Design Requirements for New Nuclear Reactor Facilities in Canada

S. Shim, M. Ohn and C. Harwood
Canadian Nuclear Safety Commission, Ontario, Canada
(Sang.Shim@cnsc-ccsn.gc.ca)

Abstract

The Canadian Nuclear Safety Commission (CNSC) has been establishing the regulatory framework for the efficient and effective licensing of new nuclear reactor facilities. This regulatory framework includes the documentation of the requirements for the design and safety analysis of new nuclear reactor facilities, regardless of size. For this purpose, the CNSC has published the design and safety analysis requirements in the following two sets of regulatory documents:

1. RD-337, *Design of New Nuclear Power Plants* and RD-310, *Safety Analysis for Nuclear Power Plants*; and
2. RD-367, *Design of Small Reactor Facilities* and RD-308, *Deterministic Safety Analysis for Small Reactor Facilities*.

These regulatory documents have been modernized to document past practices and experience and to be consistent with national and international standards. These regulatory documents provide the requirements for the design and safety analysis at a high level presented in a hierarchical structure. These documents were developed in a technology neutral approach so that they can be applicable for a wide variety of water cooled reactor facilities.

This paper highlights two particular aspects of these regulatory documents:

1. The use of a graded approach to make the documents applicable for a wide variety of nuclear reactor facilities including nuclear power plants (NPPs) and small reactor facilities; and
2. Design requirements that are new and different from past Canadian practices.

Finally, this paper presents some of the proposed changes in RD-337 to implement specific details of the recommendations of the *CNSC Fukushima Task Force Report*. Major changes were not needed as the 2008 version of RD-337 already contained requirements to address most of the lessons learned from the Fukushima event of March 2011.

1. Introduction

The CNSC regulates the Canadian nuclear sector. To regulate an evolving nuclear industry for safety, the CNSC maintains an effective and flexible regulatory framework.

The CNSC's regulatory framework consists of laws passed by the Parliament that govern the regulation of Canada's nuclear industry, supported by regulations, licences and regulatory

documents that the CNSC uses to regulate the industry. The regulatory documents fall into two broad categories: those that set out requirements, and those that provide guidance on requirements. The CNSC is committed to providing regulatory instruments that achieve clarity of its requirements.

The requirements are mandatory. Licensees or applicants must meet these requirements in order to obtain or retain a license to operate a nuclear facility. However, Licensees or applicants may propose alternatives to meeting the requirements provided that they demonstrate an equivalent or superior level of safety.

Guidance documents provide CNSC expectations to licensees and applicants on how to meet the requirements set out in CNSC's regulations, regulatory documents and licences. Review procedures are used by CNSC staff in evaluating specific problems, or identifying information required in the review of applications for licences.

The CNSC regulatory approach is to provide licensees or designers with high-level safety and design requirements. The approach in which the requirements are fulfilled is not prescribed. It is left to the licensees or designers how to meet the requirements depending on the risk associated with the individual nuclear facility. By utilizing this approach, CNSC seeks to ensure a regulatory environment that encourages innovation within the nuclear industry without compromising the high standards necessary for safety.

Therefore, the CNSC has published the design and safety analysis requirements in the following two sets:

1) Regulatory documents RD-337, *Design of New Nuclear Power Plants* [1] and RD-310, *Safety Analysis for Nuclear Power Plants* [2] applied to those facilities above the 200 MW(th) threshold; and

2) Regulatory documents RD-367, *Design of Small Reactor Facilities* [3] and RD-308, *Deterministic Safety Analysis for Small Reactor Facilities* [4] applied to those facilities below the 200 MW(th) threshold.

The regulatory documents have been modernized to document past practices and experience and to be consistent with national and international standards. These regulatory documents provide the requirements for the design and safety analysis at a high level presented in a hierarchical structure. Both sets were developed in a technology-neutral approach so that they are applicable to a wide variety of water cooled reactor facilities.

