Canada's Nuclear Regulator

Design of New Nuclear Power Plants

RD-337 version 2

July 2012

DRAFT

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Canada

Design of New Nuclear Power Plants
Regulatory Document RD-337 version 2

Catalogue number XXXXX
ISBN XXXXX

Published by the Canadian Nuclear Safety Commission

Également publié en français sous le titre de : La conception des nouvelles centrales nucléaires

Document availability

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

To order a printed copy of the document in English or French, please contact:

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

Tel.: 613-995-5894 or 1-800-668-5284 (in Canada only)
Facsimile: 613-995-5086
Email: info@cnsc-ccsn.gc.ca
Web site: nuclearsafety.gc.ca

Publishing history:

November, 2008 Version 1.0

Legend

Changes to the current RD-337 (2008 version) are indicated by:

- strikethrough for content which has been removed
- bold font for new or revised requirements
- red font for changes to address recommendations from the CNSC Fukushima Task Force

Preface

This regulatory document sets **out** the **requirements** 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 **requirements** 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.

RD-337 version 2, *Design of New Nuclear Power Plants*, supersedes the previous version published in 2008. Version 2 implements recommendations from The CNSC Fukushima Task Force Report.

The associated guidance document GD-337, *Guidance on the Design of New Nuclear Power Plants* provides expectations and guidance on how to meet the requirements of RD-337, version 2.

To the extent practicable, the **requirements** provided herein are technology-neutral with respect to water-cooled reactors.

To a large degree, RD-337 **version 2** represents the CNSC's adoption of the principles set forth by the International Atomic Energy Agency (IAEA) in **SSR 2/1**, Safety of Nuclear Power Plants: Design (which is the revision to NS-R-1) **as adapted to align with Canadian requirements**.

Similar to **SSR 2/1**, RD-337 **version 2**, 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 pertinent requirements. ~~associated with convential codes and standards. In particular, while RD-337 may assist a proponent in making a licence application.~~ **It is the applicant's or licensee's** responsibility to identify **and comply** with all applicable regulations and licence conditions.

This document may be used as part of the licensing basis for a regulated facility or activity by reference in a licence. The licensing basis sets the boundary conditions for acceptable performance at a regulated facility or activity, and thus establishes the basis for the CNSC's compliance program in respect of that regulated facility or activity.

The licensing basis for a regulated facility or activity is a set of requirements and documents comprising:

(i) the regulatory requirements set out in the applicable laws and regulations
(ii) the conditions and the safety and control measures described in the facility's or activity's licence along with the documents directly referenced in that licence
(iii) the safety and control measures described in the licence application, and the documents needed to support that licence application

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

Table of Contents

Design of New Nuclear Power Plants

1. Purpose

The purpose of this regulatory document is to set out the **requirements** of the Canadian Nuclear Safety Commission (CNSC) with respect to the design of new water-cooled nuclear power plants (NPPs or plants).

2. Scope

This document sets out CNSC **requirements** 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 **national and** 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 **requirements** associated with this regulatory document. However, the 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 **requirements** that are related to nuclear safety.

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

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

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

3. Relevant Legislation

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. **Paragraphs 3(*b*), 5(*a*), (*d*), (*e*), (*f*), (*i*) and 6(*a*), (*b*), (*h*) and 7(*f*) of the *Class I Nuclear Facilities Regulations* stipulates that an application for a licence in respect of a Class I nuclear facility, other than a licence to abandon, shall contain, in addition to other information:**

   3(*b*) "plans showing the location, perimeter, areas, structures and systems of the nuclear facility"

   5(*a*) "a description of the proposed design of the nuclear facility, including the manner in which the physical and environmental characteristics of the site are taken into account in the design"

   5(*d*) "a description of the structures proposed to be built as part of the nuclear facility, including their design and their design characteristics"

   5(*e*) "a description of the systems and equipment proposed to be installed at the nuclear facility, including their design and their design operating conditions"

   5(*f*) "a preliminary safety analysis report demonstrating the adequacy of the design of the nuclear facility"

   5(*i*) "the effects on the environment and the health and safety of persons that may result from the construction, operation and decommissioning of the nuclear facility"

   6(*a*) "a description of the structures at the nuclear facility, including their design and their design operating conditions"

   6(*b*) "a description of the systems and equipment at the nuclear facility, including their design and their design operating conditions"

   6(*h*) "the effects on the environment and the health and safety of persons that may result from the operation and decommissioning of the nuclear facility"

   7(*f*) "the effects on the environment and the health and safety of persons that may result from the decommissioning and the measures that will be taken to prevent or mitigate those effects"
6. Other sections of the *Class I Nuclear Facilities Regulations*, as well as sections of the *Radiation Protection Regulations* and the *Nuclear Security Regulations* that pertain to the design of a new nuclear power plant.

4. Safety Objectives and Concepts

4.1 General nuclear safety objective

In support of the NSCA and **its** 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 **three** complementary safety objectives, dealing with radiation protection, the technical aspects of the design, **and environmental protection**. The technical safety objective is interdependent with administrative and procedural measures that are taken to ensure defence against hazards due to ionizing radiation.

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 **shall** provide 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 will be below prescribed limits, and the likelihood of accidents with serious radiological consequences will be extremely low.

4.1.3 Environmental protection objective

The environmental protection objective is to provide all reasonably practical mitigation measures to protect the environment in operational states and accident conditions.

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

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 **shall be** performed to confirm that these criteria, 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 **shall be** calculated in the deterministic safety analysis for a period of 30 days after the analyzed event.

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

1. 0.5 millisievert 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 **shall be** provided a level of protection from the consequences of nuclear power plant operation, such that there is no significant additional risk to the life and health of individuals.
2. Societal risks to life and health from nuclear power plant operation **shall be** comparable to or less than the risks of generating electricity by viable competing technologies, and **shall** not significantly add to other societal risks.

Quantitative application of the safety goals

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

1. core damage frequency
2. small release frequency
3. large release frequency

A core damage accident results from a postulated initiating event (PIE) followed by the failure of one or more safety system(s) or safety support system(s). Core damage frequency is a measure of the plant's accident 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 **shall be** 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 **shall be** 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 **shall be** 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 **shall be** carried out. These analyses **shall** identify all sources of exposure, in order to evaluate potential radiation doses to workers at the plant and to the public, and to evaluate potential effects on the environment.

