipment to which it is providing the service;
3. Provide continuity of the service until a long term (normal or back up) service is re-established;
4. Have a margin in capacity to allow for future increases in demand; and
5. Be testable under design load conditions.

7.7 Guaranteed Shutdown State

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

7.8 Post Accident Instrumentation

Instrumentation and recording equipment shall ensure that essential information is available for:

1. Monitoring the course of DBAs;
2. Indicating the status of essential equipment; and
3. Predicting the locations and quantities of radioactive materials that could escape from the locations intended in the design.

Instrumentation sufficient to support post-accident procedures for indicating status making decision shall be classified as a complementary design feature. The recording capability shall be provided to record the vital plan parameters during accidents.

7.9 Fire Safety

The plant, including external buildings and SSCs integral to the operation of the nuclear facility, shall be designed to meet the following requirements.

7.9.1 General Provisions

Suitable incorporation of operational procedures, redundant SSCs, physical barriers; spatial separation, fire protection systems, and design for fail safe operation shall be such that the following general objectives are achieved:

1. To prevent the initiation of fires;
2. To limit the propagation and effects of fires that do occur;
3. To quickly detect and suppress fires thereby limiting damage;
4. To confine the spread of fires and their by products which have not been extinguished;
5. To prevent loss of redundancy in safety and safety support systems, and to provide assurance of safe shutdown;
6. To ensure the monitoring of critical safety parameters remains available;
7. To prevent exposure, uncontrolled release or unacceptable dispersion of hazardous substances, nuclear material, or radioactive material, due to fires;
8. To prevent the detrimental effects of event mitigation efforts, both inside and outside of containment;
9. To ensure structural sufficiency and stability from fires;

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

Fire suppression system pressure retaining components shall be designed to modern international standards and codes and registered with an Authorized Inspection Agency.

7.9.2 Safety to Life

The design shall protect workers and the public from fire or explosion initiated event sequences 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; and
2. Persons intimate with the initial event have a decreased risk of injury or death.

To demonstrate that the above life safety objectives have been achieved in accordance with established radiological, toxicology and human factors criteria, the design shall provide:

1. Effective and reliable means of detecting fires for all areas;
2. Effective and reliable means of emergency notification to workers, including the nature of the emergency and protective actions by workers;
3. Multiple and separate safe egress paths from any area;
4. Exit locations that are easily accessible to workers;
5. Sufficient exiting capacity for the number of workers accounting for the emergency movement of crowds;
6. Effective and reliable identification and illumination of egress routes and exits;
7. Protection of workers from fires and their by-products (i.e. combustion products, smoke, heat, etc.) during egress and in 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 actions during or following a fire;
10. Structural integrity and stability of buildings and structures to ensure workers and emergency responder safety during and after a fire; and
11. Protection of workers from the release or dispersion of hazardous substances, radioactive material or nuclear material from fires.

7.9.3 Environmental Protection and Nuclear Safety

The design shall minimize the release, dispersion and impact of hazardous substances or radioactive material from fires on the environment.

Fire shall be treated as a design basis accident. 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.

7.10 Seismic Qualification

The seismic qualification of all SSCs shall be in accordance with the requirements for design basis earthquakes (DBEs) and site design earthquakes (SDEs) given in the applicable modern standards and codes.

The design shall include instrumentation for monitoring seismic activity at each nuclear reactor site. This instrumentation shall meet the requirements of applicable modern standards and codes.

For design of NPPs to be built in areas of unusual geological complexity, or for which historical seismicity information is unreliable, incomplete, or indicates appropriately low earthquake levels, the available data shall be supplemented by the operation of a micro-earthquake recording system.

7.10.1 Seismic Design and Classification

Systems, structures, and components that perform the following functions shall be designed to withstand a design basis earthquake:

1. SSCs whose failure could directly or indirectly cause an accident situation leading to core damage;
2. SSCs restricting the release of radioactive material to the environment;
3. SSCs important to nuclear safety, including safety systems and their safety support systems;
4. SSCs assuring the sub-criticality of stored nuclear material; and
5. SSCs such as radioactive waste tanks containing radioactive material that, if released, would exceed regulatory dose limits.

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

The seismic qualification of SSCs shall be performed for the DBE level unless qualification to the SDE level is acceptable and justified in the design.

The seismic qualification of SSCs shall include fragility testing.

7.11 In-Service Testing, Maintenance, Repair, Inspection, and Monitoring

The structures, systems and components important to safety shall be designed to be calibrated, tested, maintained and repaired, or replaced, inspected and monitored over the lifetime of the NPP, to maintain the NPP within the boundaries of the design. Testing, calibration, maintenance and repair, replacement, inspection and monitoring shall be facilitated and performed to standards commensurate with the importance of the safety functions. There shall be no significant reduction in system availability and or undue exposure of the site personnel to radiation.

The following approach shall be followed if the SSCs important to safety cannot be designed to enable the testing, inspection, or monitoring to the extent desirable:

1. Other proven alternative methods shall be specified, such as surveillance of reference items or use of verified and validated calculation methods; and
2. Conservative safety margins shall be applied or other appropriate precautions shall be taken to compensate for possible unanticipated failures; or
3. The components shall be replaced with equal or better qualified items at 80% of their mean failure time, especially components critical to nuclear safety.

Details of how these requirements have been met shall be documented in the design.

The facilities for monitoring the chemical condition of any component shall be provided, including the sampling of fluid, air, metal and other components. The design shall specify the means to be provided for adding or modifying the chemical constitutes of fluid or air streams.

The design shall specify the commissioning requirements and targets, and consider the needs for such testing.

7.12 Civil Structures

7.12.1 Design

The design shall specify the required performance for the safety functions of the civil structures under normal operation and accident conditions.

Civil structures important to nuclear 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 events such as earthquakes, floods, high winds, tornadoes, tsunamis, and extreme meteorological conditions with which significant radiological risk may be associated shall be considered in the selection of the site and the design of the civil structures.

Settlement analysis and evaluation of soil capacity shall include consideration of the effects of fluctuating ground water on the foundations. Potential liquefiable soil strata and slope failure shall be identified and evaluated.

Civil structures shall be designed to meet the serviceability, strength, and stability requirements for all possible load combinations under normal operational, AOO, and DBA conditions, and in the event of external hazards. The serviceability requirements shall include, without being limited to, deflection, vibration, permanent deformation, cracking, and settlement.

The design specifications shall define all loads and load combinations, with due consideration given to concurrence probability and loading time history. The standards and codes used in the design shall also be identified.

The design of civil structures and the use of construction materials shall take environmental effects into account. The choice of construction material shall be commensurate with the designed service life and potential life extension of the plant.

Structural analyses for all civil structures are to be included in the plant safety assessment.

7.12.2 Surveillance

The design shall enable implementation of periodic inspection programs for structures related to nuclear safety to verify as-constructed conditions and to monitor in-service for degradations that may compromise the intended design function of the structures. In particular, equipment shall be provided to permit the monitoring of foundation settling.

Pressure and leak testing shall be performed on applicable structures to demonstrate that they meet design requirements. Routine inspection of sea and river flood defences shall be made to show fitness-for-service.

7.12.3 Lifting of Large Loads

The design shall account for the lifting of large and heavy loads, particularly those containing radioactive material. It shall identify the large loads 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 incorporate large margins, together with appropriate interlocks and other safety features.

The plant shall be placed in a cold shutdown state prior to lifting large and heavy loads above critical areas of the plant, unless it can be shown that the consequences of dropping these loads are acceptable with adequate design margins.

7.13 Commissioning Requirements

All plant systems shall be designed such that, prior to the first criticality of the reactor, tests of the equipment can be performed, to the greatest extent practicable, to verify that all design requirements have been achieved.