This paper highlights two particular aspects of these regulatory documents:

1) The use of a graded approach to make the documents applicable for a wide variety of nuclear reactor facilities including nuclear power plants (NPPs) and small reactor facilities; and

2) Design requirements that are new and different from past Canadian practices.

Finally, this paper presents some of the proposed changes in RD-337 to implement specific details of the recommendations of the *CNSC Fukushima Task Force Report*. Major changes were not needed as the 2008 version of RD-337 already contained requirements to address most of the lessons learned from the Fukushima event of March 2011.

2. CNSC Approach to Design Requirements for Nuclear Reactor Facilities

Under the *Canadian Nuclear Safety and Control Act* and its regulations, all fission reactors are considered Class IA nuclear facilities in Canada. The regulations are at a high level and there is no distinction of these nuclear reactor facilities according to their size or application. However, the CNSC regulatory framework recognizes that the risks posed by different nuclear reactor facilities can vary considerably depending on the reactor core characteristics and the design features, including the size.

Under the CNSC regulatory framework, for the purpose of setting the regulatory requirements for design and safety analysis, all nuclear reactor facilities are divided into two groups depending on total thermal output. The 200 MW(th) threshold was chosen for the following reasons:

- All the current nuclear reactor facilities in Canada that are not an NPP are below 200 MW(th). The highest rated research reactor in Canada is NRU at 135 MW(th) which was originally designed for 200 MW(th); and

- The greater potential risk is expected with the core of larger reactors as it would contain larger inventory of radionuclides.

Nuclear reactor facilities below this threshold of 200 MW(th) are termed “small reactor facilities”.

The CNSC provides the design and safety analysis requirements in the following two sets:

1) Regulatory documents RD-337, *Design of New Nuclear Power Plants* [1] and RD-310, *Safety Analysis for Nuclear Power Plants* [2] applied to those facilities above the 200 MW(th) threshold; and

2) Regulatory documents RD-367, *Design of Small Reactor Facilities* [3] and RD-308, *Deterministic Safety Analysis for Small Reactor Facilities* [4] applied to those facilities below the 200 MW(th) threshold.

It should be noted that the value of 200 MW(th) has some flexibility depending on the design of a facility. It is the responsibility of the applicant to demonstrate why the design should use a particular set of requirements.

The above two sets of the design and safety analysis requirements are similar at a high level. However, the way in which the requirements are met for small reactor facilities can be flexible through the graded approach (for example, as described in IAEA NS-R-4, *Safety of Research Reactors* [5]).

The idea of grading is not new to the CNSC. It has been used to license the variety of small reactors in Canada in a wide range of designs, power levels and utilization. With the graded approach, the risk posed by the facility determines the stringency of how safety requirements are applied. For example, a small reactor facility may not require a containment system as robust as that used in a conventional large NPP.

As another example, some small reactor designs may have inherent self-limiting power levels or systems which physically limit the amount of positive reactivity that can be inserted in the core. This feature may be used for grading the shutdown system design. So, small reactors are permitted some flexibility in the design through the application of a graded approach.

It should also be noted that across the entire continuum and depending on the hazards, all applicants may propose to apply a graded approach in certain areas of their design. These proposals would be assessed on the basis of individual merits in the safety case submitted.

Regardless of reactor facility type or size, the CNSC expects that the applicant demonstrates in the safety case that the design provisions are commensurate with the risk posed by the facility. This means that, for any size of reactor, high-level safety requirements must be met. For example, the design of any nuclear facility must provide the fundamental safety functions during and following a postulated initiating event (PIE); controlling reactivity, cooling the reactor core and confining radioactive material. These safety functions are not gradable but the design and engineering rigor necessary to adequately ensure that they are achieved will vary depending on the reactor design. For example, a forced convection cooling system to remove fission heat may be needed in one facility while the fission heat may be adequately removed by natural convection cooling in another facility. In both cases the high level core cooling safety function is achieved but with different means.