The safety analyses **shall** examine plant performance for:

1. normal operation
2. anticipated operational occurrences (AOOs)
3. design basis accidents (DBAs)
4. beyond design basis accidents (BDBAs), including **design extension conditions (DECs) - DECs include some severe accident conditions**

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

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

4.2.4 Accident mitigation and management

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

This **shall** include such measures as:

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

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

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

4.3 Safety concepts

4.3.1 Defence in depth

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

With the defence in depth approach, if a failure were to occur it **would** be detected and ~~compensation made~~, compensated or ~~it would be~~ corrected.

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

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

Level One

The aim of the first level of defence is to prevent deviations from normal operation, and to prevent failures of **structures, systems 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 Physical barriers

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

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

~~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~~
~~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.~~

OLCs shall include:

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

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

4.3.4 Interface of safety with security and safeguards

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

5. Safety Management in Design

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

The NPP design **shall**:

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

The design process **shall be** carried out by technically qualified and appropriately trained staff at all levels, and 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. **design control measures (such as processes, procedures, and practices) as part of an established management system ~~or quality assurance program~~**
4. **a safety management program that recognizes the importance of a healthy safety culture**

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 **shall be** transferred to the operating organization.

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

The applicant **or licensee shall** confirm that the design authority has achieved the following objectives 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.
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 **shall** achieve the following objectives:

1. SSCs important to safety meet their respective design requirements.
2. Due account is taken of the human capabilities and limitations of personnel.
3. Safety design information - necessary for safe operation and maintenance of the plant and for any subsequent plant modifications - is preserved.
4. OLCs are provided for incorporation into the plant administrative and operational procedures.

5. The plant design facilitates maintenance **and aging management** throughout the life of the plant.
6. The results of the **hazard analysis**, deterministic **safety analysis** and probabilistic safety assessment are taken into account.
7. Due consideration is given to the prevention of accidents and mitigation of their consequences.
8. **The** generation of radioactive and **hazardous waste** is limited to minimum practicable levels, in terms of both activity and volume.
9. A change control process is established to track design changes to provide configuration management during manufacturing, construction, commissioning and operation.
10. Physical protection systems are provided to address design basis threats.

5.3 Design control measures ~~QA Program~~

Design control measures, in the form of processes, procedures and practices, shall be established as part of the overall management ~~arrangements~~ **system so as to achieve the design objectives**. With respect to the plant design, this **shall** include identifying all performance and assessment parameters for the design, as well as detailed plans for each SSC, **in order to** ensure consistent quality of the design and the selected components.

The **design controls shall** be such that the initial design, and any subsequent change or safety improvement, is carried out in accordance with established processes and procedures ~~that~~ **which** call on appropriate standards and codes and ~~that~~ address applicable requirements and design bases. Appropriate design control measures **shall** also facilitate identification and control of design interfaces.

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

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

5.4 Proven engineering practices

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

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

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

When a new SSC design, feature or engineering practice is introduced, adequate safety **shall be** proven by a combination of supporting research and development programs and by examination of relevant experience from similar applications. An adequate qualification program **shall be** established to verify that the new design meets all applicable safety **requirements**. New designs

shall be tested before being brought into service and **shall be** monitored **while** in service **so as** to verify that the expected behaviour is achieved.

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

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

5.5 Operational experience and safety research

The NPP design **shall** draw 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. **The safety assessment for the design shall** include the requirements set by the operating organization and by regulatory authorities. The basis for the safety assessment **shall be** the data derived from the safety analysis, previous operational experience, results of supporting research, and proven engineering practices.

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

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

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

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

5.7 Design documentation

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

The design documentation **shall** include:

1. design description
2. design requirements
3. ~~system~~ **SSC** 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)
11. hazard analysis

6. Safety Requirements

6.1 Application of defence in depth

The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent to the extent practicable.

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

Level One

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

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

Level Two

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

Level Four

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

Most importantly, adequate protection **shall be** provided for the confinement function by way of a robust containment design. This includes the use of complementary design features to prevent

accident progression and to mitigate the consequences of DECs. The confinement function **shall be** further protected by severe accident management procedures.

Level Five

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

6.1.1 Physical barriers

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

To the extent practicable, the design ~~therefore~~ **shall** prevent:

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

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

6.2 Safety functions

The NPP design **shall** provide adequate means to:

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

The following fundamental safety functions **shall be** available **in operational states and** ~~during and following~~ **accident conditions**:

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

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

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

6.3 Accident prevention and plant safety characteristics

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

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

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

The design **shall** include provisions for the prevention and mitigation of radiation exposures resulting from **accident conditions**.

The design **shall** also **ensure** 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~~ **shall meet** the safety goals in subsection 4.2.2.

6.5 Exclusion zone

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

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

6.6 Facility layout

The facility layout shall take into account external hazards to enhance protection of SSCs important to safety.

The design **shall take** into account the interfaces between the safety, security **and safeguards** 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
7. interaction of building and support functions

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

6.6.1 Multi-unit requirements

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

7. General Design Requirements ~~Considerations~~

7.1 Classification of SSCs

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

In addition, all SSCs **shall** be identified as either important or not important to safety. The criterion for determining safety importance is based on:

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

SSCs important to safety **shall** include:

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

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

7.2 Plant design envelope

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

Figure 1: Plant States Considered in the Design

Plant Design Envelope			
Operational states		**Accident conditions**	
Normal operation	**Anticipated operational occurrences (AOOs)**	**Design basis accidents (DBAs)**	**Design extension conditions (DECs)**

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

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

Complementary design features address the performance of the plant in **DECs**. ~~including selected severe accidents.~~

7.3 Plant states

Plant states **considered in the design 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

4. ***Design Extension Conditions*— accident conditions, not considered design basis accidents, which are taken into account in the design of the facility. Note: DECs are a subset of beyond design basis accidents (BDBAs).** BDBAs are accident conditions less frequent and more severe than design basis accidents. A BDBA may or may not involve core degradation.

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

7.3.1 Normal operation

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

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

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

1. limits important to safety
2. constraints on control systems and procedures
3. plant maintenance, testing, and inspection requirements to ensure that SSCs function as intended, taking the ALARA principle into consideration
4. clearly defined operating configurations, such as startup, power production, shutdown, maintenance, testing, surveillance, and refuelling—these configurations **shall** include relevant operational restrictions in the event of safety system and safety support system outages

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

7.3.2 Anticipated operational occurrences

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

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

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

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

7.3.3 Design basis accidents

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

The design **shall** be such that releases to the public following a DBA will not exceed the dose acceptance ~~criteria~~ **criterion**.

