Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Regulatory Document

RD–337

Design of New Nuclear Power Plants

November 2008

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.

Regulatory Document

RD–337

DESIGN OF NEW NUCLEAR POWER PLANTS

Published by the
Canadian Nuclear Safety Commission
November 2008

Design of New Nuclear Power Plants

Regulatory Document RD–337

Published by the Canadian Nuclear Safety Commission

Catalogue number CC173-3/4-337E-PDF
ISBN 978-1-100-10645-8

Ce document est également disponible en français sous le titre *Conceptions des nouvelles centrales nucléaires*.

Document availability

The document is available in English or French on the CNSC Web site at www.nuclearsafety.gc.ca. A paper copy of the document in either official language can be ordered from:

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

Telephone: 613-995-5894 or 1-800-668-5284 (Canada only)
Facsimile: 613-992-2915
E-mail: info@cnsc-ccsn.gc.ca

PREFACE

This regulatory document sets out the expectations of the Canadian Nuclear Safety Commission (CNSC) concerning the design of new water-cooled nuclear power plants (NPPs or plants). It establishes a set of comprehensive design expectations that are risk-informed and align with accepted international codes and practices.

This document provides criteria pertaining to the safe design of new water-cooled NPPs, and offers examples of optimal design characteristics where applicable. All aspects of the design are taken into account, and multiple levels of defence are promoted in design considerations.

To the extent practicable, the guidance provided herein is technology-neutral with respect to water-cooled reactors.

RD-337 represents the CNSC's adoption of the principles set forth by the International Atomic Energy Agency (IAEA) in NS-R-1, *Safety of Nuclear Plants: Design*, and the adaptation of those principles to align with Canadian expectations. The scope of RD-337 goes beyond IAEA's NS-R-1 to address the interfaces between NPP design and other topics, such as environmental protection, radiation protection, ageing, human factors, security, safeguards, transportation, and accident and emergency response planning.

Similar to NS-R-1, RD-337 considers all licensing phases, because information from the design process feeds into the processes for reviewing an application for a *Licence to Construct* an NPP, and other licence applications.

Nothing contained in this document is to be construed as relieving any applicant or licensee from requirements associated with conventional codes and standards. In particular, while RD-337 may assist a proponent in making a licence application, it is the licensee's responsibility to identify and comply with all applicable regulations and licence conditions.

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 water-cooled nuclear power plants (NPPs or plants).

2.0 SCOPE

This document sets out CNSC expectations with respect to the design of new water-cooled NPPs, and provides examples of optimal design characteristics. All aspects of the design are taken into account, and multiple levels of defence are promoted in design considerations.

The information provided herein is intended to facilitate high quality design, and consistency with modern international codes and standards, for new water-cooled NPPs. It is recognized that specific technologies may use alternative approaches. If a design other than a water-cooled reactor is to be considered for licensing in Canada, the design is subject to the safety objectives, high level safety concepts and safety management expectations associated with this regulatory document. However, CNSC review of such a design will be undertaken on a case by case basis.

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

To the extent practicable, this document is technology-neutral with respect to water-cooled reactors, and includes direction concerning:

1. Establishing the safety goals and objectives for the design;
2. Utilizing safety principles in the design;
3. Applying safety management principles;
4. Designing systems, structures, and components;
5. Interfacing engineering aspects, plant features, facility layout; and
6. Integrating safety assessments into the design process.

To a large degree, this document represents the CNSC's adoption of the principles set forth in International Atomic Energy Agency (IAEA) document NS-R-1, *Safety of Nuclear Plants: Design*, and the adaptation of those principles to align with Canadian practices. The scope of NS-R-1 has been expanded to address the interfaces between NPP design and other topics, such as environmental protection, radiation protection, ageing, human factors, security, safeguards, transportation, and accident and emergency response planning.

3.0 RELEVANT REQUIREMENTS

The provisions of the *Nuclear Safety and Control Act* (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 (*a*) is qualified to carry on the activity that the licence will authorize the licensee to carry on; and (*b*) will, in carrying on that activity, makes adequate provision for the protection of the environment, the health and safety of persons and the maintenance of national security and measures required to implement international obligations to which Canada has agreed";
2. Subsection 24(5) of the NSCA authorizes the Commission to include in a licence any term or condition that the Commission considers necessary for the purposes of the NSCA;
3. Paragraph 3(1)(*i*) of the *General Nuclear Safety and Control Regulations* stipulates that an application for a licence shall contain, in addition to other information, "…a description and the results of any test, analysis or calculation performed to substantiate the information included in the application";
4. Paragraph 12(1)(*f*) of the *General Nuclear Safety and Control Regulations* stipulates that every licensee shall, "…take all reasonable precautions to control the release of radioactive nuclear substances or hazardous substances within the site of the licensed activity and into the environment as a result of the licensed activity";
5. 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…";
6. 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…";
7. 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 and the measures that will be taken to prevent or mitigate those effects"; and
8. Other sections of the *Class I Nuclear Facilities Regulations*, as well as sections of the *Radiation Protection Regulations* and the *Nuclear Security Regulations* that pertain to the design of a new nuclear power plant.

4.0 SAFETY OBJECTIVES AND CONCEPTS

4.1 General Nuclear Safety Objective

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

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

4.1.1 Radiation Protection Objective

The radiation protection objective is to provide that during normal operation, or during anticipated operational occurrences, 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 provides for the mitigation of the radiological consequences of any accidents.

4.1.2 Technical Safety Objectives

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

With achievement of these objectives, any radiological consequences should be minor and below prescribed limits, and the likelihood of accidents with serious radiological consequences is expected to be extremely low.

4.2 Application of the Technical Safety Objectives

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

1. Dose acceptance criteria for events within the design basis; and
2. Safety goals for beyond design basis accidents.

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

4.2.1 Dose Acceptance Criteria

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

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

1. 0.5 millisievert for any anticipated operational occurrence (AOO); or
2. 20 millisieverts for any design basis accident (DBA).

4.2.2 Safety Goals

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 are 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 are comparable to or less than the risks of generating electricity by viable competing technologies, and should not significantly add to other societal risks.

Quantitative Application of the Safety Goals

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

1. Core damage frequency;
2. Small release frequency; and
3. Large release frequency.

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

Small release frequency and large release frequency are measures of the plant's accident mitigative capabilities. They also represent measures of risk to society and to the environment due to the operation of a nuclear power plant.

Core Damage Frequency

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

Small Release Frequency

The sum of frequencies of all event sequences that can lead to a release to the environment of more than 10^{15} becquerel of iodine-131 is less than 10^{-5} per reactor year. A greater release may require temporary evacuation of the local population.

Large Release Frequency

The sum of frequencies of all event sequences that can lead to a release to the environment of more than 10^{14} becquerel of cesium-137 is less than 10^{-6} per reactor year. A greater release may require long term relocation of the local population.

4.2.3 Safety Analyses

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

The safety analyses examine plant performance for:

1. Normal operation;
2. Anticipated operational occurrences;
3. Design basis accidents; and
4. Beyond design basis accidents (BDBAs), including event sequences that may lead to a severe accident.

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

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

4.2.4 Accident Mitigation and Management

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

This includes such measures as:

1. Consideration of inherent safety features;
2. Incorporation of engineered design features;
3. Establishment by the operating organization of on-site accident management procedures; and
4. Establishment of off-site intervention measures by appropriate authorities.

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

4.3 Safety Concepts

4.3.1 Defence-in-depth

The concept of defence-in-depth is applied to all organizational, behavioural, and design-related safety and security activities to ensure that they are subject to overlapping provisions. With the defence-in-depth approach, if a failure were to occur it will be detected and compensation made, or it would be corrected.

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

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

Level One

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).

Level Two

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

Level Three

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

Level Four

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

Level Five

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

4.3.2 Consideration of Physical Barriers

An important aspect of implementing defence-in-depth in the NPP design is the provision of a series of physical barriers to confine radioactive material at specified locations.