7.14 Ageing and Wear

The design shall take into account ageing and wear effects on structures and components. These details shall include, as a minimum:

1. An assessment of design margins for structures and components to take into account all known ageing and wear mechanisms and potential degradation in all normal operating conditions, including the effects of testing and maintenance processes; and
2. The provisions for monitoring, testing, sampling, and inspection to assess ageing mechanisms, to verify predictions and identify unanticipated behaviour or degradation that may occur during operation.

7.15 Material Control

Provision shall be made to prevent and remove all foreign material and corrosion products that may impact on safety.

7.16 Transport and Packaging for Fuel and Radioactive Waste

The design shall incorporate appropriate features to facilitate transport and handling of new fuel, used fuel, and radioactive waste. Consideration shall be given to facility access and to the lifting capacity and packaging capabilities.

7.17 Escape Routes and Means of Communication

The NPP shall be provided with a sufficient number of safe escape routes available in all plant states, including seismic events. These routes shall have clear and durable signage, emergency lighting, ventilation and other building services essential to the safe use of these routes.

The escape routes shall meet the relevant Canadian requirements for radiation zoning, fire protection, industrial safety and plant security. The ability to escape from containment shall be assured regardless of the pressure in containment.

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

The design shall ensure that various means of communication are available within the nuclear power plant, in the immediate vicinity of the NPP, and to off-site agencies, as stipulated in the emergency plan. This requirement shall provide for diversity in the communication methods.

7.18 Human Factors

A human factors engineering program plan shall ensure that the design is in accordance with modern human factors standards, principles, and practices.

Relevant and proven systematic analysis techniques shall be used to address human factors issues within the design process.

The design shall reduce the likelihood of human error as far as possible, provide error recovery mechanisms, and mitigate the consequences of error in order of priority. To facilitate the interface between the operating personnel and the plant, attention shall be paid to plant layout and procedures, maintenance, inspection, and training.

Working areas and working environments shall be designed according to ergonomic principles.

To ensure an appropriate and clear distinction between the functions assigned to operating personnel and those assigned to automatic systems, the design shall include systematic consideration of human factors and the human-machine interface. This consideration shall continue in an iterative way throughout the entire design process.

The human-machine interfaces in the main control room, the secondary control room, the emergency support centre, and in the plant, shall be designed to 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 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 accident management, and that of an equipment operator.

The design shall identify the type of information that will enable an operator in a systems manager role to readily:

1. Assess the general state of the plant, whether in normal operating, AOO, or DBA states;
2. Confirm that the designed automatic safety actions are being carried out; and
3. Determine the appropriate operator-initiated safety actions to be taken.

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

Design goals shall include promoting the success of operator actions with due regard for the time available for action, the physical environment to be expected, and the psychological demands to be 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, it shall be demonstrated that:

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

7.19 Robustness against Malevolent Acts

The design shall include provisions that promote security and robustness in response to malevolent acts, in accordance with applicable regulations and modern standards and codes.

7.19.1 Design Principles

The design shall be such that the NPP and any other on-site facilities with potential to release large amounts of radioactive material or energy are robustly protected against malevolent acts.

Threats from credible malevolent acts, referred to as design basis threats (DBTs), shall be considered in the design. These threats may be carried out from underground, or from land, air, or nearby bodies of water. The potential for threat from acts by more than one team of saboteurs, who may be approaching by the same or different modes, shall also be considered.

Furthermore, given that the threat may come from inside as well as outside the plant, the design must consider placement of civil utilities to minimize access requirements for repair, maintenance, etc., to promote security from DBTs.

The design shall provide protection against DBTs, pursuant to the *Nuclear Security Regulations*. The physical protection systems shall be sufficiently flexible to accommodate future modifications as may be needed to address changes to evolving DBTs.

Vital areas to counter the DBTs shall be identified. Multiple barriers shall be provided such that the on-site response force has sufficient time to make an effective intervention. As well, the vital areas should be protected from inadvertent damage during the carrying out of defensive actions.

An assessment methodology shall be developed to assess the challenges imposed by the DBTs. This methodology shall include methods for evaluating the capabilities for meeting these challenges.

The assessment methodology for DBTs shall apply conservative design measures and sound engineering practices. Assessment for severe DBTs, referred to as beyond design basis threats (BDBTs), may be based on realistic or best estimate assumptions, methods, and analytical criteria.

7.19.2 Acceptance Criteria

The design shall provide a safe shutdown success path that allows for control of the fission reaction, cooling of the fuel, containment of any potential releases, and monitoring.

The design shall provide for ongoing availability of fundamental safety functions following an event associated with a DBT, with the goal that dose acceptance criteria will not be exceeded. The damage to the containment shall not result in the leak rate exceeding the design value at the containment design pressure.

In the case of BDBTs, the shutdown of the reactor shall be achieved and maintained as long as necessary. The containment shall be designed such that BDBTs will not result in an uncontrolled pathway for the release of radioactivity outside the containment. The design shall also facilitate mitigation and recovery efforts by the plant personnel.

7.19.3 Additional Considerations

The design shall identify vital areas, which include areas containing nuclear material or equipment required to perform fundamental safety functions. Vital areas shall be taken into account in the design and verification of robustness.

Consistent with the concept of defence-in-depth, multiple barriers shall be provided for protection against DBTs. The design shall include physical protection systems, engineering safety provisions, and measures for post-event management, as appropriate. To the extent practicable, the failure of a preceding barrier shall not compromise the integrity and effectiveness of subsequent barriers.

The design shall facilitate preparedness for, prevention and early warning of, and response to, potential malevolent acts. The design shall provide for the control and recovery of critical plant systems in the medium and long term.

The design shall minimize the number of facility access and egress points, and the entry points to protected areas. This includes vehicle, pedestrian, and large service pipes located underground that could be used to gain access to the facility.

Structures shall be designed to provide sufficient delay to allow for effective intervention by the on site response force. Detection systems shall have a high reliability in all types of weather and lighting conditions. In addition, immediate assessment systems shall be capable of identifying any cause of alarm at any point of detection.

7.20 Safeguards

The design shall ensure compliance with the obligations arising from modern standards and codes and Canada's international agreements and requirements pertaining to safeguards and non-proliferation.

7.21 Decommissioning

The design shall take into account future plant decommissioning and dismantling activities, 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 assist decontamination;
2. Plant layout will facilitate access for decommissioning or dismantling activities; and
3. The potential new facilities or expansion of the existing facilities for storing radioactive waste generated is considered.

8.0 SYSTEM-SPECIFIC REQUIREMENTS

8.1 Reactor Core

The design of the reactor core shall be such that:

1. The fission chain reaction is controlled and when necessary, terminated under all plant states, including normal operation, AOOs, DBAs, and as far as practicable, BDBAs;
2. To the extent practicable, the net effect of the prompt inherent nuclear feedback characteristics compensate for a rapid increase in reactivity;
3. Inadvertent re-criticality is prevented for all short and long term shutdown states; and
4. Prevention of re-criticality following severe accidents is considered.

The reactor core and its control and shutdown systems shall be designed with appropriate margins to ensure that the specified design limits are not exceeded in operational states, or DBAs.

The design shall provide protection against deformations to reactor structures that have the potential to adversely affect the behaviour of the core or associated systems.

The reactor core and associated cooling systems shall withstand the static and dynamic loading expected in normal operational states and DBAs, to the extent necessary to ensure safe shutdown of the reactor, to maintain the reactor sub-critical, and to ensure cooling of the core.

The reactor core and associated coolant, control, and safety systems shall be designed to enable adequate inspection and testing throughout the service lifetime, and shall include the following provisions:

1. Inspection programs shall be developed; and
2. Testing programs for the control and shutdown systems shall be developed in accordance with the reliability requirements for the systems.