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

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

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

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

7.3.4 Design extension conditions ~~Beyond design basis accidents~~

The design authority **shall** identify the set of design extension conditions (DECs) based on deterministic and probabilistic methods, operational experience, engineering judgment and the results of research and analysis **for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than DBAs or that involve additional failures**.

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

~~Complementary design features 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~~ **shall be provided to cope with DECs. Their design shall be** 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 **shall be** identified. These rules and practices do not necessarily need to incorporate the same degree of conservatism as those applied to the design basis.

The design shall identify a radiological and combustible gas accident source term for use in the specification of the complementary design features ~~for BDBAs~~ for DECs. This source term is referred to as the reference source term, and **shall be** based on a set of representative core damage accidents established by the design authority.

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

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

7.3.4.1 Severe accidents

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

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

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

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

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

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

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

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

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

The design authority **shall** establish initial severe accident management guidelines**,** taking into account the plant design features **including multi-unit requirements**, and the understanding of accident progression and associated phenomena.

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

7.4 Postulated initiating events

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

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

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

7.4.1 Internal hazards

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

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

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

7.4.2 External hazards

All natural and human induced external events that may be linked with significant radiological risk shall be identified. ~~The subset of external events that the plant is designed to withstand is selected, and design basis events shall be determined from this subset.~~ **External events which the plant is designed to withstand shall be selected, and classified as DBAs or DECs.**

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

Applicable natural external hazards **shall** include such events as earthquakes, droughts, floods, high winds, tornadoes, tsunami, and extreme meteorological conditions, **and shall consider the effects of climate change.** Human induced external events **shall** 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 **DECs shall be** considered in the design. Such combinations **shall be** identified early in the design phase, and **shall** be confirmed using a systematic approach.

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

7.5 Design rules and limits

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

The design **shall** also **identify** SSCs to which design limits are applicable. These design limits **shall be** specified for **operational states and accident conditions.**

7.6 Design for reliability

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

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

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

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

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

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

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 occurrences such 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 **shall be** considered in determining where to apply the principles of **separation,** diversity and independence **so as** 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.

7.6.1.1 Separation

The design **shall** provide sufficient physical separation between:

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

This **shall** apply to equipment and to **the** routing of ~~the following~~ items **including**:
1. electrical cables for power and control of equipment
2. piping for service water for the cooling of fuel and process equipment
3. tubing and piping for compressed air or hydraulic drives for control equipment

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

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

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

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

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

7.6.1.2 Diversity

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

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

7.6.1.3 Independence

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

7.6.2 Single failure criterion

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

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

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

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

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

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

Exemptions for passive components **shall** 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 **shall include** ~~analytical~~ justification of such exemptions, **by analysis and testing**. **The justification shall take** loads and environmental conditions into account, as well as the total period of time after the PIE for which the functioning of the component is necessary.

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

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

7.6.3 Fail-safe design

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

7.6.4 Allowance for equipment outages

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

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

7.6.5 Shared systems

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

1. the process and safety functions are not required or credited at the same time
2. if the process function is operating, and a PIE in that system is postulated, it can be shown that all essential safety functions of the system that are required to mitigate the PIE are unaffected
3. the system is designed to the standards of the function of higher importance with respect to safety

4. if the process function is used intermittently, then the availability of the safety function after each use, and its continued ability to meet ~~expectations~~ **requirements**, can be demonstrated by testing
5. the ~~expectations~~ **requirements** for instrumentation sharing are met

7.6.5.1 Shared instrumentation for safety systems

Instrumentation **shall** not typically **be** shared between safety systems.

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

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

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

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

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

7.6.5.2 Sharing of SSCs between reactors

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

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

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

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

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

7.7 Pressure retaining SSCs

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

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

The design **shall** minimize the likelihood of flaws in pressure boundaries. This **shall** include timely detection of flaws in pressure boundaries important to safety. ~~in a manner that supports leak-before-break detection capability.~~

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

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

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

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

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

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

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

7.8 Equipment environmental qualification

The design **shall include** ~~provides~~ an equipment environmental qualification program. Development and implementation of this program **shall** ensure that the following functions **can be** ~~are~~ carried out: ~~in post-accident conditions~~

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

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

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

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

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

7.9 Instrumentation and control

7.9.1 General ~~Considerations~~

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

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

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

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

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

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

The design **shall** also include the capability to trend and automatically record measurement of any derived parameters that are important to safety.
Instrumentation **shall be** adequate for measuring plant parameters for emergency response purposes.

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

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

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

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

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

7.9.2 Use of computer-based systems or equipment

Appropriate standards and ~~codes~~ **practices** for the development and testing ~~and maintenance~~ of computer hardware and software **shall be** ~~applied to the design of systems or equipment important to safety that are controlled by computer~~ **established and implemented throughout the lifetime of the system or equipment, and in particular, throughout the software development cycle.**

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

If 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—**shall be** developed, inspected, and tested in accordance with standards of a category commensurate with the safety function provided by the given system or equipment.

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

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

1. functions not essential to safety are separate from and shown not to impact the safety function
2. the safety function is normally executed in processors separate from software that implements other functions, such as control, monitoring, and display
3. the ~~expectations~~ **requirements** associated with diversity apply to computer-based systems that perform similar safety functions—the choice of diversity type be justified
4. the design incorporates fail-safe and fault tolerance features, and the additional complexity ensuing from these features results in an overall gain in safety
5. ~~the design provides protection against physical attack, intentional and non-intentional intrusion, fraud, viruses, and other malicious threats~~
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 Accident monitoring instrumentation ~~Post-accident instrumentation~~

Instrumentation and recording equipment **shall be** such that essential information is available to support plant procedures during and following **accident conditions such as:**

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

7.10 Safety support systems

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

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

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

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

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

The emergency support systems **shall**:

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

7.11 Guaranteed shutdown state

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

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

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

7.12 Fire safety

The design of the NPP, including that of external buildings and SSCs integral to plant operation, **shall** include 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 **shall** achieve the following general objectives:

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

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

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

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

7.12.2 Safety to life

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

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

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

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

7.12.3 Environmental protection and nuclear safety

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

7.13 Seismic qualification

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

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

7.13.1 Seismic design and classification

The design authority **shall identify** SSCs important to safety that are credited to withstand a design basis earthquake (DBE), and ensure that they are qualified accordingly. This **shall apply** to:

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

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

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

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

A beyond design basis earthquake shall be considered a DEC. SSCs credited to function during and after a beyond design basis earthquake shall be demonstrated to be capable of performing their intended function under the expected conditions. Such demonstration shall provide high confidence of low probability of failure under beyond design basis earthquake conditions for these SSCs.

