Canada's Nuclear Regulator

Design of Small Reactor Facilities

RD-367

June 2011

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Canada

Design of Small Reactor Facilities
Regulatory Document RD-367

Catalogue number CC172-71/2011E-PDF
ISBN 978-1-100-18751-8

Published by the Canadian Nuclear Safety Commission June 2011

Également publié en français sous le titre de : *Conception des installations dotées de petits réacteurs*

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

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

Publishing History:
June 2011 Version 1.0

Preface

This regulatory document sets out the requirements of the Canadian Nuclear Safety Commission (CNSC) for the design of new small reactor facilities. It establishes a set of design requirements that aligns with accepted national and international codes and standards.

A small reactor facility is defined as a reactor facility containing a reactor with a power level of less than approximately 200 megawatts thermal (MWt) that is used for research, isotope production, steam generation, electricity production or other applications.

The graded approach may be used for the design of small reactor facilities. The graded approach is a method in which the stringency of the design measures and analyses applied is commensurate with the level of risk posed by the reactor facility. Designs using the graded approach shall demonstrate they meet the safety objectives and the requirements set out in this regulatory document. Further information can be found in the International Atomic Energy Agency (IAEA) Safety Standards Series No. NS-R-4, *Safety of Research Reactors*.

The scope of RD-367, *Design of Small Reactor Facilities*, goes beyond IAEA NS-R-4 to address the interfaces between reactor design and topics such as environmental protection, radiation protection, aging, human factors, security, safeguards, transportation, and accident and emergency response planning.

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

Table of Contents

Design of Small Reactor Facilities

1. Introduction

1.1 Purpose

This regulatory document sets out the requirements of the Canadian Nuclear Safety Commission (CNSC) for the design of new small reactor facilities.

1.2 Scope

A small reactor facility is defined as a reactor facility containing a reactor with a power level of less than approximately 200 megawatts thermal (MWt) that is used for research, isotope production, steam generation, electricity production or other applications.

This document is technology neutral and includes:

- safety goals and objectives for the design
- safety concepts in the design
- safety management principles
- design of structures, systems and components
- safety, security and engineering aspects of the reactor facility features and layout
- integration of safety assessments and the design process

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

This document is consistent with the philosophy and technical content of modern national and international codes and standards. In particular, it is based in part on the International Atomic Energy Agency's (IAEA) publication, *Safety of Research Reactors,* IAEA Safety Standards Series No. NS-R-4, 2005.

1.3 Relevant regulations

The relevant sections of the regulations made under the *Nuclear Safety and Control Act* (NSCA) relevant to this document include:

- Paragraph 3(1)(*d*) of the *General Nuclear Safety and Control Regulations* stipulates that an application for a licence shall contain, in addition to other information, "a description of any nuclear facility, prescribed equipment or prescribed information to be encompassed by the licence".

- Paragraph 3(1)(*e*) of the *General Nuclear Safety and Control Regulations* stipulates that an application for a licence shall contain, in addition to other information, "the proposed measures to ensure compliance with the Radiation Protection Regulations and the Nuclear Security Regulations".
- Paragraph 3(1)(*g*) of the *General Nuclear Safety and Control Regulations* stipulates that an application for a licence shall contain, in addition to other information, "the proposed measures to control access to the site of the activity to be licensed and the nuclear substance, prescribed equipment or prescribed information".
- Paragraph 3(1)(*h*) of the *General Nuclear Safety and Control Regulations* stipulates that an application for a licence shall contain, in addition to other information, "the proposed measures to prevent loss or illegal use, possession or removal of the nuclear substance, prescribed equipment or prescribed information".
- 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".
- Paragraph 5(*f*) of the *Class I Nuclear Facilities Regulations* stipulates that an application for a licence to construct a Class I nuclear facility shall contain, in addition to other information, "a preliminary safety analysis report demonstrating the adequacy of the design of the nuclear facility".
- Paragraph 5(*g*) of the *Class I Nuclear Facilities Regulations* stipulates that an application for a licence to construct a Class I nuclear facility shall contain, in addition to other information, "a proposed quality assurance program for the design of the nuclear facility".
- Paragraph 12(1)(*c*) of the *General Nuclear Safety and Control Regulations* stipulates that every licensee shall "take all reasonable precautions to protect the environment and the health and safety of persons, and to maintain the security of nuclear facilities and of nuclear substances".
- 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".
- Paragraph 5(*a*) of the *Class I Nuclear Facilities Regulations* stipulates that an application for a licence to construct a Class I nuclear facility shall contain, in addition to other requirements, "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".
- Paragraph 5(*i*) of the *Class I Nuclear Facilities Regulations* stipulates that an application for a licence to construct a Class I nuclear facility shall contain, in addition to other requirements, information on "the effects on the environment and the health and safety of persons that may result from the construction, operation and decommissioning of the nuclear facility, and the measures that will be taken to prevent or mitigate those effects".
- Paragraph 6(*h*) of the *Class I Nuclear Facilities Regulations* stipulates that an application for a licence to operate a Class I nuclear facility shall contain, in addition to other information, "the effects on the environment and the health and safety of persons that may result from the operation and decommissioning of the nuclear facility".

- Paragraph 7(*f*) of the *Class I Nuclear Facilities Regulations* stipulates that an application for a licence to decommission a Class I nuclear facility shall contain, in addition to other information, "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".

2. Graded Approach

The graded approach is a method in which the stringency of the design measures and analyses applied are commensurate with the level of risk posed by the reactor facility.

Designs using the graded approach shall demonstrate that the safety objectives and the requirements in this document are met.

Licensees or applicants may find further guidance on use of the graded approach in IAEA NS-R-4, *Safety of Research Reactors.*

2.1 Application of graded approach

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

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

3. Safety Objectives and Concepts

3.1 General nuclear safety objective

Small reactor facilities shall be designed and operated in a manner that will protect the health, safety and security of persons and the environment from unreasonable risk, and implement Canada's international commitments on the peaceful use of nuclear energy. This objective relies on the establishment and maintenance of effective defences against radiological and hazardous substances.

The general nuclear safety objective is supported by three complementary safety objectives dealing with radiation protection, environmental protection and the technical aspects of the design.

3.1.1 Radiation protection safety objective

The reactor facility shall be designed to ensure that during normal operation, anticipated operational occurrences (AOOs), or due to any planned release of radioactive material from the reactor facility, radiation exposures within the reactor facility are kept below the limits prescribed in the *Radiation Protection Regulations* and as low as reasonably achievable (ALARA).

The design shall also provide for the mitigation of the radiological consequences of accidents.

3.1.2 Environmental protection safety objective

The reactor facility shall be designed to ensure that during normal operation, anticipated operational occurrences and design basis accidents, there are no detrimental significant adverse effects on the environment as required by the *Canadian Environmental Assessment Act* (CEA Act).

The design shall also provide for the mitigation of the environmental consequences of beyond design basis accidents, to the extent practicable.

3.1.3 Technical safety objectives

The reactor facility shall be designed to ensure that all reasonably practicable measures to prevent accidents in the reactor facility are provided and that the consequences of accidents, if they do occur, are mitigated. 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. The likelihood of accidents with serious radiological consequences is expected to be extremely low.

3.2 Safety concepts

3.2.1 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 layers of overlapping provisions, so that if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public. This concept is applied throughout the design process and operation of the reactor facility to provide a series of levels of defence aimed at preventing accidents and to ensure appropriate protection in the event that prevention fails.

The reactor facility design shall meet the safety objectives of all five levels of defence in depth as follows:

Level 1

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

Level 2

The objective of the second level of defence is to detect and intercept deviations from normal operation in order to prevent anticipated operational occurrences from escalating to accident conditions, and to return the reactor facility to a state of normal operation.

Level 3

The objective of the third level of defence is to minimize the consequences of accidents.

Level 4

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

Level 5

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

3.2.2 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.