8.1.1 Fuel Assemblies

Fuel assemblies shall be designed to perform reliably in the anticipated conditions in the reactor core during normal operation and AOOs, and all potential conditions that could affect the fuel shall be identified.

Fuel design limits shall be specified and supported by experimental testing and analysis. Fuel power and burn-up envelopes shall be identified, used for design of the fuel and reflected in the OLC.

The fuel design limits shall encompass the plant states that may be imposed in AOOs such that the fuel remains fit for continued service following all AOOs.

The fuel shall be designed to minimize the rate of fuel failure and to limit post-defect deterioration so that leakage of fission products is minimized. Failed fuel detection and location systems shall be provided.

Fuel assemblies shall be designed to permit adequate inspection of their structure and component parts both prior to loading into the reactor and after irradiation.

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 the fuel assembly requirements can be achieved.

The requirements for reactor and fuel design shall also be maintained in the event of changes in fuel management strategy or in operational states over the operational lifetime of the plant.

8.1.2 Reactor Core Control System

The reactor core control system shall detect and intercept deviations from normal operational states 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 reactor control mechanisms shall limit the positive reactivity insertion rate to a level required to control reactivity changes and power manoeuvring.

The design shall include means of detecting levels and distributions of neutron flux. This applies to neutron flux in all regions of the core and in operational states, including after shutdown and during and after refuelling states, and states arising from anticipated operational occurrences.

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 all AOOs.

8.2 Reactor Coolant System

The reactor coolant system and its associated pressurizer and auxiliary systems shall be designed with sufficient margin to ensure that the appropriate design limits of the reactor coolant pressure boundary are not exceeded in normal operation, AOOs, or DBAs.

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

The component parts containing the reactor coolant, together with the devices that hold those parts in place, shall be designed to withstand the static and dynamic loads anticipated in normal, AOO, and DBA plant states.

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

The design shall minimize the likelihood of flaws being initiated on the pressure retaining boundary for the reactor coolant system. To permit timely detection of flaws, the design shall also ensure that any flaws that are initiated will propagate in a regime of high resistance to unstable fracture with fast crack propagation. Plant states in which components of the reactor coolant pressure boundary could exhibit brittle behaviour shall be avoided.

The design shall reflect consideration of all conditions of the boundary material in normal operation (including maintenance and testing), AOOs and DBAs. Consideration shall also be given to expected end-of-life properties affected by ageing 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 normal operation, AOOs, and DBAs, with allowance made for deterioration that may occur in service.

A system capable of detecting leakage from the reactor coolant system shall be provided.

8.2.1 In-Service Pressure Boundary Inspection

The components of the reactor coolant pressure boundary shall be designed, manufactured, and arranged in such a way that it is possible, to carry out adequate inspections and tests of the boundary throughout the lifetime of the plant.

The design shall also facilitate surveillance in order to determine the metallurgical conditions of materials.

8.2.2 Inventory

Taking volumetric changes and leakage into account, provision shall be made for controlling coolant inventory and pressure to ensure that specified design limits are not exceeded in normal operation. The systems performing this function shall have adequate capacity (flow rate and storage volumes) to meet this requirement.

The inventory in the reactor coolant system and its associated systems shall be sufficient to allow for a cool down from hot operating conditions to zero power cold conditions without the need for transfer from any other systems.

8.2.3 Cleanup

The design shall provide for adequate removal of radioactive substances from the reactor coolant, including activated corrosion products, and fission products leaking from the fuel.

8.2.4 Removal of Residual Heat from Reactor Core

Two independent systems shall be available for removing residual fission product decay heat and other residual heat from the reactor core. This heat removal shall be at a rate that prevents the specified fuel design limits and the design basis limits of the reactor coolant pressure boundary from being exceeded. These systems shall be designed to be capable of being initiated at the normal operating conditions of the reactor coolant system

The design shall include interconnections and isolation capabilities and other appropriate design features with reliability that is commensurate with system design requirements.

8.3 Steam Supply System

8.3.1 Steam Generator and Associated Piping

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

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

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

The steam generators and associated piping (i.e., the piping up to and including the first isolation valve) shall be qualified to withstand a design basis earthquake.

8.3.2 Steam and Feedwater System Piping and Vessels

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

The auxiliary feedwater, boiler pressure control, and other auxiliary systems, shall be designed to prevent AOOs escalating to accident conditions.

8.3.3 Turbine Generators

Over-speed protection systems for the turbine generators shall be provided. These systems shall be designed to ensure that the probability of failure from all causes is lower than 10^{-4}/demand.

The axes of the turbine generators shall be oriented to minimize the potential for any missiles that result from a turbine break-up striking the containment or other SSCs important to safety.

8.4 Shutdown Systems

8.4.1 Shutdown System Design

The reactor shutdown system shall be capable of promptly reducing neutronic 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 provide two redundant, separate, independent, and diverse means of shutting down the reactor.

The design shall provide two independent means of preventing re-criticality from any pathway or mechanism during all reactor shutdown states.

8.4.2 Effectiveness

The rate of reactivity, negative insertion, and depth of each shutdown system shall be commensurate with the demands posed by the AOOs and DBAs in the short and long term.

The design shall provide a high degree of confidence in the predictions of the reactor's capacity to respond to initiating events in a manner that assures effective shutdown.

One shutdown system shall be fully effective on its own for all AOOs and DBAs in all modes of operation, including the shutdown states (i.e., shall prevent the plant parameters from exceeding the derived acceptance criteria). The other shutdown system, in combination with the first, shall prevent failure of reactor shutdown leading to unacceptable consequences. The frequency of any event sequence involving failure to shutdown shall be less than 10^{-7} per plant year.

The shutdown margin for all shutdown states shall be such that the core will remain sub-critical for any credible changes in the core configuration and reactivity addition, without operator intervention.

8.4.3 Acceptance Criteria

Derived acceptance criteria for trip parameter effectiveness shall be specified for all AOOs and DBAs. A safety analysis shall be performed to demonstrate the effectiveness of the shutdown system.

8.4.4 Reactor Trip Parameters

For each event, there shall be at least one direct parameter for each of the credited shutdown systems to trip the reactor in time to meet the derived acceptance criteria. This parameter shall be based on a direct measure of the challenge to the derived acceptance criteria and/or a direct measure of the event. There shall be no gap in the trip coverage. Considering all reactor powers and all modes of reactor operation, the trip parameter shall be effective in meeting the derived acceptance criteria for the entire spectrum of failures in a given event set.

Where a direct trip parameter does not exist, two diverse trip parameters shall be required. Where the trip coverage is not adequate for some combination of plant parameter values, a second, but not necessarily diverse, trip parameter shall be provided to eliminate the gap in trip coverage.

In all cases, the derived acceptance criteria margins shall be sufficiently large, taking into account limitations in relevant knowledge and uncertainties in predicting the transient. The extent of trip coverage provided by all available parameters shall be shown for a given set of events.

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

8.4.5 Robustness

The design shall be sufficiently robust to prevent unexpected failures from impairing the shutdown systems. The systems shall meet all the requirements under single failure criterion and failsafe design. The design shall incorporate the principle of failsafe design to the greatest extent practicable.

To the extent possible, stored energy shall be used in the actuation of the shutdown system components.

8.4.6 Diversity

The design of each shutdown system shall be fully independent of all other shutdown systems. Each shutdown system design shall also be independent of process systems to the extent practicable.

The effectiveness of each shutdown system shall not be impaired by normal operation, or by a partial or complete failure in the other shutdown, safety, or process systems.

Limited instrumentation sharing between one of the shutdown systems and a process system may be permitted, provided the applicable requirements are met. This sharing can occur only with one shutdown system; it is not permitted for both.