The graded approach may also be applied to deterministic and probabilistic safety analyses. For example, the scope, extent and detail of these analyses may be significantly reduced because certain accident scenarios may not apply or may need only a limited analysis.

3. CNSC Design Requirements for New Nuclear Reactor Facilities

RD-337 for use with new NPPs and RD-367 for use with new small reactor facilities have been developed to set out CNSC requirements for the design of new water-cooled nuclear reactor facilities. Both regulatory documents provide a set of comprehensive design requirements that makes use of extensive Canadian experience. They are consistent with international standards such as:

1) IAEA NS-R-4, *Safety of Research Reactors* [5]; and

2) IAEA NS-R-1, *Safety of Nuclear Plants: Design* [6] (replaced with IAEA SSR 2/1, *Safety of Nuclear Power Plants: Design* [7]).

The requirements allow the applicant with appropriate flexibility and are provided using a technology-neutral approach for use with water cooled reactors.

The safety objectives, safety goals and design requirements in RD-337 and RD-367 have an overall objective to protect individuals, society and the environment from harm.

RD-337 and RD-367 provide the criteria pertaining to the safe design of new water-cooled reactor facilities, and offer examples of optimal design characteristics where applicable. All aspects of the design are taken into account, and multiple levels of defence are promoted in design considerations. Application of the concept of defence-in-depth throughout the facility design provides a protection over a wide range of plant states (i.e., anticipated operational occurrences (AOOs), design basis accidents (DBAs) and beyond design basis accidents (BDBAs)).

RD-337 and RD-367 consider the entire life cycle of the facility because information from the design is used for reviewing all licence applications for the siting, construction, commissioning, operation, decommissioning and abandonment of the facility.

The regulatory approach of RD-337 and RD-367 has a hierarchical structure. The main elements in the regulatory documents are:

- Safety objectives and concepts;
- Safety requirements (including the safety goals and dose acceptance criteria) for the design;
- Safety management during design;
- General and specific design requirements for structures, systems, and components (SSCs) important to safety;
- Safety assessment; and
- Alternative approaches.

It is recognized that specific technologies may use alternative approaches which should demonstrate equivalence to the outcomes associated with the use of the requirements set out in these regulatory documents.

RD-337 has been applied to CNSC's vendor pre-project design reviews and, to some extent, to the review of application for a licence to prepare site for the Darlington new build.

Evolutionary differences between the design requirements in RD-337 and RD-367 and those of the past are discussed in section 4.

It is noted that RD-337 is being revised to implement detailed lessons learned from the Fukushima event and a limited number of other necessary changes. The proposed changes to RD-337 related to the Fukushima event are discussed in section 5.

4. Evolution of Design Requirements for New Nuclear Reactor Facilities

Several design requirements in RD-337 and RD-367 have been extended from past CNSC practices such as:

- Safety classification of structures, systems and components;
- Classification of events;
- Quantitative safety goals;
- Design for severe accidents;
- Control systems to cater for AOOs;
- Design for reliability;
- Operating limits and conditions; and
- Consideration of malevolent acts in the design.

These extensions will bring the Canadian design requirements more in line with international standards, and nuclear facilities built to these requirements will provide an additional level of safety.

Several examples of the design requirements evolved from past practices are discussed below.

4.1 Classification of Structures, Systems and Components

In the past CANDU reactor systems were classified as either process systems or special safety systems (i.e., the two shutdown systems, the emergency core cooling system and the containment). Other systems were classified as safety-related, but the practice for designating systems as safety-related has varied over the years and has not followed a systematic process. A revised classification scheme based on importance to safety has been adopted in the requirements of the nuclear facility in RD-337 and RD-367.

All SSCs are classified in a consistent and clearly defined classification scheme based on the criteria for determining safety importance, i.e., SSCs either important or not important to safety. The criteria for determining safety importance are based on:

1) Safety function(s) to be performed;

2) Consequence of failure;

3) Probability that the SSC will be called upon to perform the safety function; and

4) The time following a PIE at which the SSC will be called upon to operate, and the expected duration of that operation.