4.3.3 Operational Limits and Conditions

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

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

Safe operation depends on personnel as well as equipment. OLCs therefore typically include:

1. Control system constraints and procedural constraints on important process variables;
2. Requirements for normal operation and AOOs, including shutdown states;
3. Actions to be taken and limitations to be observed by operating personnel;
4. Principal requirements for surveillance and corrective or compensatory actions; and

5. The limitations to be observed and the operational requirements to be met by SSCs in order that their intended functions, as assumed in the safety analysis, can be met.

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

5.0 SAFETY MANAGEMENT DURING DESIGN

The NPP design:

1. Meets Canadian regulatory requirements;
2. Meets the design specifications, as confirmed by safety analysis;
3. Takes account of current safety practices;
4. Fulfills the requirements of an effective quality assurance program; and
5. Incorporates only those design changes that have been justified by technical and safety assessments.

The design process is carried out by technically qualified and appropriately trained staff at all levels, and includes such management arrangements as:

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

5.1 Design Authority

During the design phase, formal design authority typically rests with the organization that has overall responsibility for the design. Prior to plant start-up, this authority 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 need to be established in formal documentation; however, the overall responsibility remains with the design authority.

The applicant confirms that the design authority has achieved the following objectives during the design phase:

1. Established a knowledge base of all relevant aspects of the plant design and kept it up-to-date, while taking experience and research findings into account;
2. Ensured the availability of the design information that is needed for safe plant operation and maintenance;
3. Established the requisite security clearances and associated security measures to protect prescribed, designated, and classified material;
4. Maintained design configuration control;
5. Reviewed, verified, approved (or rejected), and documented design changes;
6. Established and controlled the necessary interfaces with responsible designers or other suppliers engaged in design work;
7. Ensured that the necessary engineering and scientific skills and knowledge have been maintained; and
8. Ensured that, with respect to individual design changes or multiple changes that may have significant interdependencies, the associated impact on safety has been properly assessed and understood.

5.2 Design Management

Appropriate design management is expected to achieve the following objectives:

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

5.3 Quality Assurance Program

A quality assurance program is established as part of the overall management arrangements by which the plant will function to achieve objectives. With respect to the plant design, this includes identifying all performance and assessment parameters for the design, as well as detailed plans for each SSC to ensure consistent quality of the design and the selected components.

The quality assurance program is such that the initial design, and any subsequent change or safety improvement, is carried out in accordance with established procedures that call on appropriate standards and codes, and that incorporate applicable requirements and design bases. Appropriate quality assurance also facilitates identification and control of design interfaces.

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

5.4 Proven Engineering Practices

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

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

SSCs important to safety are of proven designs, and are designed according to the standards and codes identified for the NPP.

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

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

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

5.5 Operational Experience and Safety Research

The NPP design draws on operational experience that has been gained in the nuclear industry, and on the results of relevant research programs.

5.6 Safety Assessment

Safety assessment is a systematic process applied throughout the design phase to ensure that the design meets all relevant safety requirements. This includes the requirements set by the operating organization and by regulatory authorities. The basis for the safety assessment is the data derived from the safety analysis, previous operational experience, results of supporting research, and proven engineering practices.

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

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

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

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

5.7 Design Documentation

The design documentation includes the following information:

1. Design description;
2. Design requirements;
3. System classifications;
4. Description of plant states;
5. Security system design, including a description of physical security barriers;
6. Operational limits and conditions;
7. Identification and categorization of initiating events;
8. Acceptance criteria and derived acceptance criteria;
9. Deterministic safety analysis;
10. Probabilistic safety assessment (PSA); and
11. Hazards analysis.

6.0 SAFETY CONSIDERATIONS

6.1 Application of Defence-in-depth

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

Level One

Achievement of defence-in-depth level one calls for conservative design and high-quality construction to provide confidence that plant failures and deviations from normal operations are minimized and accidents are prevented.

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

Level Two

Defence-in-depth level two is achieved by controlling plant behaviour during and following a PIE using both inherent and engineered design features to minimize or exclude uncontrolled transients to the extent possible.

Level Three

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

Level Four

Defence-in-depth level four is achieved by providing equipment and procedures to manage accidents and mitigate their consequences as far as practicable.

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

Level Five

The design provides an adequately equipped emergency support centre, and plans for on-site and off-site emergency response.

6.1.1 Consideration of Physical Barriers

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

To the extent practicable, the design therefore prevents:

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 also allows 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 defence level.

6.2 Safety Functions

The NPP design provides 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 DBA, and in accident conditions beyond DBAs.

The following fundamental safety functions are available in normal operation, and during and following AOOs and DBAs:

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.

The above functions also facilitate response to BDBAs to the extent practicable.

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

6.3 Accident Prevention and Plant Safety Characteristics

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

1. Inherent safety features;
2. Passive safety features, or action of control systems;
3. Action of safety systems; or
4. Specified procedural actions.

6.4 Radiation Protection and Acceptance Criteria

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

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

The design includes provisions for the prevention and mitigation of radiation exposures resulting from DBAs and BDBAs.

The design also ensures that potential radiation doses to the public from AOOs and DBAs do not exceed dose acceptance criteria provided in subsection 4.2.1. The calculated overall risk to the public from all plant states meets the safety goals in subsection 4.2.2.

6.5 Exclusion Zone

The design includes adequate provision 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 takes into account the interfaces between the safety and security provisions of the NPP and other aspects of the facility layout, such as:

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

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

7.0 GENERAL DESIGN CONSIDERATIONS

7.1 Classification of SSCs

The design authority classifies SSCs in a consistent and clearly defined classification scheme. The SSCs are then designed, constructed, and maintained such that their quality and reliability is commensurate with this classification.

In addition, all SSCs are identified as either important or not important to safety. The criteria for determining safety importance are based on:

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

SSCs important to safety include:

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

The design provides appropriately designed interfaces between SSCs of different classes to minimize the risk of an SSC less important to safety from adversely affecting the function or reliability of an SSC of greater importance.

7.2 Plant Design Envelope

The design authority establishes the plant design envelope, which comprises the design basis and complementary design features.

The design basis specifies the capabilities that are necessary for the plant in normal operation, AOOs, and DBAs.

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

Complementary design features address the performance of the plant in BDBAs, including selected severe accidents.

7.3 Plant States

Plant states are grouped into the following four categories:

1. *Normal Operation*—operation within specified OLCs, including start-up, power operation, shutting down, shutdown, maintenance, testing, and refuelling;
2. *Anticipated Operational Occurrence*—a deviation 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 Accidents*—accident conditions for which an NPP is designed according to established design criteria, and for which damage to the fuel and the release of radioactive material are kept within regulated limits; and
4. *Beyond Design Basis Accidents*—accident conditions less frequent and more severe than a design basis accident. A BDBA may or may not involve core degradation.

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

7.3.1 Normal Operation

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

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

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

1. Limits important to safety;
2. Constraints on control systems and procedures;
3. Plant maintenance, testing, and inspection requirements to ensure that SSCs function as intended, taking the ALARA principle into consideration; and
4. Clearly defined operating configurations, such as start-up, power production, shutdown, maintenance, testing, surveillance, and refuelling—these configurations 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, form the basis for establishing the OLCs according to which the plant will be authorized to operate, as discussed in subsection 4.3.3 of this document.

7.3.2 Anticipated Operational Occurrences

The design includes provisions such that releases to the public following an AOO do not exceed the dose acceptance criteria.

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

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

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

7.3.3 Design Basis Accidents

The set of design basis accidents sets the boundary conditions according to which SSCs important to safety are designed.

The design is such that releases to the public following a DBA will not exceed the dose acceptance criteria.

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

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

The design takes 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 are facilitated by the provision of adequate instrumentation to monitor plant status, and controls for manual operation of equipment.