The functional diversity of the two shutdown systems shall be such that common-mode failures do not disable both systems.

8.4.7 Common Cause Failures

The design of each shutdown system shall be such that its effectiveness is not impaired by the consequential effects of the initiating event, including the environment it creates. Shutdown system components shall meet all applicable requirements for equipment qualification.

Both shutdown systems shall be qualified to remain functional during and following a design basis earthquake.

The design shall be such that, in the case of a maximum credible catastrophic external event such as a plane crash or missile strike on the reactor building, at least one of the shutdown systems shall remain functional.

8.4.8 Reliability

Each shutdown system shall be designed to ensure that the probability of its failure on demand from all causes is lower than 10^{-3}.

The design of each shutdown system shall permit ongoing demonstration that it 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 done at a frequency commensurate with applicable requirements.

8.4.9 Human Error

Human error in design, construction, operation, maintenance, and testing have the potential to disable one or both of the shutdown systems simultaneously; therefore, appropriate design measures and administrative controls shall be implemented and monitored to minimize the potential for, and impact of, human error.

8.4.10 Monitoring and Operator Action

Means for monitoring the status of the shutdown systems, and manual actuation, shall be provided in the main control room. Means of manual actuation and sufficient information indicating the status of reactor core shall be provided in a physically separate secondary control area.

An operator shall not be able to prevent initiation of automatic shutdown. Once initiated, it shall not be possible for an operator to arrest the progress of shutdown action.

The need for manual actuation of the shutdown systems shall be minimized.

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

8.4.11 Applicable Standards and Codes

The design shall meet all applicable standards and codes for shutdown system design.

8.5 Emergency Core Cooling System

All water-cooled nuclear power reactors 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 significant loss of reactor coolant. All equipment required for correct operation of the ECCS shall be considered to be part of the system or its safety support system(s).

Safety support systems shall include systems that supply electrical power or cooling water to equipment used in the operation of the ECCS, and shall meet all relevant requirements.

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

1. All fuel in the reactor and all fuel assemblies shall be kept in a configuration such that continued removal of the decay heat produced by the fuel can be maintained; and
2. The system shall be capable of supplying a continued cooling flow (recovery flow path) to prevent further damage to the fuel after adequate cooling of the fuel is re-established by the ECCS.

Following an accident, operation of ECCS equipment shall not be dependent on power supplies from the electrical grid or from the turbine generators associated with any reactor unit on the same site as the reactor involved in the accident.

The ECCS recovery flow path shall not allow debris to impede the recovery of coolant following a loss of coolant accident (LOCA).

Design shall be such that maintenance and reliability testing conducted when ECCS availability is required shall be carried out without a reduction in the effectiveness of the system below the OLCs.

Design shall be such that, in the event of an accident, it is not readily possible for an operator to prevent injection of emergency coolant from taking place when such injection is required.

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

For any ECC piping in an extension of containment that could contain radioactivity from the reactor core, the following shall be satisfied:

1. It shall be designed as a piping extension to containment and shall meet the requirements for metal penetrations of containment;
2. All piping and components of the ECC recovery flow path/loop piping that are open to the containment atmosphere shall be designed for a pressure greater than the containment design pressure;
3. All ECC recovery flow path/loops shall be housed in a confinement structure that prevents leakage of radioactivity to the environment and to adjacent structures; and
4. This housing shall include detection capability for leakage of radioactivity and the capability to return the radioactivity to the flow path.

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

Inadvertent operation of all or part of the ECCS shall not have a detrimental effect on plant safety.

8.6 Containment

The containment design shall comprise the following:

1. General requirements;
2. Strength of the containment structure;
3. Capability for pressure tests;
4. Leakage;
5. Containment penetrations;
6. Containment isolation;
7. Reactor coolant system auxiliaries that penetrate containment;
8. Systems connected to containment atmosphere;
9. Closed systems;
10. Containment air locks;
11. Internal structures of the containment;
12. Containment pressure and energy management;
13. Control and cleanup of the containment atmosphere;

14. Coverings, coatings, and materials; and
15. Severe accidents.

8.6.1 General Requirements

All nuclear power reactors shall be installed within a containment structure that is intended to minimize the release of radioactive materials to the environment during normal operation, and to meet the safety goals. Containment shall also assist in mitigating the consequences of beyond design basis accidents.

The design of the containment system shall account for all AOOs and DBAs, and shall consider BDBAs, including severe accident conditions (see Section 7.2.2.4, "Beyond Design Basis Accident").

The containment shall be designed as both a safety system and a complementary design feature in accordance with the general design requirements of this regulatory document. The containment design shall include leak-tight structures and associated systems for pressure and temperature control, as well as features for the isolation, management, and removal of fission products, hydrogen, and other substances that could be released into the containment atmosphere.

There shall be a clearly defined continuous leak-tight containment envelope. The boundary of this containment envelope shall be 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 a containment extension.

The containment design shall incorporate systems 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 free radioactive material within the containment envelope; and
4. Equipment required to limit the release of radioactive material from the containment envelope following an accident.

The autonomy of the compressed air system shall be demonstrated when the design includes the use of compressed air or non-condensable gas systems in response to a design-basis accident. In the event of a loss of compressed air, containment isolation valves must fail in their safe state.

Compressed air systems shall be designed such that over-pressurization and bypassing of containment can be prevented.

The design shall provide for sufficient biological shielding for all plant states.

8.6.2 Strength of the Containment Structure

The strength of the containment structure shall provide sufficient margins of safety based on potential internal overpressures, under pressures, temperatures, dynamic effects such as missile impacts, and reaction-forces anticipated to result in the event of DBAs. Application of strength margins shall apply to access openings, penetrations and isolation valves, and to the containment heat removal system. The margins shall also reflect:

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

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

The containment structure shall be designed to withstand external impacts to allow preservation of key safety functions of the plant. Consideration shall be given to the external events identified in the site evaluation for the NPP, including such natural phenomena as flooding and tornadoes, and human-induced events such as aircraft crashes or external explosions.

All parts of the containment system credited in the safety analysis following a DBE shall be designed to remain fully functional.

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

8.6.3 Capability for Pressure Tests

The containment structure shall be designed to enable pressure testing at a specified pressure to demonstrate structural integrity. Testing shall be conducted before operation of the plant, and throughout the plant’s lifetime, as required by modern applicable standards and codes.

8.6.4 Leakage

8.6.4.1 Design Limiting Leakage Rate

A derived leakage rate limit shall be:

1. Below the applicable safety limit;
2. As low as is practicably attainable; and
3. Consistent with state-of-the-art design practices.

The safety limit leakage rate is the rate that assures all of the following factors:

1. Normal operation release limits are met; and
2. AOOs and DBAs shall not result in exceeding dose acceptance criteria.

The derived value shall be referred to as the design limiting leakage rate.

8.6.4.2 Test Acceptance Leakage Rate Limits

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

8.6.4.3 Leak Rate Testing

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

1. At design pressure at commissioning; and
2. Over the service lifetime of the reactor, either at the containment design pressure or at reduced pressures that permit estimation of the leakage rate at the containment design pressure as required by modern standards and codes.

To the extent practical, penetrations shall be designed to allow individual testing of each penetration.

The design shall be such that any gross breach of the containment envelope can be readily and reliably detected.

8.6.5 Containment Penetrations

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

All containment penetrations shall meet 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, jet forces, and pipe whip.

All penetrations shall be designed to allow for periodic inspection as required by modern standards and codes.

If resilient seals such as elastomeric seals, electrical cable penetrations, or expansion bellows are used with penetrations, they shall be designed with the capability 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.

8.6.6 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 sealable. This provision 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.

The lines that penetrate containment shall be fitted with at least two containment isolation valves arranged in series. The isolation valves shall be located as close to the containment as practical.