The design shall minimize:

- challenges to the integrity of physical barriers
- failure of a barrier when challenged
- failure of a barrier as a consequence of failure of another barrier

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

The design shall determine the need for an exclusion zone based on several factors, including:

- evacuation needs (refer to section 4.3)
- land usage needs
- security requirements
- environmental factors

4. Safety Requirements

The licensee or applicant is responsible for ensuring that the design meets the following safety requirements.

4.1 Application of defence in depth

Defence in depth shall be incorporated into the design to meet the objectives of the five levels of defence in depth.

The design shall provide multiple physical barriers to the uncontrolled release of radioactive materials to the environment.

Level 1

The design shall be conservative and the construction shall be of sufficiently high quality to provide confidence that reactor facility failures and deviations from normal operations are minimized and accidents are prevented.

Level 2

The design shall provide for control of the reactor facility behaviour during and following a postulated initiating event (PIE) using inherent and engineered design features to minimize or exclude uncontrolled transients, to the extent possible.

Level 3

The design shall provide for inherent safety features, fail-safe design, engineered design features and procedures that minimize the consequences of design basis accidents (DBAs). Automatic activation of the engineered design features shall be provided to minimize the need for operator actions in the early phase of a DBA.

Level 4

The design shall provide for equipment and procedures to manage accidents and mitigate their consequences, to the extent practicable.

Adequate protection shall be provided for the confinement function.

Level 5

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

4.2 Safety functions

The design shall ensure that fundamental safety functions are available in normal operation, and during and following AOOs and DBAs. These functions include:

- control of reactivity
- removal of heat from the core
- confinement of radioactive material
- control of operational discharges and hazardous substances
- limitation of accidental releases
- monitoring of safety critical parameters to guide operator actions

The above functions shall also facilitate response to beyond design basis accidents (BDBAs), to the extent practicable.

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

4.3 Radiation protection and acceptance criteria

4.3.1 Qualitative safety goals

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

- Individual members of the public are provided a level of protection from the consequences of reactor facility operation such that there is no significant additional risk to the life and health of individuals.
- Societal risks to life and health from reactor facility operation should not significantly add to other societal risks.

4.3.2 Radiation protection for normal operation

The design shall be such that during normal operation, including maintenance and decommissioning, doses are controlled to remain below the limits prescribed in the *Radiation Protection Regulations*. In addition, radiation doses to the public and to site personnel shall be ALARA.

All actual and potential sources of radiation shall be identified and provision shall be made to ensure that sources are kept under strict technical and administrative control.

4.3.3 Dose acceptance criteria for AOOs and DBAs

The design shall meet the following dose acceptance criteria:

- 0.5 millisieverts (mSv) for any AOO
- 20 millisieverts (mSv) for any DBA

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

4.3.4 Quantitative safety goals for BDBAs

The design shall meet the following three quantitative safety goals:

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, whose release to the environment requires temporary evacuation of the local population, shall be less than 10^{-5} per reactor year.

Large release frequency

The sum of frequencies of all event sequences, whose release to the environment requires long-term relocation of the local population, shall be less than 10^{-6} per reactor year.

4.4 Accident prevention, mitigation and management

The design shall include provisions 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.

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

The design shall apply the principles of defence in depth to minimize sensitivity to PIEs and the need for operator intervention in order to bring the reactor to a safe state.

Following a PIE, the reactor facility shall be rendered safe by including:

- inherent safety features
- passive safety features or action of control systems
- action of safety systems
- specified procedural actions

4.5 Operational limits and conditions

The operational limits and conditions (OLCs) shall be established to ensure that the reactor facility operates in accordance with design assumptions and intent, and shall include the limits within which the reactor facility has been shown to be safe.

5. Safety Analysis

The overall safety assessment of the reactor facility design includes hazards analysis, deterministic safety analysis and probabilistic safety analysis techniques.

These analyses shall identify all sources of radioactive and hazardous materials in order to evaluate potential radiation doses to workers at the reactor facility and to the public, and to evaluate potential effects of the reactor facility on the environment.

The safety analysis confirms that the design is capable of meeting the safety requirements, dose acceptance criteria and safety goals. The safety analysis also contributes to demonstrating that the reactor facility provides defence in depth.

5.1 Safety analysis objectives

As per *Class I Nuclear Facilities Regulations*, a preliminary safety analysis report demonstrating the adequacy of the facility design is required for an application for a licence to construct a Class I nuclear facility. A final safety analysis report is required for an application for a licence to operate a Class I nuclear facility.

The final safety analysis shall:

- reflect the 'as-built' reactor facility, including aging effects
- demonstrate that the design can withstand and effectively respond to identified PIEs
- demonstrate the effectiveness of the safety systems and safety support systems
- derive the OLCs for the reactor facility, including:
  a. operational limits and set points important to safety
  b. allowable operating configurations and constraints for operational procedures
- establish requirements for emergency response and accident management
- 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 safety analysis
- confirm that the dose and derived acceptance criteria are met for all AOOs and DBAs
- demonstrate that all safety goals for BDBAs, including severe accidents, have been met

5.2 Hazards analysis

A hazards analysis shall demonstrate the ability of the design to effectively respond to credible common-cause events.

For each common-cause PIE, the hazards analysis shall identify:

- applicable acceptance criteria
- the hazardous materials in the reactor facility and at the reactor facility site
- 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)
- operator actions and operating procedures for the event
- reactor facility or operating procedure parameters for which the event is limiting

The hazards analysis shall confirm that:

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

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

- include a general description of the physical characteristics of the reactor facility that outlines the prevention and protection systems to be provided
- include the list of equipment needed to bring the reactor facility to a safe shutdown state
- define and describe the characteristics associated with hazards for all areas that contain hazardous materials
- describe the performance criteria for detection systems, alarm systems and mitigation systems, including requirements such as seismic or environmental qualification
- describe the control and operating room areas and the protection systems provided for these areas, including additional facilities for maintenance and operating personnel
- describe the operator actions and operating procedures of importance to the given analysis
- identify the reactor facility parameters for which the event is limiting
- explain the inspection, testing and maintenance parameters needed to protect system integrity
- 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

5.3 Deterministic safety analysis

The deterministic safety analysis shall:

- confirm that OLCs comply with the assumptions and intent of the design for normal operation of the reactor facility
- characterize the events that are appropriate for the site and reactor facility design
- analyze and evaluate event sequences that result from failure of SSCs
- compare the results of the safety analysis with derived acceptance criteria, design limits, dose acceptance criteria and safety goals
- establish and confirm the design basis
- demonstrate that AOOs, DBAs and BDBAs can be managed by automatic response of safety systems in combination with prescribed operator actions

Detailed requirements for the deterministic safety analysis are provided in CNSC regulatory document RD-308, *Deterministic Safety Analysis for Small Reactor Facilities.*

5.4 Probabilistic safety assessment

The probabilistic safety assessment (PSA) shall:

- identify accident scenarios with the potential for significant core degradation
- 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

- provide probability assessments for the occurrence of core damage states and major off-site releases
- identify systems for which design improvements or modifications to operating procedures could reduce the probability of severe accidents or mitigate their consequences
- assess the adequacy of reactor accident management and emergency procedures
- consider the potential effects of human actions on system reliability

The PSA is conducted using a graded approach to each of the requirements specified in CNSC regulatory standard S-294, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*.

6. Safety Management During Design

The safety management system shall ensure that the reactor facility design:

- meets Canadian regulatory requirements
- meets all design specifications, including those confirmed by safety analysis
- takes into account current safety practices
- fulfills the requirements of an effective quality assurance or management system program
- incorporates only those design changes that have been justified by technical and safety assessments

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

- a clear division of responsibilities with corresponding lines of authority and communication
- clear interfaces between the groups engaged in different parts of the design, and between designers, utilities, suppliers, builders and contractors, as appropriate
- policies, processes and procedures that form part of a quality assurance or management system program
- a positive safety culture throughout all levels of the organization

6.1 Design authority

The licensee shall be ultimately responsible for the design of the reactor facility.

During the design phase a formal design authority shall be established. The tasks and functions of the design authority shall be formally documented.