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

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

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

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

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

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

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

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

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

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

7.15 Civil structures

7.15.1 Design

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

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

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

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

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

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

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

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

7.15.2 Surveillance

The design **shall** enable implementation of periodic inspection programs for structures related to nuclear safety, **in order** to verify as-constructed conditions.

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

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

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

7.15.3 Lifting of large loads

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

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

7.16 Construction and commissioning

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

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

The design shall include provisions to facilitate the commissioning activities. In particular, the design of the instrumentation and control systems shall make provisions for startup neutron sources and dedicated startup instrumentation for conditions in which they are needed.

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

7.17 Aging and wear

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

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

Additional requirements can be found in RD-334*, Aging Management for Nuclear Power Plants*.

7.18 Control of foreign material

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

7.19 Transport and packaging for fuel and radioactive waste

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

7.20 Escape routes and means of communication

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

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

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

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

7.21 Human factors

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

Human factors considerations:

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

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

Appropriate and clear distinction between the functions assigned to operating personnel and those assigned to automatic systems **shall be** facilitated by systematic consideration of human factors

and the **human-system** interface. This consideration **shall continue** in an iterative way throughout the entire design process.

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

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

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

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

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

The design **shall** provide the type of information that enables an 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 **shall** include promoting the success of operator action with due regard for the time available for response, the physical environment to be expected, and the associated psychological demands made on the operator.

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

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

7.22 Robustness against malevolent acts

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

7.22.1 Design principles

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

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

Threats identified as DBTs **shall have** credible attributes and characteristics ~~of~~ **for** 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 **shall be** assessed in order to establish means of mitigation to the extent practicable.

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

7.22.2 Design methods

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

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

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

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

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

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

7.22.3 Acceptance criteria

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

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

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

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

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

For extreme events, there **shall be** at least one means of reactor shutdown and core cooling. Degradation of the containment barrier may allow the release of radioactive material; however, the degradation **shall be** limited. ~~with the goal that the dose acceptance criteria are not exceeded~~. In these cases, the response **shall include** onsite and offsite emergency measures.

7.22.4 Cyber security

The design of computer-based instrumentation and control systems important to safety shall provide a cyber security defensive architecture.

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

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

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

7.23 Safeguards

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

7.24 Decommissioning

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

1. materials are selected for the construction and fabrication of plant components and structures with the purpose of minimizing eventual quantities of radioactive waste and assisting decontamination
2. plant layout is designed to facilitate access for decommissioning or dismantling activities, **including for multi-unit plants, periods when some units are operating and some are under decommissioning**

3. consideration is given to the future potential requirements for storage of radioactive waste generated as a result of new facilities being built, or existing facilities being expanded

8. System-Specific ~~Expectations~~ Requirements

8.1 Reactor core

Reactor core parameters and their limits shall be specified. All foreseeable reactor core configurations, for various appropriate operating schedules shall be considered in the core design.

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

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

The reactor core and associated structures and cooling systems **shall**:

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

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

The design of the core **shall** be such that:

1. the fission chain reaction is controlled during **operational states**
2. the maximum degree of positive reactivity and its maximum rate of increase by insertion **in operational states** and DBAs are limited **by a combination of the inherent neutronic characteristics of the core, its thermal-hydraulic characteristics, and the capabilities of the control system and means of shutdown**, so that no resultant failure of the reactor pressure boundary will occur, cooling capability will be maintained, and no significant damage will occur to the reactor core

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

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

8.1.1 Fuel elements and assemblies

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

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

Fuel design limits **shall** be established to include, 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 **shall** reflect the importance of preserving the **fuel matrix and** cladding, **as these are first and second barriers to fission product release, respectively**. ~~and fuel matrix, as these are the first barriers to fission product release~~.

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

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

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

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

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

8.1.2 Control system

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

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

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

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

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

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

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

8.2 Reactor coolant system

The design **shall** provide 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 **operational states** or DBAs.

The design **shall** ensure 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 (RCS) **shall** be fitted with isolation devices to limit any loss of radioactive coolant outside containment.

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

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

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

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

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

8.2.1 In-service pressure boundary inspection

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

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

8.2.2 Inventory

Taking volumetric changes and leakage into account, the design **shall** provide control of coolant inventory and pressure **so as** to ensure that specified design limits are not exceeded in

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

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

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

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

8.2.3 Cleanup

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

8.2.4 Removal of residual heat from reactor core

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

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

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

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

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 **shall** allow sufficient margin to ensure that the appropriate design limits of the pressure boundary are not exceeded **in operational states and** DBAs. This provision **shall** take into account the operation of control and safety systems.

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

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

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

The MSIVs **shall be** inspectable and testable.

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

8.3.2 Steam and feedwater system piping and vessels

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

The auxiliary feedwater, ~~boiler~~ **steam generator** pressure control, and other auxiliary systems, **shall** prevent the escalation of AOOs to accident conditions.

8.3.3 Turbine generators

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

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

8.4 Means of shutdown

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

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

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

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

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

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

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

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

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

8.4.1 Reactor trip parameters

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

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

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

There **shall** be no gap in trip coverage for any operating condition (such as power, temperature **or plant age)** within the OLCs. This **shall** ensure the provision of additional trip parameters if necessary. ~~A different level of effectiveness may be acceptable for the additional trip parameters.~~

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

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

8.4.2 Reliability

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

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

8.4.3 Monitoring and operator action

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

The need for manual shutdown actuation **shall** be minimized.

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

8.5 Emergency core cooling system

All water-cooled nuclear power reactors **shall** be equipped with an emergency core cooling system (ECCS). The function of this safety system is to transfer heat from the reactor core

following a loss of reactor coolant that exceeds makeup capability. All equipment required for correct operation of the ECCS **shall** be considered part of the system or its safety support system(s).

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

The design **shall take into account** the effect on core reactivity of the mixing of ECCS water with reactor coolant water, including possible mixing due to in-leakage.

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

1. All fuel **assemblies and components** in the reactor ~~and all fuel assemblies~~ are kept in a configuration such that continued removal of the residual heat produced by the fuel can be maintained.
2. A continued cooling flow (recovery flow) 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 **shall** be such that impediment to the recovery of coolant following a loss of coolant accident by debris or other material is avoided.