Automatic isolation valves shall be designed to take the position that provides 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 acceptable with prior approval.

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

8.6.7 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 normally be 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 normally be in the closed position.

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

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

1. It shall be designed as a piping extension to containment and shall meet 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; and
4. This housing shall include detection capability for leakage of radioactivity and the capability to return the radioactivity to the flow path.

8.6.8 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 as follows:

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

The line up to and including the second valve shall be part of the containment envelope.

8.6.9 Closed Systems

All closed piping service systems shall have a 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.

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

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

8.6.10 Containment Air Locks

Personnel access to the containment shall be through airlocks. The airlocks shall be equipped with doors that are interlocked to ensure that at least one of the doors is closed during normal operation, AOOs, and DBAs. Where provision is made for entry of personnel for surveillance or maintenance purposes during normal operation, provision for personnel safety, including emergency egress, shall be specified in the design. This requirement shall also apply to equipment air locks.

8.6.11 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 that may cause damage to load bearing and safety systems during AOOs and DBAs. The internal structures shall be consistent with the hydrogen control strategy.

8.6.12 Containment Pressure and Energy Management

The design shall enable heat removal and pressure reduction in the reactor containment in all plant states. Systems designed for this purpose shall be considered part of the containment system, and shall:

1. Minimize the pressure-assisted release of fission products to the environment;
2. Preserve containment integrity; and
3. Preserve required leak tightness.

8.6.13 Control and Cleanup of the Containment Atmosphere

Systems to control fission products, hydrogen, oxygen, and other substances that may be released into the reactor containment shall be provided as necessary, to:

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

The design shall support isolation of all sources of compressed air and other non-condensable gases into the containment atmosphere following an accident. The design shall also ensure that, in the event that of an initiating event resulting in ingress of non-condensable gas, the pressure of the containment will not exceed the design. The isolation of compressed air sources shall be such as to prevent any bypass of containment.

8.6.14 Coverings, Coatings and Materials

The coverings and coatings for components and structures within the containment shall be carefully selected, and their methods of application 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.

8.6.15 Severe Accidents

Containment shall be designed such that, for a period of at least 24 hours following the onset of severe core damage, the containment leakage rate will be kept within the design limiting leakage rate. The containment shall prevent uncontrolled releases of radioactivity after this period.

The ability of the containment system to withstand loads associated with severe accidents shall be demonstrated, and shall include the following considerations:

1. Various heat sources, including decay heat, metal-water reactions, and 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 air locks and containment penetrations; and
8. Effects of the accident on the integrity and functionality of internal structures.

The containment floor in the reactor vault shall be designed, as far as practical, to:

1. Prevent a containment melt-through or failure due to the thermal impact of the core debris;
2. Facilitate cooling of the core debris; and
3. Minimize generation of non-condensable gases and radioactive products.

8.7 Heat Transfer to an Ultimate Heat Sink

Systems shall be provided to transfer residual heat from SSCs important to safety to an ultimate heat sink. This function shall be carried out at very high levels of reliability during normal operation, AOOs, and DBAs. All systems that contribute to the transport of heat by conveying heat, providing power, or supplying fluids to the heat transport systems, shall 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 system design, 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 give consideration to extending the capability to transfer residual heat from the core to an ultimate heat sink so that, in the event of a severe accident:

1. Acceptable conditions can be maintained in structures, systems, and components;
2. Radioactive materials can be confined; and
3. Releases to the environment can be limited.

8.8 Emergency Heat Removal System

The design shall provide an emergency heat removal system (EHRS). The EHRS is a safety system that provides for removal of decay heat for all AOOs and DBAs that could lead to the loss of heat removal capability via the steam generators.

The EHRS shall meet all applicable requirements, including requirements for reliability, environmental qualification, sharing, separation, tolerance to single failure, and testing.

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 a supply of water is required for the EHRS, that supply shall come from a source that is independent of the normal steam generator feedwater system.

The initiation of EHRS and, where applicable, the injection pressure and the rate of refill water into the steam generators, shall be such that no additional fuel failure will occur.

The design shall ensure that the initiation of the EHRS does not cause any failure of the steam generator tubes or significantly increase the existing leakage.

The design shall minimize the potential for internally or externally induced common cause failures that may result in the failure of both the EHRS and the normal heat sink via the steam generators.

The design shall be such that all maintenance and reliability testing that may be performed when EHRS availability is required can be carried out without a reduction in system effectiveness below that required by the OLCs.

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

8.9 Emergency Power Supplies

Emergency power supplies shall have sufficient capability and reliability to provide all the necessary power to maintain the plant in a safe state in the event of all DBAs, assuming a common cause loss of off-site power where this may occur due to the PIE, and a single failure.

The emergency power supplies shall have sufficient capacity to support severe accident management actions.

The emergency power supplies shall be designed such that they:

1. Are initiated manually; and
2. Are testable under design load conditions.

8.10 Control Facilities

8.10.1 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, and BDBAs.

The design shall identify internal and external events and all design basis and common cause events that may pose a direct threat to the continued operation of the control room. The MCR shall be designed to protect the occupants and the equipment from the effects of these events.

The MCR design shall be such that safety functions initiated by automatic control logic in response to an accident can also be initiated manually from the main and secondary control rooms.

The MCR envelope shall be identified, and shall be equipped with is own dedicated breathing air and ventilation system.

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 ensure that appropriate lighting levels and thermal environment are maintained, and that noise levels are minimized to acceptable standards and codes.

Ergonomic factors shall be taken into account in the design of the MCR to ensure both physical and visual accessibility in relation to controls and displays, without adverse impact on health and comfort. This shall include hardwired display panels as well as computerized displays, with the aim of making these displays as user friendly as possible.

Cabling for the instrumentation and control equipment in the MCR shall be arranged such that a fire in the secondary control room cannot disable the equipment in the MCR.

The design shall include devices that will efficiently provide visual and, if appropriate, audible indications of operational states and processes that have deviated from normal and that could affect safety.

Information shall be available for the operator to monitor the effects of the automatic actions of all control, safety, and safety support system actions.

The MCR shall be provided with secure communication channels to the emergency support centre and to off-site emergency response organizations.

The MCR shall allow for extended shift operating periods.

8.10.1.1 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 severe accidents.

The SPDS shall:

1. Display safety critical parameters within the full range expected in normal operation and during accidents;
2. Track data trends;
3. Indicate when process or safety limits are being approached or exceeded;
4. Display the status of safety systems; and

The SPDS shall be designed and installed in such a manner that the same information is made available in a secure manner to the emergency support centre.

8.10.2 Secondary Control Room

The design shall provide secondary control room (SCR) that is physically and electrically separate from the MCR and is capable of keeping the plant under control in case the MCR becomes uninhabitable.

The secondary control room shall be remote from the MCR to minimize the potential for common cause events to make both the MCR and SCR uninhabitable at the same time. It shall be demonstrated that at least one control room will be habitable and accessible, by means of a qualified route for all accident conditions, for any event.

Controls and displays shall be provided to support necessary operator actions.

Instrumentation and control equipment shall be available, so that the reactor can be placed and maintained in a shut down state, residual heat can be removed, and essential plant variables can be monitored.

The design shall identify internal and external events and all design basis and common cause events that may pose a direct threat to the continued operation of the SCR. The SCR shall be designed to protect the occupants and the equipment from the effects of these events.

The SCR design shall be such that safety functions initiated by automatic control logic in response to an accident can also be initiated manually from the main and secondary control rooms.

The design of the SCR shall ensure that appropriate lighting levels and thermal environment are maintained, and that noise levels are minimized to acceptable standards and codes.