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

7.3.4 Beyond Design Basis Accidents

The design authority identifies credible BDBAs, based on operational experience, engineering judgment, and the results of analysis and research. This includes events leading to significant core degradation (severe accidents), particularly those events that challenge containment.

Complementary design features are then considered with the goal of preventing identified BDBA scenarios, and mitigating their consequences if they do occur.

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

The design identifies the rules and practices that have been 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 design identifies a radiological and combustible gas accident source term for use in the specification of the complementary design features for BDBAs. This source term is referred to as the reference source term, and is based on a set of representative core damage accidents established by the design authority.

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

To the extent practicable, the design provides biological shielding of appropriate composition and thickness to protect operational personnel during BDBAs, including severe accidents.

Severe Accidents

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

Early in the design process, the various potential barriers to core degradation are identified, and features that can be incorporated to halt core degradation at those barriers are considered.

The design also identifies the equipment to be used in the management of severe accidents. A reasonable level of confidence that this equipment will perform as intended in the case of a severe accident is demonstrated by environmental, fire, and seismic assessments.

Particular attention is placed on the prevention of potential containment bypass in accidents involving significant core degradation.

Consideration is 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 applies to any system that can be shown with a reasonable degree of assurance to be able to function in the environmental conditions expected during a severe accident.

Containment maintains its role as a leak-tight barrier for a period that allows sufficient time for the implementation of off-site emergency procedures following the onset of core damage. Containment also prevents uncontrolled releases of radioactivity after this period.

The design authority establishes initial severe accident management guidelines, taking into account the plant design features and the understanding of accident progression and associated phenomena.

The design considers prevention of recriticality following severe accidents.

7.4 Postulated Initiating Events Considered in the Design

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

7.4.1 Internal Hazards

SSCs important to safety are designed and located in a manner that minimizes the probability and effects of fires and explosions caused by external or internal events.

The plant design takes 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 are provided to ensure that nuclear safety is not compromised.

The design considers the possible interaction of external and internal events, such as external events initiating internal fires or floods that may lead to the generation of missiles.

Where two fluid systems operating at different pressures are interconnected, failure of the interconnection is considered. Either both withstand the higher pressure, or provision is made so that the pressure of the system operating at the lower pressure will not be exceeded.

7.4.2 External Hazards

The design considers all natural and human-induced external events that may be linked with significant radiological risk. The subset of external events that the plant is designed to withstand is selected, and design basis events are determined from this subset.

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

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

7.4.3 Combinations of Events

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

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

7.5 Design Rules and Limits

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

The design also identifies SSCs to which design limits are applicable. These design limits are specified for normal operation, AOOs, and DBAs.

7.6 Design for Reliability

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

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

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

The reliability model for each system uses realistic failure criteria and best estimate failure rates, considering the anticipated demand on the system from PIEs.

Design for reliability includes consideration of mission times for SSCs important to safety.

The design takes 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 external emergency response services.

7.6.1 Common-cause Failures

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

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

The design provides sufficient physical separation between redundant divisions of safety support systems and process systems. This applies to equipment and to routing of the following items:

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

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

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

1. A safety system designed to act as backup is not 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 associated safety functions are also provided by another safety system to counter the possibility of failures in the process system.

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

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

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

7.6.2 Single Failure Criterion

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

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

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

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

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

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

Exemptions for passive components apply only to those components that are designed and manufactured to high standards of quality, that are adequately inspected and maintained in service, and that remain unaffected by the PIE. Design documentation includes analytical justification of such exemptions, taking loads and environmental conditions into account, as well as the total period of time after the PIE for which the functioning of the component is necessary.

Check valves are active components if they must change state following a PIE.

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

7.6.3 Fail-safe Design

The principle of fail-safe design is applied to the design of SSCs important to safety. To the greatest extent practicable, application of this principle enables plant systems to pass into a safe state if a system or component fails, with no necessity for any action to be taken.

7.6.4 Allowance for Equipment Outages

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

The design considers the time allowed for each equipment outage and the respective response actions.

7.6.5 Shared Systems

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

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

Shared Instrumentation for Safety Systems

Instrumentation is not typically shared between safety systems.

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

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

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

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

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

1. Sharing is 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 is electrically isolated so that failures cannot be propagated from one system to the other; and
3. Isolation devices between systems of different safety importance are always associated with the system classified as being of greater importance to safety.

Sharing of SSCs between Reactors

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

In exceptional cases when SSCs are shared between two or more reactors, such sharing excludes safety systems and turbine generator buildings that contain high-pressure steam and feedwater systems.

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

1. All safety requirements are met for all reactors during normal operation, AOOs, and DBAs; and
2. In the event of an accident involving one of the reactors, orderly shutdown, cool down, and removal of residual heat is achievable for the other reactor(s).

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

7.7 Pressure-retaining SSCs

All pressure-retaining SSCs are protected against overpressure conditions, and are classified, designed, fabricated, erected, inspected, and tested in accordance with established standards.

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

The design minimizes the likelihood of flaws in pressure boundaries. This includes timely detection of flaws in pressure boundaries important to safety in a manner that supports leak-before-break detection capability.

Unless otherwise justified, all pressure boundary SSCs are designed to withstand static and dynamic loads anticipated in normal operation, AOOs, and DBAs.

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

The operation of pressure relief devices does not lead to unacceptable releases of radioactive material from the plant.

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

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

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

7.8 Equipment Environmental Qualification

The design provides an equipment environmental qualification program. Development and implementation of this program ensures that the following functions are carried out in post-accident conditions:

1. The reactor is safely shut down and kept in a safe shutdown state during and following AOOs and DBAs;
2. Residual heat is removed from the reactor after shutdown, and also during and following AOOs and DBAs;
3. Potential for release of radioactive material from the plant is limited, and the resulting dose to the public from AOOs and DBAs is kept within prescribed limits; and
4. Post-accident conditions are monitored to indicate whether the above functions are being carried out.

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

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

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

7.9 Instrumentation and Control

7.9.1 General Considerations

The design includes provision of instrumentation 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 plant status.

This includes instrumentation for measuring variables that can affect the fission process, the integrity of the reactor core, the reactor cooling systems, and containment, as well as instrumentation for obtaining any information on the plant that is necessary for its reliable and safe operation.

The design is such that the safety systems and any necessary support systems can be reliably and independently operated, either automatically or manually, when necessary.

The design also includes the capability to trend and automatically record measurement of any derived parameters that are important to safety.

Instrumentation is adequate for measuring plant parameters for emergency response purposes.

The design includes reliable controls to maintain variables within specified operational ranges.

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

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

Various safety actions are 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 is available to the operator to confirm the safety action.

7.9.2 Use of Computer-based Systems or Equipment

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

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

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

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

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

1. Functions not essential to safety are separate from and shown not to impact the safety function;
2. The safety function is normally executed in processors separate from software that implements other functions, such as control, monitoring, and display;
3. The expectations associated with diversity apply to computer-based systems that perform similar safety functions—the choice of diversity type is justified;
4. The design incorporates fail-safe and fault tolerance features, and the additional complexity ensuing from these features results in an overall gain in safety;
5. The design provides protection against physical attack, intentional and non-intentional intrusion, fraud, viruses, and other malicious threats; and
6. The design provides for effective detection, location, and diagnosis of failures in order to facilitate timely repair or replacement of equipment or software.

7.9.3 Post-accident Instrumentation

Instrumentation and recording equipment is such that essential information is available to support plant procedures during and following accidents by:

1. Indicating plant status;
2. Identifying the locations of radioactive material;
3. Supporting estimation of quantities of radioactive material;
4. Recording vital plant parameters; and
5. Facilitating decisions in accident management.

7.10 Safety Support Systems

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

Where normal services are provided from external sources, backup safety support systems are also available on the site.

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

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

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

The emergency support systems:

1. Are independent of normal and backup systems;
2. Provide continuity of the service until long term (normal or backup) service is re-established;
3. Have a capacity margin that allows for future increases in demand; and
4. Are testable under design load conditions.