SSCs important to safety include:

1) Safety systems;

2) Complementary design features (discussed in section 4.2);

3) Safety support systems; and

4) Other SSCs whose failure may lead to safety concerns (e.g., process and control systems).

The SSCs in a nuclear reactor facility are designed, constructed, and maintained such that their quality and reliability are commensurate with this classification. The classification levels can be used to ensure that the application of such rules as engineering rigour, quality assurance, inspection and testing during design, construction, operation and maintenance is commensurate with the safety importance of the SSC in the overall facility's operation.

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

A SSC classification process typically includes:

- Review of PIEs;
- Identification of preventive and mitigative safety features;
- Categorization in accordance with safety significance and role to achieve the fundamental safety functions;
- Assignment of SSCs to a safety class according to a safety category; and
- Identification of design rules for classified SSCs.

The number of categories and classes of SSCs may be chosen to allow for graded engineering design rules.

4.2 Design for Severe Accidents

RD-337 and RD-367 contain deterministic and probabilistic safety requirements for BDBAs including severe accidents. For probabilistic requirements, the design must demonstrate compliance with the safety goals. The quantitative safety goals establish limits on the sum of frequencies of events that may lead to significant core degradation, short-term evacuation, or long-term relocation. Three surrogate safety goals are established:

1) Core damage frequency;

2) Small release frequency; and

3) Large release frequency.

Core damage frequency is a measure of the facility's accident preventive capabilities. Small release frequency and large release frequency are measures of the facility's accident mitigative capabilities. They also represent measures of risk to society and to the environment due to the operation of the nuclear facility.

In addition to the probabilistic requirements, RD-337 and RD-367 include a number of deterministic design considerations for BDBAs such as:

- Maintain a safe, stable state of the reactor and facility over the long term;
- Prevent re-criticality;
- Cool the core debris;
- Preclude unfiltered release;
- Prevent containment melt-through; and
- Prevent containment bypass.

The design establishes the severe accident management program and identifies the equipment to be used in the program to maintain the fundamental safety functions. The fundamental safety functions are reactivity control, removal of heat from the fuel, confinement of radioactive materials, limitation of accidental releases and monitoring of critical safety parameters to guide operator actions.

A reasonable level of confidence that this equipment will perform as intended in the case of a severe accident is demonstrated by environmental, fire, and seismic assessments. This includes complementary design features to prevent accident progression and to mitigate the consequences of design extension conditions (DECs).

A complementary design feature is a physical design feature added to the design as a stand-alone SSC or added to an existing SSC to cope with DECs. DECs are a subset of BDBAs and are defined

as accident conditions, not considered DBAs, which are considered in the design process of the facility. DECs include some severe accidents.

The containment has a key role for a severe accident to maintain its role as a leak-tight barrier for a period of time sufficient for implementation of off-site emergency procedures following severe core damage and to prevent unfiltered releases of radioactivity after this period. The containment design must withstand loads associated with DECs including considerations of pressure, heat or combustible gases.

4.3 Design for Reliability

In the past Canadian practice, the special safety systems were required to meet the unavailability target during operation. Specifically they are available for 99.9% of time in each year. Its application may be misinterpreted that there is no need to investigate causes of failure further or to improve the overall reliability of the system if the unavailability target is met during operation. The reason is that the reliability targets may be met in some cases by increasing the testing frequency rather than by addressing the reliability issue.

It was proposed to define the reliability requirements for the safety systems in meaningful terms, which is the probability that the system operates as expected when required to do so. It is expressed as the probability of failure on demand or the probability of failure during a given mission time, according to the system of interest.

RD-337 and RD-367 contain the formal reliability requirement of a safety system based on failure on demand rather than the unavailability requirement. It is consistent with the standard approach used in reliability engineering worldwide and more closely reflects international best practice.