Ergonomic factors shall be taken into account in the design of the SCR to ensure both physical and visual accessibility in relation to controls and displays, without adverse impact on health and comfort. This shall include hardwired display panels as well as computerized displays, with the aim of making these displays as user friendly as possible.

Cabling for the instrumentation and control equipment in the SCR shall be arranged such that a fire in the main control room cannot disable the equipment in the SCR.

The SCR shall be equipped with a safety parameter display system that is similar to that in the MCR. As a minimum, it shall provide the information required to facilitate the management of the reactor when the MCR is uninhabitable.

The SCR shall be provided with secure communication channels to the emergency support centre and to off-site emergency response organizations.

The SCR shall allow for extended shift operating periods.

8.10.3 Emergency Support Centre

The design shall provide for an emergency support centre that is separate from the plant control rooms, for use by the emergency support staff in the event of an emergency.

The design of the emergency support centre shall ensure that appropriate lighting levels and thermal environment are maintained, and that noise levels are minimized to acceptable standards and codes.

The emergency support centre shall be equipped with a safety parameter display system that is similar to that in the MCR.

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 emergency support centre.

The emergency support centre shall be provided with secure means of communication with the main control room, the secondary control room, and other important points in the plant, and with the on-site and off-site emergency response organizations.

The emergency support centre shall be designed to withstand all design basis external events, and shall be seismically qualified to design basis earthquake levels.

The design shall ensure that the emergency support centre:

1. Includes provisions to protect occupants, over protracted periods, from the hazards resulting from a severe accident; and
2. Is equipped with adequate facilities to allow extended operating periods.

8.10.4 Equipment Requirements for Accident Conditions

If operator action is required for actuation of any safety system or safety support system equipment, all of the following requirements must be met:

1. There shall be clear, well-defined, validated, and readily available operating procedures that identify the necessary actions;
2. There shall be 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 main control room, there shall be a minimum of 15 minutes available before the operator action is required; and
4. Following indication of the necessity for operator action outside the main control room, there shall be a minimum of 30 minutes available before the operator action is required.

The design shall be such that all necessary safety systems actions that are initiated by automatic control logic in response to an accident can also be initiated manually from the appropriate control room.

8.11 Waste Treatment and Control

The design shall include provisions to treat liquid and gaseous effluents to keep the quantities and concentrations of discharged contaminants within prescribed limits, and to support application of the ALARA principle.

The design shall also include adequate provision for the safe on-site handling and storage of radioactive and non-radioactive wastes for a period of time consistent with options for off-site management or disposal.

8.11.1 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.

The design shall include a liquid waste management system of sufficient capacity to collect, hold, mix, pump, test, treat, and sample liquid waste before discharge. The design shall consider expected waste and accidental spills or discharges.

8.11.2 Control of Airborne Material

The design shall include gaseous waste management systems with the capacity to:

1. Control all gaseous contaminants so as to conform to the ALARA principle and ensure that concentrations remain within prescribed limits;
2. Collect all potentially active gases, vapours, and airborne particulates for monitoring;
3. Pass all potentially active gases, vapours, and airborne particulates through pre, absolute, charcoal and/or high efficiency particulate Air (HEPA) filters where applicable; and
4. An off-gas system of sufficient capacity to delay the releases of potential sources of noble gases.

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, the ALARA principle being applied in normal operation; and
4. Ventilating rooms containing inert or noxious gases without impairing the capability to control radioactive releases.

8.11.3 Control of Radioactive Gaseous Releases to the Environment

The ventilation system shall be provided with filtration that will:

1. Control the release of gaseous contaminants and hazardous substances to the environment;
2. Ensure conformation to the ALARA principle; and
3. Maintain airborne contaminants within prescribed limits.

The filtration system shall be sufficiently reliable that the necessary retention factors are achieved under the expected prevailing conditions, and shall be designed in a manner that facilitates appropriate efficiency testing.

8.12 Fuel Handling and Storage

8.12.1 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 by
    a) maintaining an approved sub-criticality margin by physical means or processes, preferably by the use of geometrically safe configurations, under both normal and credible abnormal conditions,
    b) minimizing on-site consequences of postulated criticality accident to the personnel, and
    c) mitigating off-site consequences of postulated criticality accident;
2. Permit appropriate maintenance, periodic inspection, and testing of components important to safety;
3. Permit inspection of new fuel;
4. Prevent loss of or damage to the fuel; and
5. Meet Canada's international non-proliferation and safeguards requirements for recording and reporting accountancy data related to fuel containing fissile material.

8.12.2 Handling and Storage of Irradiated Fuel

The design of the handling and storage systems for irradiated fuel shall:

1. Ensure nuclear criticality safety by
    a) maintaining an approved sub-criticality margin by physical means or processes, preferably by the use of geometrically safe configurations, under both normal and credible abnormal conditions,
    b) minimizing on-site consequences of postulated criticality accident to the personnel, and
    c) mitigating off-site consequences of postulated criticality accident;
2. Permit adequate heat removal under normal operational states and DBAs;
3. Permit inspection of irradiated fuel;
4. Permit periodic inspection and testing of components important to safety;
5. Prevent the dropping of used 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 the 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. Adequately identify 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 adequate operating and accounting procedures are implemented to prevent loss of fuel; and
14. Meet Canada's international non-proliferation and safeguards requirements with respect to recording and reporting accountancy data for irradiated fuel containing fissile material.

A design for a water pool used for fuel storage shall include provisions to:

1. Control the chemistry and activity of any water in which irradiated fuel is handled or stored;
2. Monitor and control the water level in the fuel storage pool and detect leakage; and
3. Prevent the pool from emptying in the event of a pipe break.

8.12.3 Detection of Failed Fuel

The design shall provide the means to allow reliable and prompt detection of fuel defects in the reactor. Such means shall facilitate the location and removal of failed fuel to control the release of radioactive fission products into the reactor coolant.

8.13 Radiation Protection

Suitable provision shall be made in the design and layout of the plant to minimize exposure and contamination from all sources. This includes the adequate design of structures, systems, and components to:

1. Control access to the plant;
2. Minimize exposure during maintenance and inspection;
3. Shield from direct and scattered radiation;
4. Ventilate and filter for the control of 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; and
8. Provide suitable decontamination facilities.

8.13.1 Design for Radiation Protection

The shielding design shall prevent radiation levels in operating areas from exceeding the prescribed limits.

The design shall provide appropriate permanent layout and shielding of structures, systems, and components containing radioactive materials, and shall support 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.

The design shall account for frequently occupied locations, and shall support the need for human access to locations and equipment.

The design shall seek to limit the amount of activated material—a full account shall be taken of the potential build-up of radiation levels in areas of personnel occupancy.

Access routes shall be shielded where needed.

The design shall enable operator access for actions credited for post-accident conditions.

Adequate protection against exposure to radiation and radioactive contamination in accident conditions shall be provided in those parts of the facility to which access is required.

8.13.2 Access/Movement Control

The plant layout and procedures shall control access to radiation areas and areas of potential contamination.

The plant design shall minimize the movement of radioactive materials and the spread of contamination.

The design shall provide appropriate decontamination facilities for personnel.

8.13.3 Monitoring

Equipment shall be provided to ensure that there is adequate radiation monitoring in normal operational states and DBAs.

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 certain periods of time;
3. To indicate the general radiation level at appropriate locations in the event of design basis accidents and, as practicable, severe accidents; and
4. To give sufficient information in the control room or at the appropriate control position that plant personnel can 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 be such as to necessitate protective measures; and
3. To give an indication in the control room, or other appropriate locations, when a high concentration of radionuclides is detected

Facilities shall be provided for monitoring of 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.

8.13.4 Sources

The design shall provide for:

1. Appropriate disposal of radioactive materials, either to on-site 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; and
6. Minimization of radioactive waste generation.