The design authority shall achieve the following objectives during the design phase:

- establish a knowledge base of all relevant aspects of the reactor facility design and keep it up to date, while taking experience and research findings into account
- ensure the availability of the design information that is needed for safe reactor facility operation and maintenance
- establish the requisite security clearances and associated security measures to protect prescribed, designated and classified material

- maintain design configuration control
- review, verify, approve and document design changes
- establish and control the necessary interfaces with responsible designers or other suppliers engaged in design work
- ensure that the necessary engineering and scientific skills and knowledge have been maintained
- ensure 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

6.2 Design management

Design management policies, processes and procedures shall be established to control all aspects of the design and its evolution.

Appropriate design management shall achieve the following objectives:

- structures, systems and components important to safety meet their respective design requirements
- due account is taken of the human capabilities and limitations of personnel
- safety design information necessary for safe operation and maintenance of the reactor facility and for any subsequent reactor facility modifications is preserved
- operational limits and conditions are provided for incorporation into the reactor facility administrative and operational procedures
- the reactor facility design facilitates maintenance and aging management throughout the life of the facility
- the results of the deterministic and probabilistic safety assessments are taken into account
- due consideration is given to the prevention of accidents and mitigation of their consequences
- generation of radioactive and hazardous waste is limited to minimum practicable levels, in terms of both activity and volume
- a change control process is established to track design changes to provide configuration management during manufacturing, construction, commissioning and operation
- physical protection systems are provided to address design basis threats

6.3 Design policies, processes and procedures

Design policies, processes and procedures shall be established as part of the overall management arrangements to achieve the reactor facility design objectives.

The policies, processes and procedures shall include:

- design initiation, specification of scope and planning
- specification of design requirements

- selection of the design authority (refer to section 6.1)
- work control and planning of design activities
- specification and control of design inputs
- review of design concepts and selection
- selection of design tools and computer software
- conducting conceptual analysis
- conducting detailed design and production of design documentation and records
- conducting detailed safety analysis (refer to section 5.0)
- defining any limiting conditions for safe operation
- carrying out design verification and validation
- independence of individuals or groups performing verifications, validations and approvals
- configuration management
- management of the design and control of design changes
- identification and control of design interfaces

6.4 Proven engineering practices

Proven and accepted engineering methods, procedures and practices shall be used to ensure compliance of the design with regulations, codes and standards.

Modern codes and standards shall be identified and evaluated for applicability, adequacy and sufficiency to the design of SSCs important to safety.

Structures, systems and components important to safety shall be of proven designs and shall be designed according to appropriate codes and standards.

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 design requirements. New designs shall be tested before being brought into service and shall be monitored in service to verify that the expected behaviour is achieved.

6.5 Operational experience and safety research

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

6.6 Safety assessment

A safety assessment process shall be applied throughout the design phase of the project to ensure that the design meets safety requirements.

Before the design is submitted, an independent 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 reactor facility 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.

6.7 Design documentation

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

7. General Design Requirements

7.1 Radiation protection

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

- control access to the reactor facility
- minimize radiation exposure during maintenance and inspection
- provide shielding from direct and scattered radiation
- provide ventilation and filtering to control airborne radioactive materials
- limit the activation of corrosion products by proper specification of materials
- minimize the spread of radioactive material
- monitor radiation levels
- provide suitable decontamination facilities

7.1.1 Design for radiation protection

The shielding design shall prevent radiation exposure to the operator in operating areas from exceeding the prescribed limits.

To minimize radiation exposure, the reactor facility layout shall provide for efficient operation, inspection, maintenance and replacement activities. 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 provide radiation shielding 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 accident conditions in those parts of the reactor facility to which access is required.

7.1.2 Access and movement control

The reactor facility 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 shall provide appropriate decontamination facilities for personnel.

7.1.3 Monitoring

Equipment shall be provided to ensure that there is adequate radiation monitoring for normal operation, AOOs, DBAs and, as practicable, BDBAs.

Stationary alarming dose rate meters shall be provided:

- for monitoring the local radiation dose rate at places routinely occupied by operating personnel
- where the changes in radiation levels may be such that access may be limited for periods of time
- to indicate the general radiation level at appropriate locations in the event of AOOs, DBAs and, as far as practicable, BDBAs
- to give sufficient information in the control room or at the appropriate control location for normal operation, AOOs, DBAs and, as practicable, BDBAs to enable facility personnel to initiate corrective actions when necessary

Monitors shall be provided for measuring the airborne activity of radioactive substances in the reactor facility.

Facilities shall be provided for monitoring individual doses 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 the reactor facility or the environment in normal operation, AOOs, DBAs and, as practicable, BDBAs.

Devices for measuring radioactive surface contamination shall be provided.

7.1.4 Sources of radiation

The design shall provide for:

- appropriate disposal of radioactive materials, either to on-site storage or through removal from the site
- reduction in the quantity and concentration of radioactive materials produced

- control of dispersal within the reactor facility
- control of releases to the environment
- decontamination facilities for equipment and for handling any radioactive waste arising from decontamination activities
- minimization of radioactive waste generation

7.2 Environmental protection and mitigation

7.2.1 Design for environmental protection

The design shall make adequate provision to protect the environment and to mitigate the impact of a reactor facility 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 biophysical environmental effects of a reactor facility on the environment, and the effects of the environment on the reactor facility.

7.2.2 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.

The factors that are considered shall include:

- resource requirements for the reactor facility (e.g., fuel, energy, water)
- depletion of ground and surface water resources
- contamination of air, soil and water resources
- nuclear and hazardous substances used
- types of waste generated (e.g., gaseous, liquid, solid)
- quantities of waste generated
- impact of cooling water intake on entrainment and impingement
- 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 reactor facility OLCs.

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

7.2.3 Monitoring environmental impact

The design shall provide the means for monitoring nuclear and hazardous substance releases to the environment in the vicinity of the reactor facility.

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

7.3 Classification of structures, systems and components

Structures, systems and components shall be identified, classified and documented in a systematic, consistent and clearly defined classification scheme. The classification scheme shall include a process for assigning importance to safety.

The SSCs shall be designed, constructed and maintained such that their quality and reliability is commensurate with their classification.

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

7.4 Reactor facility design envelope

The reactor facility design envelope, which comprises the design basis and complementary design features, shall be established.

The utilization of the reactor facility shall be taken into account establishing the design envelope.

The design basis shall specify the capabilities that are necessary for the reactor facility in normal operation, AOOs and DBAs.

Conservative design measures and sound engineering practices shall be applied in the design basis for normal operation, AOOs and DBAs.

Complementary design features shall address the performance of the reactor facility for BDBAs, including selected severe accidents.

7.5 Reactor states

Reactor states shall be grouped into the following four categories: normal operation, anticipated operational occurrences, design basis accidents and beyond design basis accidents (refer to the defence in depth in sections 3.2.1 and 4.1, and the acceptance criteria in section 4.3).

The utilization of the reactor facility shall be taken into account when establishing the reactor states.

7.5.1 Normal operation

The design shall facilitate safe operation of the reactor facility 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:

- limits important to safety
- constraints on control systems and procedures
- reactor facility maintenance, testing and inspection requirements
- clearly defined operating configurations such as startup, at-power operation, shutdown, maintenance, testing, surveillance and refuelling (these configurations include relevant operational restrictions in the event of safety system and safety support system outages)

These requirements and limitations, together with the results of safety analysis, form the basis for establishing the OLCs as described in section 4.5.

7.5.2 Anticipated operational occurrences

The response of the reactor 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.

The design shall provide that SSCs not involved in the initiation of an AOO will remain operable following the AOO.

7.5.3 Design basis accidents

To prevent progression to a more severe condition that may threaten the next barrier, the design shall include provision to automatically initiate the necessary safety systems where prompt and reliable action is required in response to a PIE. Where prompt action is not necessary, provision shall be made to support timely detection of and manual response to such conditions.

The design shall take into account operator actions that may be necessary to diagnose the state of the reactor 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 reactor 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.