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

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

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

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

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

Intermediate or secondary cooling piping loops **shall** have leak detection, whether the ECCS recovery system is inside or outside of containment, with the leak detection being such that 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 **shall** have no detrimental effect on plant safety.

8.6 Containment

8.6.1 General Requirements

Each nuclear power reactor **shall** be installed within a containment structure, **so as** to minimize the release of radioactive materials to the environment during **operational states** and DBAs. Containment **shall** also assist in mitigating the consequences of **DECs**. **In particular, the containment and its safety features shall be able to perform their credited functions during accident conditions, including melting of the reactor core.**

~~The containment system is designed for all AOOs and accident conditions.~~

The containment **shall** be a safety system and **shall** include complementary design features, both of which **shall** be subject to the respective design ~~expectations~~ **requirements** provided in this regulatory document.

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

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

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

The containment **shall** include at least the following subsystems:

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

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

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

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

8.6.2 Strength of the containment structure

The strength of the containment structure **shall** provide sufficient margins of safety based on potential internal overpressures, underpressures, temperatures, dynamic effects such as missile generation, and reaction-forces anticipated to result in the event of DBAs. ~~Application of~~ Strength

margins **shall be applied** to access openings, penetrations, and isolation valves, and to the containment heat removal system.

The margins **shall** reflect:

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

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

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

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

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

8.6.3 Capability for pressure tests

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

8.6.4 Leakage

Leakage rate limits

The safety leakage rate limit **shall** assure that:

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

The design leakage rate limit **shall** be:

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

Test acceptance leakage rate limits

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

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

1. for commissioning, at the containment design pressure
2. over the service lifetime of the reactor, **in accordance with applicable codes and standards** ~~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 **shall** be designed to allow individual testing of each penetration.

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

8.6.5 Containment penetrations

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

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

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

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

8.6.6 Containment isolation

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

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

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

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

Reactor coolant system auxiliaries that penetrate containment

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

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

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

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

1. **The** design parameters 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.
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, **shall** be provided with two isolation barriers that meet the following **requirements**:

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

Closed systems

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

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

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

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

8.6.7 Containment airlocks

Personnel access to the containment **shall take place** ~~be~~ through airlocks that are equipped with doors that are interlocked to ensure that at least one of the doors is closed during **operational states and accident conditions.**

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

8.6.8 Internal structures of the containment

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

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

8.6.9 Containment pressure and energy management

The design **shall** enable heat removal and pressure reduction in the reactor containment in **operational states and accident conditions.** Systems designed for this purpose **shall be treated as** ~~considered~~ part of the containment system, and be capable of:

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

8.6.10 Control and clean up of the containment atmosphere

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

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

The design **shall** also:

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

8.6.11 Coverings, coatings and materials

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

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

8.6.12 Design extension conditions ~~Severe accidents~~

Following onset of core damage, the containment boundary **shall** be capable of contributing to the reduction of radioactivity releases to allow sufficient time for the implementation of offsite emergency procedures. This **requirement** applies to ~~a representative set of severe accidents~~ **DECs with core damage**.

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

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

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

The design authority ~~should consider~~ **shall demonstrate that** ~~incorporation of~~ complementary design features **have been incorporated** that will:

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

8.7 Heat transfer to an ultimate heat sink

The design **shall** include systems for transferring residual heat from SSCs important to safety to an ultimate heat sink. This **overall** function **shall** be subject to very high levels of reliability during **operational states and accident conditions.** All systems that contribute to the transport of heat by conveying heat, providing power, or supplying fluids to the heat transport systems,

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

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

1. acceptable conditions can be maintained in SSCs
2. radioactive materials can be confined
3. releases to the environment can be limited

8.8 Emergency heat removal system

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

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

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

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

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

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

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

8.9 Electrical power systems

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

1. **sufficient capacity to support the safety functions of the connected loads in operational states and accident conditions**
2. **availability and reliability is commensurate with the safety significance of the connected loads**

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

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

The design shall specify:

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

The electrical power systems shall include appropriate protection, control, monitoring and testing facilities.

8.9.1 Standby and emergency power systems

The **standby and** emergency power **systems shall** have sufficient capacity and reliability, for a specified mission time, **and in the presence of a single failure** to provide the necessary power to:

1. maintain the plant in a safe **shutdown** state and ensure nuclear safety in **accident conditions**
2. **support severe accident management actions**

Dedicated onsite fuel storage facilities shall have a sufficient quantity of fuel to operate standby and emergency power sources while supplying connected loads.

The preferred power supply (PPS) to the electrical power systems shall be from offsite power or the main generator.

The design shall:

1. **identify all events for which actuation of standby and emergency power sources are required**
2. **specify the required start-up time and safety load energization times for standby and emergency power sources such that they are available in a time commensurate with the safety function of the connected loads**
3. **specify conditions for electrical protection to trip standby and emergency power sources to protect equipment from significant failure**
4. **minimize challenges to standby and emergency power supplies as a result of an electrical system disturbance or transient condition**
5. **specify requirements for standby and emergency power supplies including all support auxiliaries and fuel supplies**

~~These expectations requirements **shall** be met following a common-cause loss of offsite power where this may occur as a result of a PIE, and in the presence of a single failure in the EPS.~~

The design of the emergency power system shall take into account common-cause failures involving loss of normal power supply and standby power supply (if applicable). The

emergency power system shall be electrically independent, physically separate and diverse from normal and standby power systems.

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

~~The EPS system **shall** include appropriate control, monitoring and testing facilities.~~

The **standby and** emergency power **sources shall**:

1. **be preferably** initiated automatically or manually ~~following a DBA or DEC as determined by the nuclear safety requirements of the plant~~
2. be **capable of being periodically tested** under load conditions representing full load demand and **full mission time**

The design of the DC power systems and uninterruptible AC power systems (if applicable) shall specify operating mission times when performing the intended safety functions of the connected loads and meet the capacity requirements of section 7.10.

The design shall include provisions for periodic testing for DC power and uninterruptible AC power supplies to confirm their capability.

8.9.2 Alternate AC power supply

The electrical power system design shall include provisions for mitigating the complete loss of onsite and offsite AC power. This is accomplished by the use of an onsite or offsite portable or transportable power sources, or a combination of these.