8.13.5 Monitoring Environmental Impact

The design shall provide for determining the radiological impact on 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 materials in the environment; and
4. The possibility of any unauthorized discharge routes.

9.0 SAFETY ANALYSIS

9.1 General

A safety analysis of the plant design shall be carried out using hazards analysis, deterministic safety analysis, and probabilistic safety assessment. The safety analysis shall demonstrate achievement of all levels of defence-in-depth, and that the design is capable of meeting the applicable requirements, dose acceptance criteria, and safety goals.

The first step of each part of the safety analysis shall be to systematically identify postulated initiating events (PIE). This shall be done in a systematic manner such as that defined by the failure modes and effects analysis methodology. PIE identification shall consider both direct and indirect events.

9.2 Analysis Steps

The safety analysis is iterative with the design process. Two reports shall be issued: a preliminary safety analysis report, and a final safety analysis report.

The preliminary safety analysis assists in the establishment of the design-basis requirements for the items important to safety, and demonstrates whether the plant design meets applicable requirements.

The final safety analysis shall:

1. Reflect the as-built plant;
2. Demonstrate that the design can withstand and effectively respond to postulated initiating events;
3. Demonstrate the effectiveness of the safety systems and safety support systems;

4. Derive the OLCs for the plant, including
    a) operational limits and set points for process and control systems, and
    b) allowable operating configurations and constraints for operational procedures;
5. Establish requirements for emergency response and accident management;
6. 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;
7. Confirm that the dose and derived acceptance criteria are met for all AOOs and DBAs; and
8. Demonstrate that all safety goals are met.

9.3 Hazards Analysis

Hazards analysis is the process of collecting and evaluating information about a facility to identify the associated hazards and determine which are significant and must be addressed. A hazards analysis shall be performed to demonstrate the ability of the design to effectively respond to credible common cause events.

As discussed in Section 9.1, above, the first step of the hazards analysis shall be to identify PIEs. The hazards analysis shall then 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—exceptions can be made only if justification is provided to support the assumption that non-qualified systems will not fail);
4. Operator actions and operating procedures for each event; and
5. Plant or operating procedure parameters for which the event is limiting.

The hazards analysis shall demonstrate that:

1. The plant design incorporates sufficient diversity and separation to cope with the credible common cause events;
2. SSCs are qualified to survive and function during and following credible common cause events, as applicable; and
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, and

d) safety-critical parameters can be monitored by the operator.

Hazards analysis reports shall include the findings of the analysis and the basis for those findings. As well they shall:

1. Include a general description of the physical characteristics of the facilities that outlines the prevention and protection systems to be provided;
2. Include the safe shutdown equipment list;
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; and
9. Define the emergency planning and coordination requirements for effective mitigation, including any necessary compensatory measures to compensate for the failure or inoperability of any active or passive protection system or feature.

9.4 Deterministic Safety Analysis

A deterministic safety analysis of the plant design shall be performed in accordance with CNSC regulatory document RD-310, *Safety Analysis for Nuclear Power Plants*.

9.5 Probabilistic Safety Assessment

A probabilistic safety assessment (PSA) shall be performed to:

1. Identify accident scenarios with the potential for significant core degradation;
2. Demonstrate that a balanced design has been achieved such that no particular feature or event makes a disproportionately large or significantly uncertain contribution to the total frequency of severe accident;
3. Provide probability assessments for the occurrence of severe core damage states and major off-site releases;

4. Identify systems for which design improvements or modifications to operating procedures could reduce the probability of severe accidents or mitigate their consequences; and
5. Assess the adequacy of plant accident management and emergency procedures.

The PSA shall be conducted in accordance with the requirements specified in CNSC regulatory standard S-294, *Probabilistic Safety Assessment for Nuclear Power Plants*.

10.0 ENVIRONMENTAL PROTECTION AND MITIGATION

10.1 Environmental Impact Estimate

The design shall make adequate provision to protect the environment and to mitigate the impact of the NPP on the environment. A review of the design shall be conducted to confirm that this provision has been met.

A systematic approach shall be used to assess the potential bio-physical environmental effects of the project on the environment, and the effects of the environment on the project.

The environmental assessment shall include consideration of potential adverse effects the environment may have on the project, including the effects of environmental condition changes on the quality and quantity of resources required for plant operation.

10.2 Release of Nuclear and Hazardous Substances

The design shall demonstrate through process, monitoring, control, prevention, and mitigation, that the releases of nuclear and hazardous substances are as low as reasonably achievable.

Through life cycle assessment, the design shall identify sources and environmental stressors and aspects of the design, operation, and decommissioning together with their possible environmental impacts on human and non-human biota, including:

1. Resource requirements, such as fuel and energy;
2. Depletion of water resources (ground and surface waters);
3. Contamination of air, soil and ground and surface waters;
4. Nuclear and hazardous substances used; and
5. Waste types (gaseous, liquid and solid) and quantity generated.

The design shall consider technological options in establishing design objectives for controlling and monitoring releases during start-up, normal operation, and shutdown, potential abnormal and emergency situations. Appropriate limits shall be included in the operational limits and conditions for the plant.

11.0 ALTERNATIVE APPROACHES

The expectations in this regulatory document are intended to be, to the extent practicable, technology neutral. It is recognized that specific technologies may use alternative approaches.

The Commission will consider alternative approaches to the expectations in this document where there are special circumstances. Such circumstances include, but are not limited to, the following:

1. The alternative approach would result in an equivalent level of safety;
2. Application of the requirement conflicts with other rules or requirements;
3. Application of the requirement would not serve the underlying purpose, or is not necessary to achieve the underlying purpose; or
4. Compliance would result in undue hardship or other costs that are significantly in excess of those contemplated when the regulatory document was adopted.

Any such alternative approaches shall demonstrate equivalence to the outcomes associated with the use of the expectations here, and such a demonstration will be examined in greater depth by the Commission to gain such an assurance.

GLOSSARY

Accident/Accident Condition
An abnormal situation that may increase the risk of harm to the health and safety of persons or the environment.

Actuation parameter (also trip parameter) set point
Parameter value that triggers activation of a safety or complementary design system.

ALARA (as low as reasonably achievable)
Principle related to the determination of the level of protection and safety at which levels of individual or collective potential exposures shall be kept "as low as reasonably achievable," economic and social factors being taken into account.

AOO (anticipated operational occurrence)
An operational process that deviates from normal operation without exceeding safety limits to result in an accident condition. AOO includes all postulated initiating events with frequencies of occurrence greater than 10^{-2} per year.

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

(BDBA) Beyond design basis accident
An accident less frequent and more severe than a design basis accident (DBA).

Common cause event
An event in which multiple systems, components, structures, or procedures are affected by a single cause.

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

Complementary design features

Design features introduced to address beyond design basis accidents, including severe accidents.

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

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

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

Crediting
Acknowledgment that something is responsible for causing an action.

CSA
Canadian Standards Association.

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

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

DBE (design basis earthquake)
An engineering representation of the potentially severe effects of earthquakes that have sufficiently low probability of being exceeded during the life of the plant.

Design basis threat
A set of malevolent acts considered possible by the CNSC.

Diversity
The principle that requires two or more systems or components serving the same or similar purpose to be functionally different in design and/or operation.

Exclusion area (exclusion zone)
A parcel of land within or surrounding a nuclear facility on which there is no permanent dwelling and over which a licensee has the legal authority to exercise control

Environment
The components of the Earth, including:

1. Land, water, and air , including all layers of the atmosphere;

2. All organic and inorganic matter and living organisms; and

3. Interacting natural systems that include components referred to above.

External event
Any event that proceeds from the environment external to NPP, and can cause failure of plant's SSC.
Note: External events include, but are not limited to, earthquakes, floods, and hurricanes.