7.11 Guaranteed Shutdown State

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

The design provides two independent means of preventing recriticality from any pathway or mechanism during the GSS.

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

7.12 Fire Safety

The design of the NPP, including that of external buildings and SSCs integral to plant operation, includes provisions for fire safety.

7.12.1 General Provisions

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

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

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

Fire is considered an internal hazard. The essential safety functions are therefore available during a fire.

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

7.12.2 Safety to Life

The design provides protection to workers and the public from event sequences initiated by fire or explosion in accordance with established radiological, toxicological, and human factors criteria. With this protection:

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.

The following design provisions demonstrate that the above life safety objectives have been achieved:

1. Effective and reliable means of fire detection in all areas;
2. Effective and reliable means of emergency notification, including the nature of the emergency and protective actions to be taken;
3. Multiple and separate safe egress routes from any area;
4. Easily accessible exits;
5. Effective and reliable identification and illumination of egress routes and exits;
6. Sufficient exiting capacity for the number of workers (taking into account the emergency movement of crowds);
7. Protection of workers from fires and fire by-products (i.e., combustion products, smoke, heat, etc.) during egress and in areas of refuge;
8. Protection of workers performing plant control and mitigation functions during or following a fire;
9. Adequate supporting infrastructure (lighting, access, etc.) for workers to perform emergency response, plant control, and mitigation activities during or following a fire;
10. Sufficient structural integrity and stability of buildings and structures to ensure safety of workers and emergency responders during and after a fire; and
11. Protection of workers from the release or dispersion of hazardous substances, radioactive material, or nuclear material as a result of fire.

7.12.3 Environmental Protection and Nuclear Safety

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

7.13 Seismic Qualification

The seismic qualification of all SSCs aligns with the requirements of Canadian national—or equivalent—standards.

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

7.13.1 Seismic Design and Classification

The design authority identifies SSCs important to safety that are credited to withstand a design basis earthquake (DBE), and ensures that they are qualified accordingly. This applies to:

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

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

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

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

7.14 In-service Testing, Maintenance, Repair, Inspection, and Monitoring

In order to maintain the NPP within the boundaries of the design, the SSCs important to safety are calibrated, tested, maintained and repaired (or replaced), inspected, and monitored over the lifetime of the plant.

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

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

In cases where SSCs important to safety cannot be designed to support the desirable testing, inspection, or monitoring schedules, the following approach is taken:

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

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

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

The design also considers the needs for related testing when specifying the commissioning requirements for the plant.

7.15 Civil Structures

7.15.1 Design

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

Civil structures important to safety are 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 are considered in the design of civil structures.

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

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

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

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

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

7.15.2 Surveillance

The design enables implementation of periodic inspection programs for structures related to nuclear safety to verify as-constructed conditions.

The design also facilitates monitoring in-service for degradations that may compromise the intended design function of the structures.

In particular, the design permits monitoring of foundation settling.

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

The design facilitates routine inspection of sea, lake, and river flood defences and demonstrates fitness for service.

7.15.3 Lifting of Large Loads

The lifting of large and heavy loads, particularly those containing radioactive material, is considered in the NPP design. This includes identification of 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 therefore needs to incorporate large margins, appropriate interlocks, and other safety features to accommodate the lifting of large loads.

7.16 Commissioning

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

7.17 Ageing and Wear

The design considers the effects of ageing and wear on SSCs. For SSCs important to safety, this consideration includes:

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

7.18 Control of Foreign Material

The design provides for exclusion and removal of all foreign material and corrosion products that may have an impact on safety.

7.19 Transport and Packaging for Fuel and Radioactive Waste

NPP design incorporates appropriate features to facilitate transport and handling of new fuel, used fuel, and radioactive waste. Related considerations include facility access, as well as lifting and packaging capabilities.

7.20 Escape Routes and Means of Communication

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

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

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

The design ensures that diverse methods of communication are available within the NPP and in the immediate vicinity, and also to off-site agencies, in accordance with the emergency response plan.

7.21 Human Factors

The design includes a human factors engineering program plan.

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

Human factors considerations:

1. Reduce the likelihood of human error as far reasonably achievable;
2. Provide means for identifying the occurrence of human error, and methods by which to recover from such error; and
3. Mitigate the consequences of error.

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

Appropriate and clear distinction between the functions assigned to operating personnel and those assigned to automatic systems is facilitated by systematic consideration of human factors and the human-machine interface. This consideration continues 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, 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 are 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 is considered to have dual roles—that of a systems manager, including responsibility for accident management, and that of an equipment operator. Verification and validation activities are comprehensive, such that the design conforms to human factors design principles and meets usability requirements.

The design identifies the type of information that facilitates an operator’s ability 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 provides the type of information that enables an individual in an equipment operator role to identify the parameters associated with individual plant systems and equipment, and to confirm that the necessary safety actions can be initiated safely.

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

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

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

7.22 Robustness against Malevolent Acts

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

7.22.1 Design Principles

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

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

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

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

Consistent with the concept of defence-in-depth, the design provides multiple barriers for protection against malevolent acts, including physical protection systems, engineered safety provisions, and measures for post-event management, as appropriate. The failure of a preceding barrier should not compromise the integrity and effectiveness of subsequent barriers.

7.22.2 Design Methods

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

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

Vital areas are identified and are taken into account in the design and verification of robustness. For vital areas, the design should allow enough delay for effective intervention by the on-site or off-site response force, taking structures, detection, and assessment into account. These areas should be protected from inadvertent damage during the carrying out of defensive actions.

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

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

The design authority also develops a methodology for assessing the challenges associated with BDBTs. This methodology is applied to determine the margins available for shutdown and for containment of radioactivity. Significant degradation of engineering means may be permitted.

7.22.3 Acceptance Criteria

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

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

For more severe events there is a safe shutdown path that comprises at least one means of:

1. Reactor shutdown;
2. Fuel cooling; and
3. Retention of radioactivity from the reactor.

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

For extreme events, there is at least one means of reactor shutdown and core cooling. Degradation of the containment barrier may allow the release of radioactive material; however, the degradation should be limited with the goal that the dose acceptance criteria are not exceeded. In these cases, the response includes on-site and off-site emergency measures.

7.23 Safeguards

NPP design is subject to the obligations arising from Canada's international agreements, and to requirements pertaining to safeguards and non-proliferation.

The design and the design process ensure compliance with the obligations arising from the safeguards agreement between Canada and the IAEA. In general, these features are associated with the permanent installation of safeguards equipment and the provision of services required for ongoing operation of that equipment.

7.24 Decommissioning

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

1. Materials are selected for the construction and fabrication of plant components and structures with the purpose of minimizing eventual quantities of radioactive waste and assisting decontamination;
2. Plant layout is designed to facilitate access for decommissioning or dismantling activities; and
3. Consideration is given to the future potential requirements for storage of radioactive waste generated as a result of new facilities being built, or existing facilities being expanded.

8.0 SYSTEM-SPECIFIC EXPECTATIONS

8.1 Reactor Core

The design provides 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 structures and cooling systems:

1. Withstand static and dynamic loading, including thermal expansion and contraction;
2. Withstand vibration (such as flow-induced and acoustic vibration);
3. Ensure chemical compatibility;
4. Meet thermal material limits; and
5. Meet radiation damage limits.

The reactor core design facilitates the application of a guaranteed shutdown state as described in subsection 7.11.

The design of the core is such that:

1. The fission chain reaction is controlled during normal operation and AOOs; and
2. The maximum degree of positive reactivity and its maximum rate of increase by insertion in normal operation, AOOs, and DBAs are limited so that no resultant failure of the reactor pressure boundary will occur, cooling capability will be maintained, and no significant damage will occur to the reactor core.