7.5.4 Beyond design basis accidents

Credible BDBAs shall be identified based on operational experience, engineering judgment and the results of analysis and research.

Complementary design features shall be provided with the goal of preventing accident progression and mitigating the consequences of selected severe accidents if they do occur.

Complementary design features shall include design or procedural considerations, or both.

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 an accident source term of radiological, combustible and hazardous substances for use in the specification of the complementary design features for BDBAs.

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

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

7.5.5 Severe accidents

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

Particular attention shall be placed on the prevention of potential confinement bypass in accidents involving significant core degradation.

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

Severe accident management guidelines shall be established, taking into account the reactor facility design features and the understanding of accident progression and associated phenomena.

The design shall minimize the possibility of recriticality following severe accidents.

7.6 Postulated initiating events

Postulated initiating events that can lead to AOOs or accidents shall be identified, and shall include credible failures or malfunctions of SSCs, operator errors, internal hazards, and external hazards.

7.6.1 Internal hazards

The reactor facility design shall take into account the potential for internal hazards. Appropriate preventive and mitigation measures shall be provided to ensure that safety is not compromised.

The subset of internal events that the reactor facility is designed to withstand shall be selected, and DBAs as well as BDBAs shall be determined from this subset.

Structures, systems and components 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 design shall address the possible interaction of external and internal events, such as external events initiating internal fires or floods that may lead to the generation of missiles.

Where two fluid systems operating at different pressures are interconnected, failure of the interconnection shall be addressed.

7.6.2 External hazards

The design shall take into account all natural and human-induced external events that are relevant to the design and may be linked to significant radiological risk and other hazards. The subset of external events that the reactor facility is designed to withstand shall be selected, and DBAs as well as BDBAs shall be determined from this subset.

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

7.6.3 Combinations of events

Combinations of randomly occurring individual events that could credibly lead to AOOs, DBAs or BDBAs 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.

7.7 Design rules and limits

The engineering design rules for all SSCs shall be specified. These rules shall comply with appropriate engineering safety and design practices such as Canadian Standards Association (CSA) and American Society of Mechanical Engineers (ASME) codes and standards.

SSCs to which design limits are applicable shall be identified. These design limits shall be specified for normal operation, AOOs, DBAs and, to the extent praticable, BDBAs.

7.8 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 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}.

7.8.1 Common-cause failures

The potential for common-cause failures of SSCs important to safety shall be addressed in determining where to apply the principles of diversity, separation and independence to achieve the necessary reliability.

The design shall provide sufficient physical separation between redundant divisions of safety systems, safety support systems and process systems.

The effectiveness of specified physical separation or protective measures against common-cause events shall be assessed.

Diversity shall be applied to redundant systems or components that perform the same safety function.

7.8.2 Single failure criterion

All safety groups shall be designed to function in the presence of a single failure. Each safety group shall perform all safety functions required for a PIE in the presence of any single component failure, as well as:

- all failures caused by that single failure
- all identifiable but non-detectable failures, including those in the non-tested components
- 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 associated consequential failures shall be conducted for each element of each safety group until all safety groups have been considered.

7.8.3 Fail-safe design

The principle of fail-safe design shall be applied to the design of SSCs important to safety.

7.8.4 Allowance for equipment outages

Considering utilization of the reactor facility, the design shall include provisions for adequate redundancy, reliability and effectiveness to allow for on-power maintenance and on-power testing of systems important to safety.

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

7.8.5 Shared systems

The design shall minimize the sharing of SSCs between safety systems, systems important to safety and process systems. If sharing is included in the design, it shall be demonstrated that SSC safety functions are not compromised.

7.9 Pressure-retaining structures, systems and components

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

All pressure-retaining SSCs of the reactor coolant system and auxiliaries shall be designed with an appropriate safety margin in normal operation, AOOs, DBAs and, to the extent practicable, BDBAs.

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

All pressure-boundary SSCs shall be designed to withstand static and dynamic loads anticipated in normal operation, AOOs and DBAs.

Pressure-retaining components and their layout in the reactor facility shall be designed to permit safe inspection of their pressure boundaries throughout their design life.

The design shall include measures for timely detection of degradation or changes in behaviour in pressure boundaries important to safety and include where practicable protection against postulated pressure boundary failures.

The operation of pressure relief devices shall not lead to uncontrolled releases of radioactive material or hazardous substances from the reactor facility.

Adequate isolation shall be provided at the interfaces between the reactor coolant system (RCS) and connecting systems operating at lower pressures to prevent the overpressure of such systems and possible loss of coolant accidents.

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

7.10 Equipment environmental qualification

The design shall provide for equipment environmental qualification to ensure the safety functions identified in section 4.2 can be carried out during post-accident conditions.

Equipment qualification shall also include consideration of any unusual environmental conditions that can reasonably be anticipated and that could arise during normal operation and AOOs.

Equipment credited to operate during BDBA and severe accident states shall be assessed to confirm its capacity to perform its intended function under the expected environmental conditions.

7.11 Instrumentation and control

All instrumentation and control equipment shall be designed in accordance with applicable modern codes and standards. The design shall consider normal operation, AOOs, DBAs and, to the extent practicable, BDBAs. The design shall consider the effects of aging as described in section 7.20.

7.11.1 General considerations

The design shall include provisions for instrumentation to monitor reactor facility variables and systems over the respective ranges for normal operation, AOOs, DBAs and, to the extent practicable, BDBAs, to ensure that adequate information can be obtained on reactor facility status. Particular attention shall be paid to the provision of startup instrumentation.

The design shall be such that the safety systems and any necessary support systems shall be reliably and independently operated.

The design shall include the capability to trend and automatically record measurements of any derived parameters that are important to safety.

Instrumentation shall be capable of measuring reactor facility parameters for emergency response purposes.

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

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 shall 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.

7.11.2 Use of computer-based systems or equipment

Appropriate codes and standards for the development, 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. These codes and standards shall be implemented throughout the life cycle of the system or equipment. In this respect, special attention shall be given to the software development cycle.

A top-down software development process shall be used to facilitate verification and validation activities.

Software provided by a third-party vendor that is used in systems or equipment important to safety 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 shall be systematically documented in the design documentation.

7.11.3 Post-accident instrumentation

Instrumentation and recording equipment shall be such that essential information is available to support reactor facility procedures during and following accidents.

7.12 Safety support systems

Safety support systems shall ensure that the fundamental safety functions are available during normal operation, AOO, DBA and, to the extent practicable, BDBA states.

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

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:

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

The emergency support systems shall:

- be independent of normal and backup systems
- provide continuity of the service until long term (normal or backup) service is re-established
- have a capacity margin that allows for future increases in demand
- be testable under design load conditions

7.13 Guaranteed shutdown state

The guaranteed shutdown state (GSS) shall provide a shutdown margin such that the core will remain subcritical for any credible changes in the core configuration and reactivity addition.

The design shall provide means to achieve GSS that will support safe production, experimental or maintenance activities of the reactor facility.

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

7.14 Provision for extended shutdown

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

7.15 Fire safety

The design of the reactor facility, including external buildings and SSCs integral to reactor facility safe operation, shall adhere to applicable national fire codes and standards.

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

7.15.1 General provisions

The following fire safety objectives shall be achieved:

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

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

The design of buildings or structures shall use non-combustible or fire retardant and heat resistant materials.

7.15.2 Safety to life

The design shall provide protection to workers and the public from event sequences involving fire or explosion in accordance with established radiological, toxicological and human factors criteria.

7.15.3 Environmental protection and nuclear safety

The design for fire safety 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.

7.16 Seismic qualification

The seismic qualification of all SSCs shall comply with the requirements of Canadian or equivalent standards.

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

7.16.1 Seismic design and classification

Structures, systems and components important to safety that are credited to withstand a design basis earthquake shall be identified and qualified accordingly.

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

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

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

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

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

7.18 Civil structures

7.18.1 Design

Civil structures important to safety shall be designed for normal operation, AOOs, DBAs and, to the extent practicable, BDBAs.