Fail-Safe Design
Design whose most probable failure modes do not result in a reduction of safety.

Fire
A fire or explosion initiating event or event sequences.

(GSS) Guaranteed Shutdown state
A set of conditions that provide sufficient guarantee that the reactor will remain in the shutdown state despite any credible failure

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

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

Independent systems
Systems that do not share any components among each other.

Internal event
An event internal to NPP, which is a result of human error or failure in a system, structure or component.

Item important to safety
An item that is part of a safety group and/or whose malfunction or failure could lead to personal injury or unnecessary exposure to ionizing radiation to the site personnel or members of the public.

Jet impact
Refers to the potential internal hazard associated high pressure steam released from a pressure-retaining component.

Missile generation
The internal hazard associated with the sudden high speed propulsion of debris.

Mission time
The duration of time within which a system or component is required to operate or be available to operate and fulfill its function, following some event, such as an initiating event or upset event.

Nuclear power plant (NPP, plant)
Any fission reactor installation constructed to generate electricity on a commercial scale. A nuclear power plant is a Class IA nuclear facility, as defined in the *Class I Nuclear Facilities Regulations*.

Normal operation
Operation within specified operational limits and conditions.

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

Plant state
A configuration of NPP components, including the physical and thermodynamic states of the materials and the process fluids in them.
Note: For the purpose of this document a plant is said to be in one of the following states: normal operation, anticipated operational occurrence, design basis accident, or beyond design basis accident (severe accidents are a subset of the beyond design basis states).

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

(At) Power
A plant state characterized by the reactor being critical and producing power, with automatic actuation of safety systems not blocked and with essential support systems aligned in their normal power configuration.

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

Pressure boundary
A boundary of any pressure-retaining vessel, system or component of a nuclear or non-nuclear system, where the vessel, system or component is registered, or eligible for registration, under boiler or pressure vessel legislation.

Probabilistic safety assessment (PSA)
A comprehensive and integrated assessment of the safety of the NPP or reactor that, by considering the initial plant state and the probability, progression, and consequences of equipment failures and operator response, derives numerical estimates of a consistent measure of the safety of the NPP or reactor. Such assessments are most useful in assessing the relative level of safety.

Process
Set of interrelated activities that transform inputs into outputs.

Process system
Systems whose primary function is to support (or contribute to) the production of either steam or electricity.

Proven design
A design of a component(s) can be proven either by showing compliance with accepted engineering standards, or by a history of experience, or by test, or some combination of these. New component(s) are 'proven' by performing a number of acceptance and demonstration tests that show the component(s) meets pre-defined criteria.

Residual heat
The sum of heat originating from radioactive decay and the fission in the fuel in the shutdown state, and the heat stored in reactor related structures, systems and components.

Risk-informed decision making
Application of probabilistic risk assessment to make decisions about nuclear safety in a manner that complements the deterministic approach and supports the defence-in-depth philosophy. The quantitative estimate of risk (based on probability and consequences) is considered in the light of the degree of confidence not only in the assessment of probabilities but also in the analysis methodology and the underlying knowledge base used to predict the consequences. Where the level of uncertainty is high either in the estimate of probability or in the knowledge base, more weight is given to the deterministic approach.

Risk significant system
Any system of the plant that, if it fails to meet its design and performance specifications, could result in unreasonable risk to the health and safety of persons, to national security or to the environment.

SAMG
Severe Accident Management Guidelines

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

Structures are the passive elements: buildings, vessels, shielding, etc. A system comprises several components, assembled in such a way as to perform a specific (active) function. A component is a discrete element of a *system*. Examples are wires, transistors, integrated circuits, motors, relays, solenoids, pipes, fittings, pumps, tanks and valves.

Safeguards
NPP design features that reflect obligations arising from the Safeguards Agreements between Canada and the International Atomic Energy Agency.

Safety analysis:
Analysis by means of appropriate analytical tools that establishes and confirms the design basis for the items important to safety; and ensures that the overall plant design is capable of meeting the acceptance criteria for each plant state.

Safety group
Assembly of structures, systems and components designated to perform all actions required for a particular postulated initiating event to ensure that the specified limits for AOOs and DBAs are not exceeded. It may include certain safety and safety support systems, and safety related or any interacting process system.

Safety related system
Systems and components and structures thereof, which by virtue of failure to perform in accordance with the design intent, have the potential to impact on the radiological safety of the public or plant personnel from the operation of the NPP. Those systems, and the components and structures thereof, are associated with:

(1) Regulating (including controlled start-up and shutdown) and cooling of the reactor core under normal conditions (including all normal operating and shutdown conditions)

(2) Regulating, shutdown, and cooling of the reactor core under anticipated transient conditions, accident conditions, and the maintenance of the reactor core in a safe shutdown state for an extended period following such conditions; and

(3) Limiting the release of radioactive material and the exposure of plant personnel and/or the public to meet the criteria established by the licensing authority with respect to radiation exposure during and following normal, anticipated transient conditions and accident conditions.

Safety support systems
Systems designed to support the operation of safety systems.

Safety systems
Systems designed for the sole purpose of limiting or mitigating the accidents for which the Operational Limits and Conditions may be exceeded.

Severe accident:
A beyond design basis accident that involves significant core degradation.

Severe threat:
A credible threat of a malevolent act that is more severe than the Design Basis Threat.

Single failure
A single failure in a structure, system or component that results in the loss of its capability to perform its intended safety function(s); also included in the single failure is any consequential failure(s) that may result from it.

Single failure criterion
A criterion or requirement applied to a system such that it must be capable of performing its task in the presence of any single failure.

Site design earthquake
An engineering representation of the effects of possible earthquakes with an occurrence rate, based on historical records, not greater than 0.01 per year.

Severe core damage
Accident conditions more severe than a design DBA and involving significant core degradation.

Shutdown state
Plant state characterized by sub-criticality of reactor.
Note: At shutdown, automatic actuation of safety systems could be blocked and support systems may remain in abnormal configurations.

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

Structures are the passive elements: buildings, vessels, shielding, etc. A system comprises several components, assembled in such a way as to perform a specific (active) function. A component is a discrete element of a *system*. Examples are wires, transistors, integrated circuits, motors, relays, solenoids, pipes, fittings, pumps, tanks and valves.

Trip Parameter (Actuation Parameter)
Parameter value beyond which activation of a safety or complementary design system is triggered.

Ultimate Heat Sink
A medium to which the residual heat can always be transferred, even if all other means of removing the heat have been lost or are insufficient. This medium is normally a body of water or the atmosphere.

ASSOCIATED DOCUMENTS

The following CNSC regulatory documents could be adapted or adopted to support the solution being proposed by the current document:

1. P-325, *Nuclear Emergency Management*;
2. G-144, *Trip Parameter Acceptance Criteria for the Safety Analysis of CANDU Nuclear Power Plants*;
3. R-52, *Design Guide for Basic and Intermediate Level Radioisotope Laboratories*;
4. R-9, *Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants*;
5. R-8, *Requirements for Shutdown Systems for CANDU Nuclear Power Plants*;
6. R-7, *Requirements for Containment Systems for CANDU Nuclear Power Plants*;
7. R-77, *Overpressure Protection Requirements for Primary Heat Transport Systems in CANDU Power Reactors Fitted with Two Shutdown Systems*;
8. R-10, *The Use of Two Shutdown Systems in Reactors*;
9. S-98 rev 1, *Reliability Programs for Nuclear Power Plants*;
10. S-294, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*;
11. G-306, *Severe Accident Management Programs for Nuclear Reactors*;
12. G-205, *Entry to Protected and Inner Areas*;
13. G-225, *Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills*;
14. RD-310, *Safety Analysis for Nuclear Power Plants.*