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

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

8.1.1 Fuel Elements and Assemblies

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

Fuel assemblies and the associated components are designed to withstand the anticipated irradiation and environmental conditions in the reactor core, and all processes of deterioration that can occur in normal operation and AOOs. At the design stage, consideration is given to long-term storage of irradiated fuel assemblies after discharge from the reactor.

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

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

Fuel assemblies are designed to permit adequate inspection of their structures and component parts prior to and following irradiation.

In DBAs, the fuel assembly and its component parts remain in position with no distortion that would prevent effective post-accident core cooling or interfere with the actions of reactivity control devices or mechanisms. The acceptance criteria for the fuel for DBAs are consistent with these expectations.

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

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

8.1.2 Control System

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

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

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

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

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

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

8.2 Reactor Coolant System

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

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

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

Plant states in which components of the pressure boundary could exhibit brittle behaviour should be avoided.

The design reflects consideration of all conditions of the boundary material in normal operation (including maintenance and testing), AOOs, and DBAs, as well as 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, minimizes the likelihood of failure and associated consequential damage to other items of the reactor coolant system. This applies to normal operation, AOOs, and DBAs, with allowance for deterioration that may occur in service.

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

8.2.1 In-service Pressure Boundary Inspection

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

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

8.2.2 Inventory

Taking volumetric changes and leakage into account, the design provides control of coolant inventory and pressure to ensure that specified design limits are not exceeded in normal operation. This expectation extends to the provision of adequate capacity (flow rate and storage volumes) in the systems performing this function.

The inventory in the reactor coolant system and its associated systems are sufficient to support 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 provides 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

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

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

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

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

8.3 Steam Supply System

8.3.1 Steam Lines

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

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

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

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

The MSIVs are testable.

Steam lines up to and including the first isolation valve and, where applicable, steam generators, are qualified to withstand a design basis earthquake.

8.3.2 Steam and Feedwater System Piping and Vessels

All piping and vessels are typically separated from electrical and control systems to the extent practicable.

The auxiliary feedwater, boiler pressure control, and other auxiliary systems, prevent the escalation of AOOs to accident conditions.

8.3.3 Turbine Generators

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

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

8.4 Means of Shutdown

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

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

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

At least one means of shutdown is independently capable of rendering the reactor subcritical from normal operation, in AOOs, and in DBAs, and maintaining the reactor subcritical by an adequate margin and with high reliability for even the most reactive conditions of the core.

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

While resetting the means of shutdown, the maximum degree of positive reactivity and the maximum rate of increase are within the capacity of the reactor control system.

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

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

8.4.1 Reactor Trip Parameters

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

For each credited means of shutdown, the design specifies a direct trip parameter to initiate reactor shutdown for all AOOs and DBAs in time to meet the respective derived acceptance criteria. Where a direct trip parameter does not exist for a given credited means, there are two diverse trip parameters specified for that means.

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

There is no gap in trip coverage for any operating condition (i.e., power, temperature, etc.) within the OLCs. This is ensured by providing additional trip parameters if necessary. A different level of effectiveness may be acceptable for the additional trip parameters.

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

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

8.4.2 Reliability

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

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

8.4.3 Monitoring and Operator Action

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

The need for manual shutdown actuation is minimized.

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

8.5 Emergency Core Cooling System

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

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

The design considers the effect on core reactivity of the mixing of ECCS water with reactor coolant water, including possible mixing due to in-leakage.

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

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

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

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

In the event of an accident when injection of emergency coolant is required, it is not readily possible for an operator to prevent the injection from taking place.

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

ECCS piping in an extension of containment that could contain radioactivity from the reactor core is subject to the following expectations:

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

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

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

8.6 Containment

8.6.1 General Requirements

Each nuclear power reactor is installed within a containment structure to minimize the release of radioactive materials to the environment during normal operation, AOOs, and DBAs. Containment also assists in mitigating the consequences of BDBAs.

The containment system is designed for all AOOs and DBAs, and also considers BDBAs, including severe accident conditions.

The containment is a safety system and includes complementary design features, both of which are subject to the respective design expectations provided in this regulatory document.

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

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

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

The containment includes at least the following subsystems:

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

When the containment design includes the use of compressed air or non-condensable gas systems in response to a DBA, the autonomy of the compressed air system is demonstrated. In the event of a loss of compressed air, containment isolation valves fail in their safe state.

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

8.6.2 Strength of the Containment Structure

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

The margins reflect:

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

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

The containment structure protects systems and equipment important to safety in order to preserve safety functions for the plant.

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

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

8.6.3 Capability for Pressure Tests

The containment structure is subject to pressure testing at a specified pressure to demonstrate structural integrity. Testing is conducted before plant operation commences and throughout the plant's lifetime.

8.6.4 Leakage

Leakage Rate Limits

The safety leakage rate limit assures that:

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

The design leakage rate limit is:

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

Test Acceptance Leakage Rate Limits

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

Leak Rate Testing

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

1. For commissioning, at the containment design pressure; 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.

To the extent practicable, penetrations are to be designed to allow individual testing of each penetration.

The design is expected to provide for ready and reliable detection of any significant breach of the containment envelope.

8.6.5 Containment Penetrations

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

All containment penetrations are subject to the same design expectations as the containment structure itself, and are to 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 are designed to allow for periodic inspection.

If resilient seals such as elastomeric seals, electrical cable penetrations, or expansion bellows are used with penetrations, they have the capacity for leak testing at the containment design pressure. To demonstrate continued integrity over the lifetime of the plant, this capacity supports 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, is to 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.

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

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

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

Reactor Coolant System Auxiliaries that Penetrate Containment

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

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

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

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

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

Systems Connected to Containment Atmosphere

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

1. Two automatic isolation valves in series for lines that may be open to the containment atmosphere;
2. Two closed isolation valves in series for lines that are normally closed to the containment atmosphere; and
3. The line up to and including the second valve is part of the containment envelope.

Closed Systems

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

Where failure of a closed loop is assumed to be a PIE or the result of a PIE, the isolations for reactor coolant system auxiliaries apply.

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.

8.6.7 Containment Air Locks

Personnel access to the containment is through airlocks that are 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, the design specifies provisions for personnel safety, including emergency egress. This expectation also applies to equipment air locks.

8.6.8 Internal Structures of the Containment

The design provides for ample flow routes between separate compartments inside the containment. The openings between compartments are to be large enough to prevent significant pressure differentials that may cause damage to load bearing and safety systems during AOOs and DBAs.

The design of internal structures considers any hydrogen control strategy, and assists in the effectiveness of that strategy.

8.6.9 Containment Pressure and Energy Management

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

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

8.6.10 Control and Cleanup of the Containment Atmosphere

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

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

The design also:

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

8.6.11 Coverings, Coatings, and Materials

The coverings and coatings for components and structures within the containment are carefully selected, and their methods of application specified to ensure fulfillment of their safety functions. The primary objective of this expectation 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 takes 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.

8.6.12 Severe Accidents

Following onset of core damage, the containment boundary should be capable of contributing to the reduction of radioactivity releases to allow sufficient time for the implementation of off-site emergency procedures. This expectation applies to a representative set of severe accidents.

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

The ability of the containment system to withstand loads associated with severe accidents is demonstrated in design documentation, and includes the following considerations:

1. Various heat sources, including residual heat, metal-water reactions, combustion of gases, and standing flames;
2. Pressure control;
3. Control of combustible gases;
4. Sources of non-condensable gases;
5. Control of radioactive material leakage;
6. Effectiveness of isolation devices;
7. Functionality and leak tightness of air locks and containment penetrations; and
8. Effects of the accident on the integrity and functionality of internal structures.

The design authority should consider incorporation of complementary design features that will:

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

8.7 Heat Transfer to an Ultimate Heat Sink

The design includes systems for transferring residual heat from SSCs important to safety to an ultimate heat sink. This function is subject to 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, are therefore designed in accordance with the importance of their contribution to the function of heat transfer as a whole.