The required performance for the safety functions of the civil structures under normal operation, AOOs, DBAs, and BDBAs shall be specified.

Civil structures important to safety shall be designed to keep radiation levels and radioactive releases as required by section 4.3.

Civil structures important to safety shall be designed so as to minimize the probabilities and effects of internal and external hazards.

Civil structures shall be designed to meet the serviceability, strength and stability requirements for all possible load combinations under normal operation, AOO, DBA and, to the extent practicable, BDBA conditions, and in the event of external hazards.

The design shall specify and provide for all loads and load combinations, with due consideration given to the concurrence probability and loading time history. Environmental effects shall be considered in the design of civil structures and the selection of construction materials.

The required degree of leak tightness of civil structures containing radioactive material and the requirements for the ventilation system shall be specified in accordance with the safety analysis of the reactor facility and its utilization.

7.18.2 Surveillance

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

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

The design shall permit monitoring of foundation settling.

7.18.3 Lifting of large loads

The lifting of large and heavy loads, particularly those containing radioactive material, shall be accounted for in the reactor facility design. This shall include identification of the large loads, lay down areas and situations where they need to be lifted over areas of the reactor facility that are critical to safety.

7.19 Commissioning

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.

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.

7.20 Aging and wear

The design shall provide for the effects of aging and wear on SSCs important to safety.

7.21 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.

7.22 Transport and packaging for fuel and radioactive waste

The design shall incorporate appropriate features to facilitate transport and handling of new fuel, used fuel and radioactive waste in accordance with the requirements of *Packaging and Transport of Nuclear Substances Regulations.*

7.23 Escape routes and means of communication

The design shall provide a sufficient number of safe escape routes that will be available in all reactor states, including seismic events.

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

7.24 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 aspects of the design.

The human factors engineering program shall facilitate the interface between the operating personnel and the reactor facility by promoting attention to reactor facility layout and procedures, maintenance, inspection, training, commissioning, decommissioning 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-machine interface.

The human-machine interfaces in the reactor facility and, in particular, the main control room, the secondary control room and the emergency support centre 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 to confirm that the design conforms to modern human factors codes and standards, meets human factors requirements and adequately accommodates all necessary operator actions.

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

- assess the general state of the reactor facility, whether in normal operating, AOO or DBA states
- confirm that the designed automatic safety actions are being carried out
- determine the appropriate operator-initiated safety actions to be taken
- identify the parameters associated with individual plant systems and equipment
- confirm that the necessary actions can be initiated safely

Design goals shall promote the success of operator action by having 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.

7.25 Robustness against malevolent acts

The physical security protection system shall:

- use a risk-informed process, such as a threat and risk assessment (TRA), that forms the basis for a design strategy to reduce the likelihood of theft and/or sabotage of nuclear substances that are used, stored, processed or otherwise possessed in accordance with the requirements of the *General Nuclear Safety and Control Regulations* and *Class I Nuclear Facilities Regulations*
- physical security measures shall be designed in accordance with the requirements of the *Nuclear Security Regulations*, and shall also include any additional mitigation measures required to address the adversarial profile defined in the design basis threats (DBTs)

7.25.1 Design principles

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

Consistent with the defence in depth concept, 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 physical protection system shall be designed and evaluated to address DBTs. Beyond design basis threats (BDBTs) shall be assessed in order to establish means of mitigation, to the extent practicable.

7.25.2 Design methods

A methodology shall be developed for assessing the challenges imposed by DBTs and evaluating the capabilities for meeting these challenges, including a 'site-specific' TRA to identify associated threats, risks and vulnerabilities. The methodology shall apply conservative design measures and sound engineering practices.

A methodology for assessing the challenges associated with BDBTs shall be developed to determine the margins available for reactor shutdown, fuel cooling and confinement of radioactivity.

The reactor facility design shall consider the role of structures, pathways, equipment and instrumentation in providing detection, delay and response to threats.

Locations of SSCs that need to be protected shall be identified as vital areas and shall be taken into account in the design and verification of robustness.

The design shall provide a means for access control and detection, and for minimizing the number of access and egress points.

The design shall address the need for placement of civil utilities to minimize access requirements for such activities as repair and maintenance in order to reduce threats where nuclear material may be used, processed, stored or otherwise possessed including vital areas.

7.25.3 Acceptance criteria

The physical security protection system shall be designed to provide an effective detection, assessment, delay-associated response capability prior to the theft or sabotage of nuclear material.

All fundamental safety functions shall remain effective for DBTs.

For BDBTs, there shall be at least one means of reactor shutdown and core cooling; however, degradation of the confinement barrier may occur. For BDBTs, any release of radioactive material shall be within limits of the safety goals.

7.25.4 Prescribed information

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

7.26 Safeguards

The design shall ensure that the obligations arising from Canada's international agreements and requirements pertaining to safeguards and non-proliferation are met.

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 ongoing operation of that equipment.

7.27 Provision for utilization and modification

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

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

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

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

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

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

7.28 Reactor facility layout

The design shall take into account the interfaces between the safety and security provisions of the reactor facility and other aspects of the reactor facility layout.

When there are conflicting design requirements in the determination of reactor facility layout requirements, the design shall provide an assessment of options, demonstrating that an optimized configuration has been sought for the reactor facility layout.

7.29 Decommissioning

During the design, future reactor facility decommissioning and dismantling activities shall be taken into account such that:

- materials are selected for the construction and fabrication of reactor components and structures with the purpose of minimizing eventual quantities of radioactive waste and assisting decontamination
- reactor facility layout is designed to facilitate access for decommissioning or dismantling activities
- 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 Requirements

8.1 Reactor core

All foreseeable reactor core configurations from the initial core through to the equilibrium core for various appropriate operating schedules shall be considered in the core design.

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

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

The anticipated upper limit of possible deformation or other changes due to irradiation conditions shall be evaluated. These analyses shall be supported by data from experiments and from experience with irradiation.

The reactor core and associated structures and cooling systems shall:

- withstand static and dynamic loading, including thermal effects
- withstand vibration (such as flow-induced or acoustic vibration)
- ensure chemical compatibility
- meet thermal material limits
- meet radiation damage limits to materials

The reactor core shall be designed so that the reactor can be shutdown, cooled and held subcritical with an adequate margin for normal operation, AOOs and DBAs. The state of the reactor shall be assessed for selected BDBAs (refer to section 7.5).

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

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

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

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

The design of the reactor core shall be such that:

- rapid changes in reactor power can be controlled by a combination of the inherent neutronic characteristics of the core, its thermal-hydraulic characteristics and the capabilities of the control and shutdown systems for normal operation and design basis accident conditions
- power oscillations can be reliably and readily detected and controlled
- specified design limits are not exceeded during normal operation, AOOs and DBAs
- prompt criticality is avoided in any accident
- when prompt criticality can be exceeded, it is demonstrated experimentally that the resulting energy deposition does not result in damage to fuel or the reactor coolant boundary

The reactor core, including the fuel elements, reactivity control mechanisms, experimental devices, reflectors, fuel channel and structural parts, shall be designed to maintain the relevant parameters within specified limits for normal and accident conditions.

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

The reactor core design shall include provisions for a guaranteed shutdown state as described in section 7.13.

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

8.1.1 Experimental devices

This section is applicable when the reactor core employs experimental devices such as loops for fuel and material testing, irradiation sites or beam tubes.

The reactor behaviour under normal operation, transient and accident conditions shall be analyzed, including experimental devices. Any safety impact of any failure of experimental devices on the reactor core or that of any failure of the reactor core on the experimental devices shall be addressed.

A design basis shall be established for each experimental device associated with the reactor facility. The radioactive inventory of the experimental device, as well as the potential for the generation or release of energy shall be taken into consideration.

If safety devices are interconnected with the safety system, they shall be designed to maintain the quality of the safety system. The possibility of deleterious interactions with the safety system shall be assessed.

Where necessary for the safety of the reactor and the safety of the experiment, the design shall provide appropriate monitoring of the parameters for experiments in the main control room and shall include specific safety features, if necessary, for the reactor systems, experimental devices and any other related facility.