The alternate AC power source shall be available and located at or nearby the NPP, and shall:

1. **be connectable to but not normally connected to the offsite or onsite standby and emergency AC power systems**
2. **have minimum potential for common mode failure with offsite power or the onsite standby and emergency AC power sources**
3. **be available in a timely manner after the onset of a station blackout**
4. **have sufficient capacity and reliability for operation of all systems required for coping with station blackout and for the time required to bring and maintain the plant in a safe shutdown state**

The design shall include provision for periodic capacity testing of the alternate power supply to confirm its capability to cope with a station blackout event.

8.10 Control facilities

8.10.1 Main control room

The design **shall** provide for a main control room (MCR) from which the plant can be safely operated, and from which measures can be taken to maintain the plant in a safe state or to bring it back into such a state after the onset of AOOs and **accident conditions.**

The design **shall** identify events both internal and external to the MCR ~~that~~ **which** may pose a direct threat to its continued operation, and **shall** provide practicable measures to minimize the effects of these events.

The safety functions **that can be** initiated by automatic control logic in response to an accident **shall be** capable of being initiated manually from the **MCR**. ~~main and secondary control rooms~~

The layout of the controls and instrumentation, and the mode and format used to present information, **shall** provide operating personnel with an adequate overall picture of the status and performance of the plant and provide the necessary information to support operator actions.

The design of the MCR **shall be** such that appropriate lighting levels and thermal environment are maintained, and noise levels **shall** be minimized in accordance with applicable standards and codes.

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

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

The design **shall** provide visual and, if appropriate, audible indications of plant ~~states~~ **conditions** and processes that have deviated from normal operation and that could affect safety.

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

The MCR **shall** be provided with secure communication channels to the emergency support centre and to offsite emergency response organizations, and to allow for extended operating periods.

8.10.1.1 Safety parameter display system

The MCR **shall** contain a safety parameter display system that presents sufficient information on safety-critical parameters for the diagnosis and mitigation of **accident conditions.**

The safety parameter display system **shall** have the following capabilities:

1. Display safety critical parameters within the full range expected in **operational states and accident conditions**.
2. Track data trends.
3. Indicate when process or safety limits are being approached or exceeded.
4. Display the status of safety systems.

The safety parameter display system **shall** be 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 **shall be** integrated and harmonized with the overall control room **human-system** ~~system~~ interface design.

8.10.2 Secondary control room

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

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

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

Safety functions initiated by automatic control logic in response to an accident **shall** also be capable of being initiated manually from ~~both the MCR and~~ the SCR.

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

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

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

The SCR **shall be** equipped with a safety parameter display system similar to that in the MCR. As a minimum, this display system **shall** provide the information required to facilitate ~~the management of the reactor~~ **placing and keeping the plant in a safe shutdown state** when the MCR is uninhabitable.

The SCR **shall be** provided with secure communication channels to the emergency support centre and to offsite emergency response organizations.

The SCR **shall** allow for extended operating periods.

8.10.3 Emergency support centre

The design **shall** provide for an **onsite** 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 **shall** ensure that appropriate lighting levels and thermal environment are maintained, and that noise levels are minimized in accordance with applicable standards and codes.

The emergency support centre **shall** include 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, **shall be** accessible from the emergency support centre.

The emergency support centre **shall** include secure means of communication with the MCR, the SCR, and other important points in the plant, and with onsite and offsite emergency response organizations.

The design **shall** ensure that the emergency support centre:

1. includes provisions to protect occupants over protracted periods from the hazards resulting from **accident conditions** ~~a severe accident~~
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~~ **requirements shall** apply:

1. there are clear, well-defined, validated, and readily available operating procedures that identify the necessary actions
2. there is instrumentation in the control rooms to provide clear and unambiguous indication of the necessity for operator action
3. following indication of the necessity for operator action inside the **control rooms** ~~MCR~~, there is at least **30 minutes** available before the operator action is required
4. following indication of the necessity for operator action outside the **control rooms** ~~MCR~~, there is a minimum of **1 hour** 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 activities such as ~~**the**~~ diagnosing the event and accessing ~~**to**~~ the remote station.

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

8.11 Water treatment and control

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

The design of the NPP **shall** minimize the generation of radioactive and hazardous waste. The design **shall** also include adequate provision for the safe onsite handling and storage of radioactive and hazardous wastes, for a period of time consistent with options for offsite management or disposal.

8.11.1 Control of liquid releases to the environment

To ensure that emissions and concentrations remain within prescribed limits, the design **shall** include suitable means for controlling liquid releases to the environment in a manner that conforms to the ALARA principle.

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

8.11.2 Control of airborne material within the plant

The design **shall** include gaseous waste management systems capable of:

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

The design **shall** provide a ventilation system with an appropriate filtration system capable of:

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

8.11.3 Control of gaseous releases to the environment

The ventilation system **shall** include filtration that will:

1. control the release of gaseous contaminants and hazardous substances to the environment
2. ensure conformation to the ALARA principle
3. maintain airborne contaminants within prescribed limits

The filtration system **shall** reliably achieve the necessary retention factors under the expected prevailing conditions, and **shall** be designed in a manner that facilitates appropriate efficiency testing.

8.12 Fuel handling and storage

The design shall provide barriers to prevent the insertion of incorrect, defective or damaged fuel into the reactor.

The design shall include provisions to prevent contamination of the fuel and the reactor.

The design shall meet the requirements found in RD-327, *Nuclear Criticality Safety*.

8.12.1 Handling and storage of non-irradiated fuel

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

1. ensure nuclear criticality safety by
    a. maintaining an approved subcriticality margin by physical means or processes, preferably by the use of geometrically safe configurations, under both normal and credible abnormal conditions,
    b. minimizing onsite consequences to personnel of postulated criticality accidents, and
    c. mitigating offsite consequences of postulated criticality accidents
2. permit appropriate maintenance, periodic inspection, and testing of components important to safety
3. permit inspection of non-irradiated fuel
4. prevent loss of or damage to the fuel
5. meet Canada's safeguards requirements for recording and reporting accountancy data, and for monitoring flows and inventories related to non-irradiated fuel containing fissile material