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

The design extends 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 SSCs;
2. Radioactive materials can be confined; and
3. Releases to the environment can be limited.

8.8 Emergency Heat Removal System

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

If the design of the plant is such that the EHRS is required to mitigate the consequences of a DBA, then the EHRS is designed as a safety system.

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

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

The design supports maintenance and reliability testing without a reduction in system effectiveness below that required by the OLCs.

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

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

8.9 Emergency Power Supply

The emergency power supply (EPS) system has sufficient capacity and reliability, within a specified mission time, to provide the necessary power to maintain the plant in a safe state and ensure nuclear safety in the event of all DBAs. These expectations are met following a common-cause loss of off-site power where this may occur as a result of a PIE, and in the presence of a single failure in the EPS.

The EPS system has sufficient capacity and capability, within a specified mission time, to support severe accident management actions.

The EPS system includes appropriate control, monitoring and testing facilities.

The emergency power supply:

1. Is initiated either automatically or manually following the DBAs as determined by the nuclear safety requirements of the plant; and
2. Can be tested under load conditions representing full load demand.

8.10 Control Facilities

8.10.1 Main Control Room

The design provides 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, to the extent practicable, following BDBAs.

The design identifies events both internal and external to the MCR that may pose a direct threat to its continued operation, and provides practicable measures to minimize the effects of these events.

The 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 layout of the controls and instrumentation, and the mode and format used to present information, 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 is such that appropriate lighting levels and thermal environment are maintained, and noise levels are minimized to applicable standards and codes.

The design of the MCR takes ergonomic factors into account to provide both physical and visual accessibility to controls and displays, without adverse impact on health and comfort. This includes hardwired display panels as well as computerized displays, with the aim of making these displays as user friendly as possible.

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

The design provides visual and, if appropriate, audible indications of plant states and processes that have deviated from normal operation and that could affect safety.

The design also allows for the display of information needed to monitor the effects of the automatic actions of all control, safety, and safety support system.

The MCR is to be provided with secure communication channels to the emergency support centre and to off-site emergency response organizations, and to allow for extended operating periods.

8.10.1.1 Safety Parameter Display System

The MCR contains a safety parameter display system that presents sufficient information on safety-critical parameters for the diagnosis and mitigation of DBAs and BDBAs, including severe accidents.

The safety parameter display system has the following capabilities:

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; and
4. Display the status of safety systems.

The safety parameter display system is designed and installed such that the same information is made available in a secure manner to the emergency support centre.

The safety parameter display system is integrated and harmonized with the overall control room human-system interface design.

8.10.2 Secondary Control Room

The design provides a secondary control room (SCR) that is physically and electrically separate from the MCR, and from which the plant can be placed and kept in a safe shutdown state when the ability to perform essential safety functions from the MCR is lost.

The design identifies all events that may pose a direct threat to the continued operation of the MCR and the SCR. The design of the MCR and the SCR are such that no event can simultaneously affect both control rooms to the extent that the essential safety functions cannot be performed.

For any PIE, at least one control room is habitable, and is accessible by means of a qualified route.

Instrumentation, control equipment, and displays are available in the SCR, so that the essential safety functions can be performed, essential plant variables can be monitored, and operator actions are supported.

Safety functions initiated by automatic control logic in response to an accident can also be initiated manually from both the MCR and the SCR.

The design of the SCR ensures that appropriate lighting levels and thermal environment are maintained, and noise levels align with applicable standards and codes.

Ergonomic factors apply to the design of the SCR to ensure physical and visual accessibility in relation to controls and displays, without adverse impact on health and comfort. These include hardwired display panels as well as computerized displays that are as user friendly as possible.

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

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

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

The SCR allows for extended operating periods.

8.10.3 Emergency Support Centre

The design provides 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 emergency support centre design ensures that appropriate lighting levels and thermal environment are maintained, and that noise levels are minimized to applicable standards and codes.

The emergency support centre includes a safety parameter display system similar to those in the MCR and in the SCR.

Information about the radiological conditions in the plant and its immediate surroundings, and about meteorological conditions in the vicinity of the plant, is to be accessible from the emergency support centre.

The emergency support centre includes secure means of communication with the MCR, the SCR, and other important points in the plant, and with on-site and off-site emergency response organizations.

The design ensures 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 expectations apply:

1. There are clear, well-defined, validated, and readily available operating procedures that identify the necessary actions;
2. There is instrumentation in the control rooms to provide clear and unambiguous indication of the necessity for operator action;
3. Following indication of the necessity for operator action inside the MCR, there is at least 15 minutes available before the operator action is required; and
4. Following indication of the necessity for operator action outside the MCR, there is a minimum of 30 minutes available before the operator action is required.

Alternative action times may be used if justified, making due allowance for the complexity of the action to be taken, and for the time needed for such activities as the diagnosing the event and accessing to the remote station.

For automatically initiated safety systems and control logic actions, the design facilitates backup manual initiation from inside the appropriate control room.

8.11 Waste Treatment and Control

The design includes provisions to treat liquid and gaseous effluents in a manner that will keep the quantities and concentrations of discharged contaminants within prescribed limits, and that will support application of the ALARA principle.

The design also includes 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 includes suitable means for controlling liquid releases to the environment in a manner that conforms to the ALARA principle.

This includes a liquid waste management system of sufficient capacity to collect, hold, mix, pump, test, treat, and sample liquid waste before discharge, taking expected waste and accidental spills or discharges into account.

8.11.2 Control of Airborne Material within the Plant

The design includes gaseous waste management systems capable of:

1. Controlling all gaseous contaminants so as to conform to the ALARA principle and ensure that concentrations remain within prescribed limits;
2. Collecting all potentially active gases, vapours, and airborne particulates for monitoring;
3. Passing all potentially active gases, vapours, and airborne particulates through pre-filters, absolute filters, charcoal filters, or high efficiency particulate air filters where applicable; and
4. Delaying releases of potential sources of noble gases by way of an off-gas system of sufficient capacity.

The design provides a ventilation system with an appropriate filtration system capable of:

1. Preventing unacceptable dispersion of all airborne contaminants within the plant;
2. Reducing the concentration of airborne radioactive substances to levels compatible with the need for access to each particular area;
3. Keeping the level of airborne radioactive substances in the plant below prescribed limits, applying the ALARA principle in normal operation; and
4. Ventilating rooms containing inert or noxious gases without impairing the capability to control radioactive releases.

8.11.3 Control of Gaseous Releases to the Environment

The ventilation system includes 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 reliably achieves the necessary retention factors under the expected prevailing conditions, and is 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:

1. Ensures nuclear criticality safety by
    a) maintaining an approved subcriticality 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 to personnel of postulated criticality accidents, and
    c) mitigating off-site consequences of postulated criticality accidents;
2. Permits appropriate maintenance, periodic inspection, and testing of components important to safety;
3. Permits inspection of non-irradiated fuel;
4. Prevents loss of or damage to the fuel; and
5. Meets Canada's safeguards requirements for recording and reporting accountancy data, and for monitoring flows and inventories related to non-irradiated fuel containing fissile material.

8.12.2 Handling and Storage of Irradiated Fuel

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

1. Ensures nuclear criticality safety by
    a) maintaining an approved subcriticality 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 to personnel of postulated criticality accidents, and

c) mitigating off-site consequences of postulated criticality accidents;

2. Permits adequate heat removal under normal operation, AOOs, and DBAs;
3. Permits inspection of irradiated fuel;
4. Permits periodic inspection and testing of components important to safety;
5. Prevents the dropping of used fuel in transit;
6. Prevents unacceptable handling stresses on fuel elements or fuel assemblies;
7. Prevents the inadvertent dropping of heavy objects and equipment on fuel assemblies;
8. Permits inspection and safe storage of suspect or damaged fuel elements or fuel assemblies;
9. Provides proper means for radiation protection;
10. Adequately identifies individual fuel modules;
11. Facilitates maintenance and decommissioning of the fuel storage and handling facilities;
12. Facilitates decontamination of fuel handling and storage areas and equipment when necessary;
13. Ensures implementation of adequate operating and accounting procedures to prevent loss of fuel;
14. Includes measures to prevent a direct threat or sabotage to irradiated fuel; and
15. Meets Canada's safeguards requirements for recording and reporting accountancy data, and for monitoring flows and inventories related to irradiated fuel containing fissile material.