Requirements for the safe utilization of experimental devices shall be included in the OLCs.

The preliminary decommissioning plan for the reactor facility shall include the decommissioning of any experimental device.

8.1.2 Fuel elements and assemblies

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. Fuel design and design limits shall use a verified and auditable knowledge base using data from experiments and from experience with irradiation.

The fuel assembly design shall include components such as the fuel material, matrix material, cladding, spacers, support plates and movable rods inside the assembly. 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 normal operation and AOOs.

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

Fuel design limits shall include, as a minimum, limits on fuel power or temperature, fuel burn-up and leakage of fission products in the reactor cooling system.

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

In DBAs, the fuel, its 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 establish acceptance criteria for DBAs that are consistent with these expectations.

Reactor and fuel assembly design shall take into account changes in fuel management strategy or in operating conditions over the lifetime of the reactor facility.

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

At the design stage, consideration shall be given to long-term storage of irradiated fuel assemblies after discharge from the reactor (see also section 8.12).

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

8.1.3 Control system

The design shall provide the means for detecting and controlling reactivity and distributions of neutron flux. Adequate means shall be provided to maintain both bulk and spatial power distributions within a predetermined range. The reactivity control mechanisms shall limit the positive reactivity insertion rate to a level that prevents prompt criticality (unless the design allows for prompt criticality as in section 8.1), and shall meet fuel acceptance criteria during transients.

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

The maximum rate of addition of positive reactivity allowed by the reactivity control system, or by an experiment when employed, shall be specified and shall be limited to values justified.

These requirements shall apply to neutron flux in all regions of the core during normal operation, including initial startup, after shutdown, startup after shutdown, and during and after refuelling states, and during AOOs.

The reactivity 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 reactivity control system and the inherent reactor characteristics shall keep all critical reactor parameters within the specified limits for a wide range of AOOs, and shall reduce the possibility of AOOs from escalating to accident conditions.

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 normal operation, AOOs or DBAs.

Materials selection shall be such that corrosion and subsequent generation of activated corrosion products (leading to radiation field build-up) is minimized.

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

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

There shall be provisions in the design of the reactor coolant system to allow for continuous monitoring of radionuclide concentrations in the coolant during normal operation.

8.2.1 In-service coolant 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 throughout the lifetime of the reactor facility.

The design shall facilitate surveillance to determine the conditions of materials for which changes in material properties are anticipated.

8.2.2 Inventory

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

8.2.3 Cleanup

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

Provisions shall be made to monitor and control the properties of all coolant systems, as appropriate.

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 reactor coolant system (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 off-site power, by incorporating suitable redundancy, diversity and independence.

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

8.3 Secondary side cooling system

When a steam supply system is installed, the system design shall meet the applicable requirements in RD-337, *Design of New Nuclear Power Plants.*

When a steam supply system is not installed, the system design shall meet the applicable requirements set out in section 8.2.

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.

Sufficient negative reactivity shall be available in the reactivity control devices in order that the reactor can be brought to subcritical condition and maintained subcritical in normal operation and in accident conditions, with account taken of the experimental arrangements with the highest positive reactivity contribution. In the design of reactivity control devices, account shall be taken of aging and the effects of irradiation, such as burnup, changes in physical properties and the production of gas.

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 in DBAs by an adequate margin, on the assumption of a single failure.

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.

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

While resetting the means of shutdown, the maximum degree of positive reactivity and the maximum rate of increase 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 within specified limits, and the possibility of recriticality or reactivity excursion following a PIE shall be minimized.

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

One or more manual initiations suitable for emergency shutdown may be necessary; this shall be reflected in the design.

Instrumentation shall be provided and tests shall be specified to be performed to ensure that the means of shutdown are always available in the state stipulated for the given condition of the reactor. For computer-based digital reactivity control systems, verification and validation of the software shall be performed.

8.4.1 Reactor trip parameters

Derived acceptance criteria shall be specified for reactor trip parameter effectiveness for all AOOs and DBAs, and a safety analysis shall be performed to demonstrate the effectiveness of the means of shutdown.

Trip parameters shall take into account effects of SSC aging on effectiveness, as well as experimental devices when employed in the reactor.

Limiting conditions for safe operation shall be prepared for experimental devices and incorporated into OLCs.

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, two diverse trip parameters shall be 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 (e.g., power, temperature) within the OLCs. This shall be ensured by providing additional trip parameters if necessary.

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.

The design shall specify periodic testing of the systems and their components at a frequency commensurate with applicable requirements.

8.4.3 Monitoring and operator action

The design shall ensure that once automatic shutdown is initiated, an operator cannot prevent its actuation.

The need for manual shutdown actuation shall be minimized.

The means for monitoring shutdown status and manual actuation shall be provided in control facilities (refer to section 8.10).

8.5 Emergency core cooling system

Where required, an emergency core cooling system (ECCS) shall be provided to prevent damage to the fuel in the event of a loss of coolant accident. The accidents with which the system must cope shall be identified and analyses shall be performed to show that the system fulfils the requirements.

The design shall demonstrate the effectiveness of ECCS, including the effect on core reactivity of mixing the ECCS coolant with reactor coolant.

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

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

Special procedures for cooling the core shall be considered, in the case of selected BDBAs.

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

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

The emergency core cooling system shall be designed to permit the periodic inspection of components and shall be designed for appropriate periodic functional testing for the verification of performance.

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 the confinement or in an extension of the confinement.

All ECCS piping in an extension of confinement that could contain radioactivity from the reactor core shall meet the following requirements:

- the requirements for metal penetrations of confinement
- all piping and components of the ECCS recovery flow path that are open to the confinement atmosphere are designed for a pressure greater than the confinement design pressure
- all ECCS recovery flow paths are housed in a confinement structure that prevents leakage of radioactivity to the environment and to adjacent structures
- 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 confinement. The leak detection shall be such that on detection of radioactivity from the ECCS recovery flow, the loops can be isolated as per the requirements for confinement isolation.

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

8.6 Means of confinement

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

8.6.1 Confinement features

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

To achieve the fundamental function of confinement, the means of confinement shall require:

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

The means of confinement shall be designed with sufficient reliability to meet two important general requirements.

First, the features for confinement shall be determined from the safety analysis. The accidents which confinement must be able to handle shall be specified. Analyses shall be provided to demonstrate that the requirements for confinement have been fulfilled. Those systems and subsystems that are essential for the proper operation of confinement shall be identified.

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

a. component reliability, system independence, redundancy, fail-safe characteristics, diversity and physical separation of redundant systems
b. the use of material to withstand the postulated DBAs and BDBAs (e.g., in relation to radiation levels or radiolytic decomposition)
c. provisions for inspection, periodic testing and maintenance (including under simulated DBA conditions, where possible) to verify that the confinement system continues to function or is in a state of readiness to perform its functions and will be reliable and effective upon demand

For the proper functioning of the means of confinement, the pressure within a barrier shall be set at such a level as to prevent the uncontrolled release of radioactive material to the environment from the barrier. In setting this pressure, variations in atmospheric conditions (e.g., wind speed, atmospheric pressure) shall be taken into account.

In the design of the means of confinement, the effects of extreme conditions (e.g., explosions within the barrier) and environmental conditions due to accidents, including conditions arising from the external and internal events, shall be taken into account in accordance with the design basis.

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

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

Each penetration of the barriers shall be capable of being automatically and reliably sealed in the event of DBA or BDBA conditions arising (including those that may produce increases in pressure) in which the control of leakage from the barrier is essential to prevent the release of radioactive material to the environment in excess of acceptable limits.

Provisions to enable initial and periodic performance tests to check air leakage rates and the operational performance of the ventilation system shall be included in the design.

Where confinement is dependent on the efficiency of filters, provision shall be made as appropriate for *in situ* periodic testing of the efficiency of the filters.

For structures and components performing the function of confinement, coverings and coatings shall be carefully selected and their methods of application shall be specified to ensure the fulfilment of their safety functions and to minimize interference with other safety functions in the event of their deterioration.