RD-337 and RD-367 explicitly specify the requirement that the safety systems and their support systems are designed to ensure that the probability of system failure on demand from all causes is lower than 10^{-3}. All SSCs important to safety are designed with sufficient quality and reliability to meet the design limits. A reliability analysis is performed for each of these SSCs. The reliability analysis should be aligned and consistent with the facility PSA analysis.

The principles of diversity, separation, and independence are applied to achieve the necessary reliability for common cause failures.

All safety systems and their safety support systems meet the single failure criterion. Each safety group perform all safety functions required for a PIE in the presence of any single component failure. This criterion extends to their support systems which supply the cooling water, the electrical power and the compressed air necessary to ensure that the safety systems continue to function. Each safety group can perform the required safety functions under the worst permissible systems configuration, taking into account maintenance, testing, inspection and repair, and allowable equipment outage times.

Regulatory requirements in the past prohibit the sharing of instrumentation and other equipment between safety systems and between safety systems and process systems. The intent was to ensure that each safety system is separated as far as practicable, so that it may be considered as fully independent. This requirement is largely deterministic rather than risk-informed and has led to designs that are complex and require significant additional maintenance. It is a unique requirement to Canada; most other jurisdictions allow extensive sharing of equipment, subject to certain conditions.

In RD-337 and RD-367, a sharing of equipment between safety systems and process systems is allowed in alignment with international practices. The sharing of process and safety functions by a system may be permitted if these functions are not both required or credited at the same time and the system is designed to the standards of the system of higher importance with respect to safety. Where sharing of instrumentation is allowed, adequate isolation between safety and process systems must be demonstrated.

4.4 Operational Limits and Conditions

Operational limits and conditions (OLCs) are a set of limits and conditions that can be monitored by the operator and that can be controlled by the operator. The basis on which the OLCs are derived is readily available in order to facilitate the ability of the operator to interpret, observe, and apply the OLCs.

RD-337 and RD-367 require that the OLCs be established to ensure that facilities operate in accordance with design assumptions and intent (parameters and components), and include the limits within which the facility has been shown to be safe.

The OLCs typically include elements such as safety limits, safety system settings, limits and conditions for normal operation and surveillance. The OLCs form a logical system in which these elements are closely interrelated and in which the safety limits constitute the ultimate boundary of the safe conditions.

The OLCs are documented in a manner that is readily accessible for control room personnel, with the roles and responsibilities clearly identified. Some OLCs may include combinations of automatic functions and actions by the operator.

Safe operation depends on personnel as well as equipment. The OLCs include safety limits, limiting settings for safety systems, operational limits and conditions for normal operation and AOOs, including shutdown states.

The OLCs provide requirements for surveillance, maintenance, testing and inspection of the facility to ensure that structures, systems and components function as intended in the design, to comply with the requirement for optimization by keeping radiation risks as low as reasonably achievable.

The OLCs specify operating configurations including operational restrictions in the event of the unavailability of safety systems or safety related systems and action statements including completion times for actions in response to deviations from the operational limits and conditions.

The OLCs should clearly state the allowable outage time for the system and any additional operational restrictions, such as suspension of additional testing on a backup system for the duration of the exception.

5. Implementation of Lessons Learned from the Fukushima Event in RD-337

The *CNSC Fukushima Task Force Report* [8] recommended enhancing selected design requirements for DBAs and BDBAs by implementing lessons from the Fukushima event.

RD-337 published in 2008 contains requirements to consider many of the phenomena that occurred at Fukushima including provisions for total loss of power, for mitigation of severe accidents, for hydrogen mitigation, and for withstanding external events.

Even though RD-337 has adequate design requirements at an overall level for severe accidents such as the Fukushima event, RD-337 is being revised to provide further clarity of the requirements that take into account detailed lessons learned from the Fukushima event such as:

- Multi-unit events;
- Complementary design features for irradiated fuel bays;
- Margins to cliff edges; and
- Reliable monitoring.