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

1. Controlling the chemistry and activity of any water in which irradiated fuel is handled or stored;
2. Monitoring and controlling the water level in the fuel storage pool;
3. Detecting leakage; and
4. Preventing the pool from emptying in the event of a pipe break.

8.12.3 Detection of Failed Fuel

The design provides a means for allowing reliable detection of fuel defects in the reactor, and subsequent removal of failed fuel if action levels are exceeded.

8.13 Radiation Protection

The design and layout of the plant make suitable provision to minimize exposure and contamination from all sources. This includes the adequate design of SSCs to:

1. Control access to the plant;
2. Minimize exposure during maintenance and inspection;
3. Provide shielding from direct and scattered radiation;
4. Provide ventilation and filtering to control airborne radioactive materials;
5. Limit the activation of corrosion products by proper specification of materials;
6. Minimize the spread of active material;
7. Monitor radiation levels; and
8. Provide suitable decontamination facilities.

8.13.1 Design for Radiation Protection

The shielding design prevents radiation levels in operating areas from exceeding the prescribed limits. This includes provision of appropriate permanent layout and shielding of SSCs containing radioactive materials, and the use of temporary shielding for maintenance and inspection work.

To minimize radiation exposure, the plant layout provides for efficient operation, inspection, maintenance, and replacement. In addition, the design limits the amount of activated material and its build-up.

The design accounts for frequently occupied locations, and supports the need for human access to locations and equipment.

Access routes are shielded where needed.

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

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

8.13.2 Access and Movement Control

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

The design minimizes the movement of radioactive materials and the spread of contamination, and to provide appropriate decontamination facilities for personnel.

8.13.3 Monitoring

Equipment is provided to ensure that there is adequate radiation monitoring in normal operation, AOOs, and DBAs.

Stationary alarming dose rate meters are therefore provided:

1. For monitoring the local radiation dose rate at places routinely occupied by operating personnel;
2. Where the changes in radiation levels may be such that access may be limited for periods of time;
3. To indicate the general radiation level at appropriate locations in the event of DBAs and, as far as practicable, severe accidents; and
4. To give sufficient information in the control room or at the appropriate control position to enable plant personnel to initiate corrective actions when necessary.

Monitors are to be provided for measuring the activity of radioactive substances in the atmosphere:

1. For areas routinely occupied by personnel;
2. For areas where the levels of activity of airborne radioactive materials may, on occasion, be expected to necessitate protective measures; and
3. To give an indication in the control room, or in other appropriate locations, of when a high concentration of radionuclides is detected.

Facilities are provided for monitoring individual doses to and contamination of personnel.

Stationary equipment and laboratory facilities are to 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 is provided for monitoring the effluents prior to or during discharge to the environment.

8.13.4 Sources

The design provides 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 provides the means for monitoring radiological releases to the environment in the vicinity of the plant, with particular reference to:

1. Pathways to the human population, including the food-chain;
2. The radiological impact, if any, on local ecosystems;
3. The possible accumulation of radioactive 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 includes hazards analysis, deterministic safety analysis, and probabilistic safety assessment techniques. The safety analysis demonstrates achievement of all levels of defence-in-depth, and confirms that the design is capable of meeting the applicable expectations, dose acceptance criteria, and safety goals.

The first step of each part of the safety analysis is to identify PIEs using a systematic methodology such as failure modes and effects analysis. PIE identification considers both direct and indirect events.

9.2 Analysis Objectives

The safety analysis is iterative with the design process, and results in two reports: 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 expectations.

The final safety analysis:

1. Reflects the as-built plant;
2. Demonstrates that the design can withstand and effectively respond to identified PIEs;
3. Demonstrates the effectiveness of the safety systems and safety support systems;
4. Derives the OLCs for the plant, including
    a) operational limits and set points important to safety, and
    b) allowable operating configurations, and constraints for operational procedures;
5. Establishes requirements for emergency response and accident management;
6. Determines 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. Confirms that the dose and derived acceptance criteria are met for all AOOs and DBAs; and
8. Demonstrates that all safety goals have been met.

9.3 Hazards Analysis

Hazards analysis is the process of collecting and evaluating information about the NPP to identify the associated hazards and determine those that are significant and must be addressed. A hazards analysis demonstrates the ability of the design to effectively respond to credible common-cause events.

As discussed in Section 9.1, the first step of the hazards analysis is to identify PIEs. For each common-cause PIE, the hazards analysis then identifies:

1. Applicable acceptance criteria (i.e., the success path criteria);
2. The hazardous materials in the plant and at the plant site;
3. All qualified mitigating SSCs credited during and following the event—all non-qualified safety or safety support systems are assumed to fail, except in cases where their continued operation would result in more severe consequences;
4. Operator actions and operating procedures for the event; and
5. Plant or operating procedure parameters for which the event is limiting.

The hazards analysis confirms that:

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

The hazards analysis report includes the findings of the analysis and the basis for those findings. This report also:

1. Includes a general description of the physical characteristics of the plant that outlines the prevention and protection systems to be provided;
2. Includes the list of safe shutdown equipment;
3. Defines and describes the characteristics associated with hazards for all areas that contain hazardous materials;
4. Describes the performance criteria for detection systems, alarm systems, and mitigation systems, including requirements such as seismic or environmental qualification;
5. Describes the control and operating room areas and the protection systems provided for these areas, including additional facilities for maintenance and operating personnel;
6. Describes the operator actions and operating procedures of importance to the given analysis;
7. Identifies the plant parameters for which the event is limiting;
8. Explains the inspection, testing, and maintenance parameters needed to protect system integrity; and
9. Defines the emergency planning and coordination requirements for effective mitigation, including any necessary measures to compensate for the failure or inoperability of any active or passive protection system or feature.

9.4 Deterministic Safety Analysis

The purpose of the deterministic safety analysis is to:

1. Confirm that OLCs comply with the assumptions and intent of the design for normal operation of the plant;
2. Characterize the events that are appropriate for the plant site and design;
3. Analyze and evaluate event sequences that result from failure of SSCs;
4. Compare the results of the analysis with dose acceptance criteria and design limits;
5. Establish and confirm the design basis; and
6. Demonstrate that AOOs and DBAs can be managed by automatic response of safety systems in combination with prescribed operator actions.

The expectations for the deterministic safety analysis are provided in CNSC regulatory document RD-310, *Safety Analysis for Nuclear Power Plants*.

9.5 Probabilistic Safety Assessment

The purpose of the probabilistic safety assessment is 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 design feature or event makes a dominant contribution to the frequency of severe accidents, taking uncertainties into account;
3. Provide probability assessments for the occurrence of 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 is conducted in accordance with the requirements specified in CNSC regulatory standard S-294, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*.

10.0 ENVIRONMENTAL PROTECTION AND MITIGATION

10.1 Design for Environmental Protection

The design makes adequate provision to protect the environment and to mitigate the impact of the NPP on the environment. A review of the design confirms that this provision has been met.

A systematic approach is used to assess the potential bio-physical environmental effects of the NPP on the environment, and the effects of the environment on the NPP.

10.2 Release of Nuclear and Hazardous Substances

The design demonstrates through process, monitoring, control, prevention, and mitigation measures, that the releases of nuclear and hazardous substances will conform to the ALARA principle.

The life cycle assessment identifies various sources of nuclear and hazardous substances in design, operation, and decommissioning, along with their possible environmental impacts on human and non-human biota.