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 function shall be highly reliable during normal operation, AOOs and DBAs. All systems that contribute to the transport of heat by conveying heat, providing power or supplying fluids to the heat transport systems shall be designed in accordance with the importance of their contribution to the function of heat transfer as a whole.

Natural phenomena and human-induced events shall be taken into account in 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 in the event of a severe accident.

8.8 Emergency heat removal system

The design shall include an emergency heat removal system (EHRS), which provides for removal of residual heat to ensure fuel design limits and reactor coolant boundary condition limits are met.

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

Correct operation of the EHRS equipment following an accident shall not be dependent on power supplies from the electrical grid.

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 required by the OLCs.

Inadvertent operation of the EHRS or of part of the EHRS shall not have a detrimental effect on reactor safety.

When firewater supply or other system components are interconnected to the EHRS, operation of one shall not impair operation of the other.

8.9 Normal and emergency power supply

The design basis for normal and emergency power supply (EPS) systems shall be specified. The availability of reliable electrical power supplies for essential functions in normal operation, AOOs, DBAs and, to the extent practicable, BDBAs shall be included.

The need for uninterruptible power supplies shall be assessed.

The EPS system shall have sufficient capacity and reliability, within a specified mission time, to provide the necessary power to maintain the reactor facility in a safe state and ensure nuclear safety in the event of all DBAs. These requirements shall be met following a common-cause loss of off-site power where this may occur as a result of a PIE, and in the presence of a single failure in the EPS.

The EPS system 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 design shall ensure that the emergency power supply:

- meets the specified maximum period for the interruption of AC and DC electrical power supplies
- is initiated either automatically or manually following the DBAs as determined by the safety requirements of the reactor facility
- can be tested to be acceptable under load conditions representing full-load demand

In the selection and routing of electrical and signal cables, common-cause failure mechanisms such as electrical interference and fire shall be considered and appropriate solutions (e.g., separation, redundancy, use of suitable materials) shall be adopted.

8.10 Control facilities

The design shall provide for control facilities from which the reactor can be safely operated, and from which measures can be taken to maintain the reactor in a safe state or to bring it back into such a state after the onset of AOOs, DBAs and, to the extent practicable, following BDBAs. Control facilities shall consist of a main control room (MCR) and a secondary control room

(SCR), if necessary. The need for a secondary control room or an emergency support centre (ESC) is determined by the safety case.

The design of the MCR and the SCR, if installed, shall be such that no event can simultaneously affect both control rooms to the extent that the essential safety functions cannot be performed**.**

8.10.1 Main control room

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

The safety functions initiated by automatic control logic in response to an accident shall also be capable of being initiated manually from the main control room and, if installed, from the 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 reactor facility and shall 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 to 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.

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 reactor states and processes that have deviated from normal operation and that could affect safety.

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

The MCR shall be designed with secure communication channels to the emergency support centre if installed, and to off-site emergency response organizations if deployed, 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 DBAs and BDBAs, including severe accidents.

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 interface design.

8.10.2 Secondary control room

This section applies when an SCR is installed.

The design, when necessary, shall provide an SCR that is physically and electrically separate from the MCR, and from which the facility 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 SCR.

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 essential safety functions can be performed, essential reactor facility variables can be monitored and operator actions 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 that 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.

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 when the MCR is uninhabitable.

The SCR shall be equipped with secure communication channels to the emergency support centre and to off-site emergency response organizations, if they are deployed.

The SCR shall allow for extended operating periods.

8.10.3 Emergency support centre

This section shall apply when an ESC is installed.

Emergency support centre design shall be separated from the main and secondary control rooms and be used by emergency support staff.

The ESC shall include secure means of communication with the MCR, the SCR and other important points in the facility, and with on-site and off-site emergency response organizations.

The ESC shall include a safety parameter display system similar to that used in the MCR. It shall also include information about the radiological and meteorological conditions in the reactor facility and its immediate surroundings.

The design of the ESC shall be such that appropriate lighting levels and thermal environment are maintained, and noise levels shall be minimized to applicable standards and codes.

8.10.4 Equipment requirements for accident conditions

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

- there shall be clear, well-defined, validated and readily available operating procedures that identify the necessary actions
- there shall be instrumentation in the control rooms to provide clear and unambiguous indication of the necessity for operator action
- following indication of the necessity for operator action inside the MCR, there shall be at least 15 minutes available before the operator action is required
- following indication of the necessity for operator action outside the MCR, there shall be a minimum of 30 minutes available before the operator action is required

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

8.11 Waste treatment and control

The design of the reactor facility shall minimize the generation of radioactive and hazardous waste. Systems shall be provided for the monitoring and handling of radioactive and hazardous waste and for its storage on the site for a reasonable period of time.

To reduce the exposure of personnel and minimize radioactive releases to the environment in a manner consistent with the ALARA principle, the design shall include provisions for:

- features such as shielding, delay tanks and/or decay systems
- liquid and gaseous effluent treatment to keep the quantities and concentrations of discharged contaminants within prescribed limits
- safe on-site handling and storage of radioactive and non-radioactive wastes for a period of time consistent with options for off-site management or disposal

8.11.1 Control of liquid releases to the environment

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

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

8.11.2 Control of airborne material within the reactor facility

The design shall include gaseous waste management systems capable of:

- controlling all gaseous contaminants so as to conform to the ALARA principle and ensure that concentrations remain within prescribed limits
- collecting all potentially radioactive gases, vapours and airborne particulates for monitoring
- directing all potentially radioactive gases, vapours and airborne particulates through pre-filters, absolute filters, charcoal filters or high-efficiency particulate air filters, where applicable
- 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:

- preventing unacceptable dispersion of all airborne contaminants within the reactor facility
- reducing the concentration of airborne radioactive substances to levels compatible with the need for access to each particular area
- keeping the level of airborne radioactive substances in the reactor facility below prescribed limits, applying the ALARA principle in normal operation
- 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 design shall include filtration to:

- control the release of gaseous contaminants and hazardous substances to the environment
- ensure conformation to the ALARA principle
- 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 testing.

8.12 Fuel handling and storage

8.12.1 Handling and storage of non-irradiated fuel

The design of the fuel handling and storage systems for non-irradiated fuel shall ensure nuclear criticality safety by:

- 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 that have frequency of occurrence equal to or more than 10^{-6} per year
- minimizing on-site consequences to personnel of postulated criticality accidents
- mitigating off-site consequences of postulated criticality accidents

Details can be found in RD-327, *Nuclear Criticality Safety* and GD-327, *Guidance on Nuclear Criticality Safety*.

The design shall also:

- permit appropriate maintenance, periodic inspection and testing of components important to safety
- permit inspection of non-irradiated fuel
- prevent loss of or damage to the fuel
- 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 ensure nuclear criticality safety by:

- 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 that have frequency of occurrence equal to or more than 10-6 per year
- minimizing on-site consequences to personnel of postulated criticality accidents
- mitigating off-site consequences of postulated criticality accidents

Details can be found in RD-327, *Nuclear Criticality Safety* and GD-327, *Guidance on Nuclear Criticality Safety*.

The design shall:

- provide for adequate heat removal under normal operation, AOOs, DBAs and, where practicable, BDBAs
- provide for inspection of irradiated fuel
- provide for periodic maintenance, inspection and testing of components
- provide for prevention of dropping used fuel in transit
- provide for prevention of unacceptable handling stresses on fuel elements or fuel assemblies
- provide for prevention of inadvertent dropping of heavy objects and equipment on fuel assemblies
- permit inspection and safe storage of suspect or damaged fuel elements or fuel assemblies
- provide for proper means of radiation protection
- adequately identify individual fuel modules
- facilitate maintenance and decommissioning of the fuel storage and handling facilities
- facilitate decontamination of fuel handling and storage areas and equipment, when necessary
- ensure implementation of adequate operating and accounting procedures to track fuel inventory

- include measures to prevent a direct threat or sabotage to irradiated fuel
- 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 irradiated fuel storage shall include provisions for:

- controlling the chemistry and activity of water in which irradiated fuel is handled or stored
- monitoring and controlling the water level and temperature in the fuel storage pool
- detecting leakage
- preventing the pool from emptying in the event of a pipe break
- sufficient space to accommodate the entire reactor core inventory when necessary

8.12.3 Detection of failed fuel

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

8.13 Auxiliary systems

The failure of any auxiliary system, irrespective of its importance to safety, shall not be able to jeopardize the safety of the reactor facility.