A few examples of proposed changes to RD-337 to implement the lessons learned from the Fukushima event are discussed below. It should be noted that RD-337 is under revision and is subject to the CNSC regulatory document publication process which includes public consultation and approval by the Commission. RD-337 will be finalized once due publication process for the document is completed.

5.1 Requirements for Multi-unit Plant

RD-337 requires that the design consider any challenges to a multi-unit site. The design specifically considers the risk associated with common-cause events affecting more than one unit at a time. Such events could exacerbate challenges that the plant personnel would face in time of an accident. The events and consequences of an accident at one unit may affect the accident progression or hamper accident management activities at the neighbouring unit; available resources (personnel, equipment and fuel) would need to be shared among several units

5.2 Requirements for Irradiated Fuel Bays

The design for a water pool used for fuel storage includes provisions for DECs; to ensure that boiling in the pool does not result in structural damage, to provide temporary connections to heat removal systems for power and cooling water and to provide hydrogen mitigation in the spent fuel pool area.

Spent fuel storage pools preclude uncontrolled leakage beyond the available cooling water make-up capability in the event of structural failure.

5.3 Severe Accident Requirements

Safety analysis is required to demonstrate that the design incorporates sufficient safety margins to cliff-edge effects. A cliff-edge effect is defined as a large increase in the severity of consequences caused by a small change of conditions. It is noted that cliff edges can be caused by changes in the characteristics of the environment, the event or changes in the plant response.

If necessary for normal operation, AOOs and DBAs, the design provides means of monitoring reactor core coolant inventory. Means of estimating the core coolant inventory in DECs is provided to the extent practicable.

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

The facility layout takes external hazards into consideration to enhance protection of SSCs important to safety. Where physical separation by distance alone may not be sufficient for some common-cause failures (such as flooding) vertical separation or other protection is provided. External events that the plant is designed to withstand are identified, and classified as DBAs or DECs.

The design of emergency power supply (EPS) considers common-cause failure coincident with a loss of normal and standby power. Where plant safety relies on availability of AC electrical power, EPS is physically separate and diverse from, and independent of normal and standby power supplies.

The emergency support systems must support continuity of the fundamental safety functions until long term (normal or backup) service is re-established:

1. Without the need for operator action to connect temporary onsite services for at least eight hours; and
2. Without the need for offsite services and support for at least 72 hours.

6. Summary and Conclusions

The CNSC has published modern design and safety analysis requirements that are applied to NPPs and small reactor facilities:

1) Regulatory documents RD-337, *Design of New Nuclear Power Plants* and RD-310, *Safety Analysis for Nuclear Power Plants*; and

2) Regulatory documents RD-367, *Design of Small Reactor Facilities* and RD-308, *Deterministic Safety Analysis for Small Reactor Facilities*.

This paper highlighted two particular aspects of these documents:

1) The use of a graded approach to make the documents applicable for a wide variety of nuclear reactor facilities including NPPs and small reactor facilities; and

2) Design requirements that are new and different from past Canadian practices. .

The paper also presented some of the proposed changes in RD-337 to implement specific details of the recommendations of the *CNSC Fukushima Task Force Report*.

7. References

[1] Canadian Nuclear Safety Commission, Design of New Nuclear Power Plants, RD-337, 2008.

[2] Canadian Nuclear Safety Commission, Safety Analysis for Nuclear Power Plants, RD-310, 2008.

[3] Canadian Nuclear Safety Commission, Design of Small Reactor Facilities, RD-367, June 2011.

[4] Canadian Nuclear Safety Commission, Deterministic Safety Analysis for Small Reactor Facilities, RD-308, June 2011.

[5] IAEA Safety Standard, NS-R-4, Safety of Research Reactors, 2005.

[6] IAEA Safety Standards, NS-R-1, Safety of Nuclear Plants: Design, 2000.

[7] IAEA Safety Standards, SSR 2/1, Safety of Nuclear Power Plants: Design, 2012.

[8] CNSC Fukushima Task Force Report, INFO-0824, October 2011.