Some of the factors that are considered include:

1. Resource requirements for the NPP, such as fuel, energy, and water;
2. Depletion of ground and surface water resources;
3. Contamination of air, soil, and water resources;
4. Nuclear and hazardous substances used;
5. Types of waste generated—gaseous, liquid and solid;
6. Quantities of waste generated;
7. Impact of cooling water intake on entrainment and impingement; and
8. Impact of water output on the thermal regime of the receiving environment.

Technological options are considered in establishing design objectives for controlling and monitoring releases during start-up, normal operation, shutdown, and potential abnormal and emergency situations. Appropriate limits are included in the plant OLCs.

Technological options for the design of cooling water systems should consider a closed-cycle technology in order to minimize adverse environmental impact on aquatic biota.

11.0 ALTERNATIVE APPROACHES

The expectations in this regulatory document are intended to be technology neutral for water-cooled reactor designs. It is recognized that specific technologies may use alternative approaches.

The CNSC will consider alternative approaches to the expectations in this document where:

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

Any alternative approach should demonstrate equivalence to the outcomes associated with the use of the expectations set out in this regulatory document.

GLOSSARY

Abbreviations

ALARA	as low as reasonably achievable
AOO	anticipated operational occurrence
BDBA	beyond design basis accident
BDBT	beyond design basis threat
CNSC	Canadian Nuclear Safety Commission
DBA	design basis accident
DBE	design basis earthquake
DBT	design basis threat
ECCS	emergency core cooling system
EHRS	emergency heat removal system
EPS	emergency power supply
GSS	guaranteed shutdown state
IAEA	International Atomic Energy Agency
MCR	main control room
MSIV	main steam isolation valve
NPP	nuclear power plant
NSCA	*Nuclear Safety and Control Act*
OLC	operational limits and conditions
PIE	postulated initiating event
PSA	probabilistic safety assessment
RCS	reactor coolant system
SCR	secondary control room
SSCs	structures, systems, and components

Terminology

Accident
Any unintended event, including operating errors, equipment failures or other mishaps, the consequences or potential consequences of which are not negligible from the point of view of protection or safety.
Note: For the purposes of this document, accidents include design basis accidents and beyond design basis accidents. Accidents exclude anticipated operational occurrences, which have negligible consequences from the perspective of protection or safety.

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

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

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

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

Commissioning
A process 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 feature

A design feature outside of the design basis envelope that is introduced to cope with beyond design basis accidents, including severe accidents.

Confinement
A continuous boundary without openings or 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 on experience or indirect information, about a phenomena or behaviour of a system being at or near the limit of expectation, which increases safety margins or makes predictions regarding consequences more severe than if best-estimate assumptions had been made.

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

Crediting
Assuming the correct operation of an SSC, or correct operator action, as part of an analysis.

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

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

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

Direct trip parameter
A value based on direct measurement of a specific challenge to the derived acceptance criteria and, if applicable, a direct measure of the event.

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

Environment
The components of the Earth, including:

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

(2) All organic and inorganic matter and living organisms; and

(3) Interacting natural systems that include components referred to in (1) and (2).

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

External event
Any event that proceeds from the environment external to a nuclear power plant, and can cause failure of structures, systems and components.
Note: External events include, but are not limited to, earthquakes, floods, and hurricanes.

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

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

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

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

Independent systems
Systems that do not share any components.

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

Jet impact
The potential internal hazard associated with high pressure fluid released from a pressure-retaining component.

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

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

Management arrangements
The means by which an organization functions to achieve its objectives, including:

(1) Physical elements, such as people, buildings, work areas, equipment, tools, etc.;
(2) Intangible elements, such as roles and responsibilities, knowledge, skills and behaviour of the people, cultural norms, agreements, understandings, decision-making processes, etc.; and
(3) The documentation that is essential to meeting the organization’s objectives.

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 an event.

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

Nuclear power plant
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*.

Plant state
A configuration of nuclear power plant 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 state).

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

Practicable
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.

Probabilistic safety assessment
A comprehensive and integrated assessment of the safety of the nuclear power plant 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 plant. Such assessments are most useful in assessing the relative level of safety.

Process
Set of interrelated activities that transform inputs into outputs.

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

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, fission in the fuel in the shutdown state, and the heat stored in reactor related structures, systems and components.

Risk significant system
Any plant system whose failure to meet design and performance specifications could result in unreasonable risk to the health and safety of persons, to national security, or to the environment.

Safeguards
A system of international inspections and other verification activities undertaken by the IAEA in order to evaluate, on an annual basis, Canada's compliance with its obligations pursuant to the safeguards agreements between Canada and the IAEA.

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 culture
The characteristics of the work environment, such as values, rules and common understandings, that influence employee perceptions and attitudes about the importance that the organization places on safety.

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

Safety support system
A system designed to support the operation of one or more safety systems.

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

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

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

Shutdown state
Characterized by subcriticality of the reactor. At shutdown, automatic actuation of safety systems could be blocked and support systems may remain in abnormal configurations.

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

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

Trip parameter
A measurement of a variable that is used to trigger a safety system action when the trip parameter set point is reached.

Trip parameter set point
Trip parameter value at which activation of a safety system is triggered.

Ultimate heat sink
A medium to which the residual heat can always be transferred, 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.

Usability
The extent to which a product can be used by specified users, to achieve specified goals, with effectiveness, efficiency, and satisfaction in a specified context of use.

Vital area
An area containing equipment, systems, or devices the sabotage of which could directly or indirectly lead to unacceptable radiological consequences.

ADDITIONAL INFORMATION

The following legislation and regulations are relevant to this document:

1. *Class I Nuclear Facilities Regulations*, SOR/2000-204
2. *General Nuclear Safety and Control Regulations*, SOR/2000-202
3. *Nuclear Safety and Control Act*, S.C.,1997, c.9
4. *Nuclear Security Regulations*, SOR/2000-209
5. *Radiation Protection Regulations*, SOR/2000-203

The following documents provide additional information pertaining to nuclear power plant design:

1. *Design Guide for Basic and Intermediate Level Radioisotope Laboratories*, R-52 rev-1, Atomic Energy Control Board, 1991
2. *Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills*, G-225, Canadian Nuclear Safety Commission, 2001
3. *Engineering Safety Aspects of the Protection of Nuclear Power Plant Against Sabotage*, International Atomic Energy Agency, Nuclear Security Series No. 4, 2007
4. *Entry to Protected and Inner Areas*, G-205, Canadian Nuclear Safety Commission, 2003
5. *Human Factors Engineering Program Plans*, G-276, Canadian Nuclear Safety Commission, 2003
6. *Human Factors Verification and Validation Plans*, G-278, Canadian Nuclear Safety Commission, 2003
7. *Keeping Radiation Exposures and Doses "As Low as Reasonably Achievable (ALARA)"*, G-129 rev-1, Canadian Nuclear Safety Commission, 2004
8. *Nuclear Emergency Management*, P-325, Canadian Nuclear Safety Commission, 2006
9. *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*, S-294, Canadian Nuclear Safety Commission, 2005
10. *Reliability Programs for Nuclear Power Plants*, S-98 rev-1, Canadian Nuclear Safety Commission, 2005
11. *Safety Analysis for Nuclear Power Plants*, RD-310, Canadian Nuclear Safety Commission, 2008

12. *Safety of Nuclear Plants: Design*, IAEA Safety Standard Series NS-R-1, International Atomic Energy Agency, Vienna, 2000

13. *Security Programs for Category I or II Nuclear Material or Certain Nuclear Facilities*, G-274, Canadian Nuclear Safety Commission, 2003

14. *Severe Accident Management Programs for Nuclear Reactors*, G-306, Canadian Nuclear Safety Commission, 2006

15. *Transportation Security Plans for Category I, II or III Nuclear Material*, G-208, Canadian Nuclear Safety Commission, 2003