Adequate measures shall be taken to prevent the release of radioactive material to the environment in the event of the failure of an auxiliary system containing radioactive material.

Abbreviations

ALARA	as low as reasonably achievable
AOO	anticipated operational occurrence
BDBA	beyond design basis accident
BDBT	beyond design basis threat
CNSC	Canadian Nuclear Safety Commission
DBA	design basis accident
DBE	design basis earthquake
DBT	design basis threat
ECCS	emergency core cooling system
EHRS	emergency heat removal system
EPS	emergency power supply
ESC	emergency support centre
GSS	guaranteed shutdown state
IAEA	International Atomic Energy Agency
MCR	main control room
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
TRA	threat and risk assessment

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) the consequences or potential consequences of which are not negligible from the point of view of protection or safety.

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

adverse impact
Adverse impact refers to risks that are significantly worse than those documented in the approved licensing basis.

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 reactor 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 accident
Accident conditions less frequent and more severe than a design basis accident. A beyond design basis accident may or may not involve core degradation.

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

Class I nuclear facility
A Class I nuclear facility refers to a Class IA and a Class IB nuclear facility as described in the *Class I Nuclear Facilities Regulations.*

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 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 from the design basis envelope that can be used to cope with beyond design basis accidents, including severe accidents.

confinement boundary
A continuous boundary without openings or penetrations that prevents the release of radioactive materials 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 method or physical structure designed to prevent the release of radioactive substances. This term is typically used in power reactors.

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

core damage frequency
An expression of the likelihood that, given the way a reactor is designed and operated, an accident could cause the fuel in the reactor to be damaged.

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.

defence in depth
A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.

design basis
The range of conditions and events taken into account in the design of structures, systems and components of a nuclear 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 reactor facility is designed according to established design criteria, and for which damage to the fuel and the release of radioactive material are kept within regulated limits.

design basis threat
The characteristics of a potential adversary in which countermeasures are incorporated into the design and evaluation of the physical protection system. The structural degradation is not expected for design basis threats.

design envelope
The design envelope comprises the design basis and complementary design features.

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

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:

- land, water and air, including all layers of the atmosphere
- all organic and inorganic matter and living organisms
- interacting natural systems that include the components listed above

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 reactor facility and can cause failure of structures, systems and components. External events include, but are not limited to, earthquakes, floods and hurricanes.

external hazard
An event of natural or human-induced origin that originates outside the site and whose effects on the reactor facility should be considered as potentially hazardous.

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

fissile material
Material that is capable of sustaining a chain reaction of nuclear fission.

fissionable material
Any materials that can undergo nuclear fission.

graded approach
A method in which the stringency of the design measures and analyses applied is commensurate with the level of risk posed by the reactor facility.

hazards analysis
The process of collecting and evaluating information about the reactor facility to identify the associated hazards and determine those that are significant and must be addressed.

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 they relate to the safety of the reactor facility, including activities during design, construction, commissioning, operation, maintenance and decommissioning phases.

independent systems
The ability of a system to perform its required function is unaffected by the operation or failure of another system.

internal event
An event internal to the reactor facility 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 shutdown 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:

- physical elements such as people, buildings, work areas, equipment, tools, etc.
- intangible elements such as roles and responsibilities, knowledge, skills and behaviour of the people, cultural norms, agreements, understandings, decision-making processes, etc.
- documentation that is essential to meeting the organization’s objectives

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

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

normal operation
Operation of a reactor facility within specified operational limits and conditions including startup, power operation, shutdown, maintenance, testing and refuelling.

operational limits and conditions
A set of rules setting out parameter limits or conditions that ensures the functional capability and the performance levels of equipment and personnel for safe operation of a reactor facility. This set of limits and conditions is monitored by or on behalf of the operator and can be controlled by the operator.

physical security protection system
A security system is designed such that an adversary(ies) must overcome or circumvent multiple obstacles or barriers, either similar or diverse, which would result in effective mitigation prior to the achieving of their goal.

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

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

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

probabilistic safety assessment (PSA)
A comprehensive and integrated assessment of the safety of the reactor facility. 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 reactor facility, as follows:

- 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
- 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
- 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, by a history of experience, by test, or by 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.

reactor facility

Any fission reactor as described in the *Class I Nuclear Facilities Regulations*, including structures, systems and components:

- that are necessary for shutting down the reactor ensuring that it can be kept in a safe shutdown state
- that may contain radioactive material and which cannot be reliably isolated from the reactor
- whose failure can lead to a limiting accident for the reactor
- that are tightly integrated into the operation of the nuclear facility
- that are needed to maintain security and safeguards

reactor state
A configuration of reactor facility components, including the physical and thermodynamic states of the materials and the process fluids in them.

For the purpose of this document, a reactor state is considered to be normal operation, anticipated operational occurrence, design basis accident or beyond design basis accident (severe accidents are a subset of the beyond design basis state).

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.

responsible designer
An organization to which the design authority has assigned responsibility for the design of specific parts of the reactor.

safeguards
A system of international inspections and other verification activities undertaken by the International Atomic Energy Agency (IAEA) 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 reactor facility design is capable of meeting the acceptance criteria for each reactor state.

safety assessment
A systematic process applied throughout the design phase to ensure that the design meets all relevant requirements that are used for the evaluation of safety.

safety case
An integrated collection of arguments and evidence to demonstrate the safety of a facility. This will normally include a safety assessment, but could also typically include information (including supporting evidence and reasoning) on the robustness and reliability of the safety assessment and the assumptions made therein.

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 function
A specific purpose that must be accomplished for 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 anticipated operational occurrences and design basis accidents are not exceeded. It may include certain safety and safety support systems, as well as any interacting process system.

safety margin
A margin to a value of 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 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.

shutdown state
A subcritical reactor state with defined margin to prevent a return to criticality without external actions.

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.

small reactor
A reactor with a power level less than approximately 200 megawatts thermal (MWt) that is used for research, isotope production, steam generation, electricity production or other applications.

structures, systems and components
A general term encompassing all of the elements of a facility or activity that 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: wires, transistors, integrated circuits, motors, relays, solenoids, pipes, fittings, pumps, tanks, valves, etc.

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:

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

trip parameter
A variable whose measure is used to trigger a safety system action when the trip setpoint is reached.

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

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

Additional Information

The following documents contain additional information that may be of interest to persons involved in the design of small reactor facilities:

- Canadian Environmental Assessment Agency, *Canadian Environmental Assessment Act*
- Communications Security Establishment, *Harmonized Threat and Risk Assessment (TRA) Methodology*, TRA-1, 2007
- International Atomic Energy Agency, *Safety of Nuclear Power Plants: Design Safety Requirements*, IAEA Safety Standards Series No. NS-R-1, 2000
- International Atomic Energy Agency, *Engineering Safety Aspects of the Protection of Nuclear Power Plants Against Sabotage*, Nuclear Security Series No. 4, 2007
- International Atomic Energy Agency, *The Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors*, IAEA Draft Safety Standards DS351, 2009
- International Atomic Energy Agency, *Safety Analysis for Research Reactors*, IAEA Safety Reports Series No. 55, 2008
- International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities*, INFCIRC/225/Rev.4 (Corrected), 1999
- International Atomic Energy Agency, *Guidance and Considerations for the Implementation of INFCIRC/225/Rev.4, The Physical Protection of Nuclear Material and Nuclear Facilities*, TECDOC-967 (Rev.1), 2002
- International Atomic Energy Agency, *Handbook on the Physical Protection of Nuclear Material and Facilities*, TECDOC-1276, 2002