8.12.2 Handling and storage of irradiated fuel

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

1. ensure nuclear criticality safety by
    a. maintaining an approved subcriticality margin by physical means or processes, preferably by the use of geometrically safe configurations, under both normal and credible abnormal conditions,
    b. minimizing onsite consequences to personnel of postulated criticality accidents, and
    c. mitigating offsite consequences of postulated criticality accidents
2. permit adequate heat removal **in operational states and accident conditions**
3. permit inspection of irradiated fuel
4. permit periodic inspection and testing of components important to safety
5. prevent the dropping of **irradiated** fuel in transit
6. prevent unacceptable handling stresses on fuel elements or fuel assemblies
7. prevent the inadvertent dropping of heavy objects and equipment on fuel assemblies
8. permit inspection and safe storage of suspect or damaged fuel elements or fuel assemblies
9. provide proper means for radiation protection
10. adequately identify individual fuel modules
11. facilitate maintenance and decommissioning of the fuel storage and handling facilities
12. facilitate decontamination of fuel handling and storage areas and equipment when necessary
13. ensure implementation of adequate operating and accounting procedures to prevent loss of fuel
14. include measures to prevent a direct threat or sabotage to irradiated fuel
15. meet Canada's safeguards requirements for recording and reporting accountancy data, and for monitoring flows and inventories related to irradiated fuel containing fissile material

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

1. controlling the chemistry and activity of any water in which irradiated fuel is handled or stored
2. monitoring and controlling the water level in the fuel storage pool
3. detecting leakage
4. preventing the pool from emptying in the event of a pipe break
5. **sufficient space to accommodate the entire reactor core inventory at all times**

The design of irradiated fuel storage pools shall include means for preventing the uncovering of fuel in the pool in operational states and accident conditions.

The design for a water pool used for fuel storage shall include provisions for DECs by:

1. **ensuring that boiling in the pool does not result in structural damage**
2. **providing temporary connections to enable the refill of the pool using temporary supplies**
3. **providing temporary connections to heat removal systems for power and cooling water**
4. **providing hydrogen mitigation in the spent fuel pool area**
5. **ensuring that severe accident management actions related to the spent fuel pool can be carried out in the absence of the shielding normally provided by the pool water**

8.12.3 Detection of failed fuel

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

8.13 Radiation protection

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

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

8.13.1 Design for radiation protection

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

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

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

Access routes **shall be** shielded where needed.

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

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

8.13.2 Access and movement control

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

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

8.13.3 Monitoring

Equipment **shall** be provided to ensure that there is adequate radiation monitoring in **operational states and accident conditions.**

Stationary alarming dose rate meters **shall** be provided:

1. for monitoring the local radiation dose rate at places routinely occupied by operating personnel
2. where the changes in radiation levels may be such that access may be limited for periods of time
3. to indicate, **automatically and in real-time**, the general radiation level at appropriate locations in **operational states and accident conditions**
4. to give sufficient information in the control room or at the appropriate control ~~position~~ **location for operational states and accident conditions**, to enable plant personnel to initiate corrective actions when necessary

Monitors **shall** be provided for measuring the activity of radioactive substances in the atmosphere:

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

Facilities **shall** be provided for monitoring individual doses to and contamination of personnel.

Stationary equipment and laboratory facilities **shall** be provided to determine the concentration of selected radionuclides in fluid process systems as appropriate, and in gas and liquid samples taken from plant systems or the environment.

Stationary equipment **shall** be provided for monitoring the effluents prior to or during discharge to the environment.

8.13.4 Sources

The design **shall** provide for:

1. appropriate disposal of radioactive materials, either to onsite storage or through removal from the site

2. reduction in the quantity and concentration of radioactive materials produced
3. control of dispersal within the plant
4. control of releases to the environment
5. decontamination facilities for equipment, and for handling any radioactive waste arising from decontamination activities
6. minimization of radioactive waste generation

8.13.5 Monitoring environment impact

The design **shall** provide 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
4. the possibility of any unauthorized discharge routes

9. Safety Analysis

9.1 General

A safety analysis of the plant design **shall** include hazard analysis, deterministic safety analysis, and probabilistic safety assessment techniques. The safety analysis **shall** demonstrate achievement of all levels of defence in depth, and confirm that the design is capable of meeting the applicable expectations, dose acceptance criteria, and safety goals.

Radioactive sources other than the reactor core, such as the irradiated fuel bay, shall be considered. Multi-unit impacts, if applicable, shall be included.

The first step of each part of the safety analysis **shall** identify PIEs using a systematic methodology such as failure modes and effects analysis. Both direct and indirect events **shall** be considered in PIE identification.

9.2 Analysis objectives

The safety analysis **shall be** iterative with the design process, and result in two reports: a preliminary safety analysis report, and a final safety analysis report.

The preliminary safety analysis **shall** assist in the establishment of the design-basis requirements for the items important to safety, and demonstrate whether the plant design meets applicable requirements.

The final safety analysis **shall**:

1. **reflect** the as-built plant
2. **account for postulated aging effects on SSCs important to safety**
3. **demonstrate** that the design can withstand and effectively respond to identified PIEs
4. **demonstrate** the effectiveness of the safety systems and safety support systems
5. **derive** the OLCs for the plant, including
    a. operational limits and set points important to safety
    b. allowable operating configurations, and constraints for operational procedures

6. **establish** requirements for emergency response and accident management
7. **determine** post-accident environmental conditions, including radiation fields and worker doses, to confirm that operators are able to carry out the actions credited in the analysis
8. **demonstrate that the design incorporates sufficient safety margins to cliff-edge effects**
9. **confirm** that the dose and derived acceptance criteria are met for all AOOs and DBAs
10. **demonstrate** that all safety goals have been met

9.3 Hazards analysis

Hazard analysis **shall** collect and evaluate information about the NPP to identify the associated hazards and determine those that are significant and must be addressed. A hazards analysis **shall** demonstrate the ability of the design to effectively respond to credible common-cause events.

As discussed in section 9.1, the first step of the hazards analysis **shall** identify PIEs. For each common-cause PIE, the hazard analysis **shall** identify:

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

The hazard analysis **shall** confirm that:

1. the plant design incorporates sufficient diversity and separation to cope with credible common-cause events
2. credited SSCs are qualified to survive and function during and following credible common-cause events, as applicable
3. the following criteria are met
    a. the plant can be brought to a safe shutdown state
    b. the integrity of the fuel in the reactor core can be maintained
    c. the integrity of the reactor coolant pressure boundary and containment can be maintained
    d. safety-critical parameters can be monitored by the operator

The hazard analysis report **shall** include the findings of the analysis and the basis for those findings. This report **shall** also:

1. **include** a general description of the physical characteristics of the plant that outlines the prevention and protection systems to be provided
2. **include** the list of safe shutdown equipment
3. **define** and describe the characteristics associated with hazards for all areas that contain hazardous materials
4. **describe** the performance criteria for detection systems, alarm systems, and mitigation systems, including requirements such as seismic or environmental qualification
5. **describe** the control and operating room areas and the protection systems provided for these areas, including additional facilities for maintenance and operating personnel
6. **describe** the operator actions and operating procedures of importance to the given analysis
7. **identify** the plant parameters for which the event is limiting

8. **explain** the inspection, testing, and maintenance parameters needed to protect system integrity
9. **define** the emergency planning and coordination requirements for effective mitigation, including any necessary measures to compensate for the failure or inoperability of any active or passive protection system or feature

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
6. demonstrate that AOOs and DBAs can be managed by automatic response of safety systems in combination with prescribed operator actions
7. **demonstrate that DECs can be prevented or mitigated by complementary design features and prescribed operator actions**

The requirements 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 **and the potential for significant radioactive releases to the environment**
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~~ **site-specific quantitative** assessments for the occurrence of core damage states and major offsite releases
4. identify systems for which design improvements or modifications to operating procedures could reduce the probability of severe accidents or mitigate their consequences
5. assess the adequacy of plant accident management and emergency procedures
6. **consider the potential effects of human errors**

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

10. Environmental Protection and Mitigation

10.1 Design for environmental protection

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

A systematic approach **shall be** 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 **shall** demonstrate through process, monitoring, control, prevention, and mitigation measures that the releases of nuclear and hazardous substances will conform to the ALARA principle.

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

Some of the factors that **shall be** considered include:

1. resource requirements for the 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
8. impact of water output on the thermal regime of the receiving environment

Technological options **shall be** considered in establishing design objectives for controlling and monitoring releases during startup, normal operation, shutdown, and potential abnormal and emergency situations. Appropriate limits **shall be** included in the plant OLCs.

Technological options for the design of cooling water systems **shall** consider ~~a closed-cycle~~ **the best available technology and techniques economically achievable (BATEA)** in order to minimize adverse environmental impact. ~~on aquatic biota.~~

11. Alternative Approaches

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

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

1. the alternative approach would result in an equivalent or superior level of safety
2. **the** application of the ~~expectations~~ **requirements** in this document conflicts with other rules or requirements
3. **the** application of the ~~expectations~~ **requirements** in this document would not serve the underlying purpose, or is not necessary to achieve the underlying purpose

~~4. application of the expectations requirements 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 **shall** demonstrate equivalence to the outcomes associated with the use of the ~~expectations~~ **requirements** set out in this regulatory document.

Abbreviations

ALARA	as low as reasonably achievable
AOO	anticipated operational occurrence
BATEA	**best available technology and techniques economically achievable**
BDBA	beyond design basis accident
~~CNSC~~	~~Canadian Nuclear Safety Commission~~
DBA	design basis accident
DBE	design basis earthquake
ECCS	emergency core cooling system
EHRS	emergency heat removal system
EPS	emergency power supply
GSS	guaranteed shutdown state
IAEA	International Atomic Energy Agency
I&C	instrumentation and control
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

Glossary

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

accident
Any unintended event (including operating errors, equipment failures or other mishaps), whose consequences or potential consequences of 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

environment
The components of the Earth, including:

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

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

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

external event
~~Any event that proceeds from the environment, external to a nuclear power plant, and can cause failure of structures, systems and components.~~

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

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

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

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

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

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

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

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

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.~~
3. ~~the documentation that is essential to meeting the organization's objectives~~

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

missile generation
The ~~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 startup, power operation, shutting down, shutdown, maintenance, testing and refuelling.

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

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

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

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

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

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

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

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 *and DECs***~~ are subsets of the beyond design basis accident state).

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

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

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

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

pressure boundary
A boundary of any pressure-retaining vessel, system, or component of a nuclear or non-nuclear system.

probabilistic safety assessment
A comprehensive and integrated assessment of the safety of the nuclear power plant. **The safety assessment considers the probability, progression and consequences of equipment failures or transient conditions to derive numerical estimates that provide a consistent measure of the safety of the nuclear power plant, as follows:**

1. **a Level 1 PSA identifies and quantifies the sequences of events that may lead to the loss of core structural integrity and massive fuel failures**
2. **a Level 2 PSA starts from the Level 1 results and analyses the containment behaviour, evaluates the radionuclides released from the failed fuel and quantifies the releases to the environment**
3. **a Level 3 PSA starts from the Level 2 results and analyses the distribution of radionuclides in the environment and evaluates the resulting effect on public health.**

process
Set of interrelated activities that transform inputs into outputs.

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

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~~.

safe shutdown state
A state characterized by subcriticality of the reactor in which the fundamental safety functions can be ensured and maintained stable for a long time.

safeguards
A system of international inspections and other verification activities undertaken by the International Atomic Energy Agency (IAEA) in order to evaluate, on an annual basis, Canada's compliance with its obligations pursuant to the 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 employees' 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 margin
A margin to a value of a safety variable for a barrier or a system at which damage or loss would occur. Safety margins are considered for those systems and barriers whose failure could potentially contribute to radiological releases.

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

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

severe accident
~~A beyond design basis accident that involves significant core degradation.~~

Accident conditions more severe than a design basis accident and involving significant core degradation.

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

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

A failure that results in the loss of capability of a component to perform its intended safety function(s), and any consequential failure(s) resulting from it.

station blackout
A complete loss of alternating current (AC) power from offsite and onsite main generator, standby and emergency power sources. Note that it does not include failure of uninterruptible AC power supplies (UPS) and DC power supplies. It also does not include failure of alternate AC power.

structures, systems and components (SSCs)
A general term encompassing all of the elements 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.

SSCs important to safety
Structures, systems and components of the nuclear power plant associated with the initiation, prevention, detection or mitigation of any failure sequence and that have the most significant impact in reducing the possibility of damage to fuel, associated release of radionuclides or both.

threat and risk assessment
A threat and risk assessment is an evaluation of the adequacy of an existing or a proposed physical protection system designed to safeguard against:

1. intentional acts that could pose a threat to the security of the nuclear facility
2. the exploitation of weaknesses in the physical protection measures of a nuclear facility

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

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

ultimate heat sink
A medium to which the residual heat can always be transferred and is normally an inexhaustible natural body of water or the atmosphere.

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

vital area
As defined in the *Nuclear Security Regulations,* a vital area means an area inside a protected area containing equipment, systems, devices or a nuclear substance, the sabotage of which could or would likely pose an unreasonable risk to the health and safety of persons, arising from exposure to radiation.