DESIGN REQUIREMENTS FOR SMALL REACTOR FACILITIES IN CANADA
(FOCUS ON DIFFERENCES FROM THOSE FOR NPPs)

SANG SHIM
Canadian Nuclear Safety Commission, Ontario, Canada
Sang.Shim@cnsc-ccsn.gc.ca

ABSTRACT

The Canadian Nuclear Safety Commission (CNSC) has established the regulatory framework for the efficient and effective licensing of all nuclear reactor facilities. This regulatory framework includes the documentation of the requirements for the design and safety analysis of all nuclear reactor facilities whether they are small reactor facilities or nuclear power plants (NPPs) 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-367, *Design of Small Reactor Facilities* and RD-308, *Deterministic Safety Analysis for Small Reactor Facilities*; and
2. RD-337, *Design of New Nuclear Power Plants* and RD-310, *Safety Analysis for Nuclear Power Plants*.

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 focuses on the key differences in the design requirements as applied to small reactor facilities in comparison with those applied to NPPs, in particular:

1) The application of a graded approach to make the documents applicable for a wide variety of designs, power levels and utilization associated with small reactor facilities; and
2) Utilization aspects associated with small reactor facilities.

Finally, this paper presents some of the proposed considerations in design requirements to implement specific details of the recommendations of the *CNSC Fukushima Task Force Report*. Major changes were found unnecessary since the original version of these documents 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 health, safety, security, the environment, and the implementation of international obligations to which Canada has agreed, 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 how to meet the 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 relevant Canadian laws particularly *the Canadian Nuclear Safety and Control Act*, CNSC's regulations, licences, and regulatory documents. Review procedures are used by CNSC staff in evaluating specific subjects, 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 prescriptive. 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.

In the CNSC regulatory framework, CNSC staff uses the 14 safety and control areas of technical topics to assess and evaluate all regulated facilities and activities. The CNSC framework provides regulatory requirements and guidance on these 14 safety and control areas. For the areas of physical design and deterministic safety analysis, the CNSC has published their requirements in the following two sets:

- Regulatory documents RD-367, *Design of Small Reactor Facilities* [1] and RD-308, *Deterministic Safety Analysis for Small Reactor Facilities* [2] applied to those facilities below the 200 MW(th) threshold; and

- Regulatory documents RD-337, *Design of New Nuclear Power Plants* [3] and RD-310, *Safety Analysis for Nuclear Power Plants* [4] applied to those facilities above 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 focuses on the key differences in the design requirements as applied to small reactor facilities in comparison with those applied to NPPs, in particular:

1) The application of a graded approach to make the documents applicable for a wide variety of designs, power levels and utilization associated with small reactor facilities. Details of Canadian practices of the application of a graded approach to design requirements are presented; and
2) Utilization aspects associated with small reactor facilities.

Finally, this paper presents some of the proposed considerations in design requirements to implement specific details of the recommendations of the *CNSC Fukushima Task Force Report*. Major changes to these documents were found unnecessary since the original version of these documents 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 I nuclear facilities in Canada. The regulations are provided 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 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 operating 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:

- Regulatory documents RD-367, *Design of Small Reactor Facilities* [1] and RD-308, *Deterministic Safety Analysis for Small Reactor Facilities* [2] applied to those facilities below the 200 MW(th) threshold; and

- Regulatory documents RD-337, *Design of New Nuclear Power Plants* [3] and RD-310, *Safety Analysis for Nuclear Power Plants* [4] applied to those facilities above 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 that an appropriate set of requirements are met for their design.

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 are more flexible through the graded approach (for example, as described in IAEA NS-R-4, *Safety of Research Reactors* [5]) than that of NPPs.

3. CNSC Design Requirements Common to All Nuclear Reactor Facilities

RD-367 for use with small reactor facilities and RD-337 for use with NPPs have been developed to set out CNSC requirements for the design of 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:

- IAEA NS-R-4, *Safety of Research Reactors* [5]; and
- IAEA SSR 2/1, *Safety of Nuclear Power Plants: Design* [6] (updated from IAEA NS-R-1, *Safety of Nuclear 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 general design requirements in RD-367 and RD-337 are nearly the same and have an overall objective to protect individuals, society and the environment from harm.

Both regulatory documents RD-367, design requirements applied to small reactor facilities and RD-337, those applied to NPPs provide the criteria pertaining to the safe design of 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., normal operation, anticipated operational occurrences (AOOs), design basis accidents (DBAs) and beyond design basis accidents (BDBAs)).

Both regulatory documents RD-367 and RD-337 consider the entire life cycle of a nuclear 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-367 and RD-337 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;
- Safety assessment;
- Alternative approaches;
- General design requirements for structures, systems, and components (SSCs) important to safety; and
- Specific design requirements for SSCs important to safety.

The design requirements for small reactor facilities in RD-367 share most of the requirements for NPPs in RD-337. As discussed in Section 4, the key differences of RD-367 in comparison with RD-337 are to be able to accommodate the variety of designs and power levels in small reactor facilities thus allowing more flexibility of meeting the requirements through a graded approach. Other differences between RD-367 and RD-337 are in specific requirements for SSCs since small reactor facilities may not necessarily use the same SSCs as those of NPPs depending on their design and utilization. However, RD-337 for NPPs contains details of the specific design requirements for SSCs important to safety since they are common to water-cooled NPPs, and have been established over time based on national and international knowledge and experience.

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.

It is noted that these two documents RD-367 and RD-337 are being updated to implement lessons learned from the Fukushima event. The proposed changes related to the Fukushima event are discussed in Section 5.

4. Key Differences in Design Requirements for Small Reactor Facilities from Those of NPPs

This section discusses the key differences in the design requirements as applied to small reactor facilities in comparison with those applied to NPPs, in particular:

1) The application of a graded approach to make the documents applicable for a wide variety of designs, power levels and utilization associated with small reactor facilities. Details of Canadian practices of the application of a graded approach to design requirements are presented; and
2) Utilization aspects associated with small reactor facilities.

4.1 Application of a Graded Approach for Small Reactor Facilities

RD-367 allows for the use of a graded approach. The graded approach is an approach 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 demonstrate that the safety objectives and the design requirements in RD-367 are met. Licensees or applicants may find further guidance on use of the graded approach such as in IAEA NS-R-4, *Safety of Research Reactors.*

When a graded approach is applied, RD-367 provides factors to be considered including:

- 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 facility;
- Presence of high energy sources and other radioactive and hazardous sources;
- Safety design features;
- Source term;
- Siting; and
- Proximity to populated areas.

The idea of grading is not new to the CNSC. It has been used to license the variety of small reactor facilities 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.

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) such as 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 an example of the reactivity control function, 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.

For an example of the cooling function of the reactor core, 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.

For an example of the containment safety function, a small reactor facility may not require a containment system as robust as that used in a conventional large NPP. The design requirements in RD-367 or RD-337 are such that confinement is a fundamental safety function and a means to achieve this safety function is provided for any reactor facility.

The confinement is designed to ensure that a release of radioactive material following an accident involving disruption of the core is within acceptable limits. The confinement includes physical barriers designed to prevent or mitigate an unplanned release of radioactive material to the environment during normal operation, AOOs, DBAs and selected BDBAs. To achieve the fundamental function of confinement, the means of confinement are provided to:

- 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; and
- Radiation shielding.

RD-367 provides detailed requirements for the confinement design that are based on a graded approach. The safety case of a small reactor facility demonstrates the fulfillment of this confinement function. For any small reactor facility, the design of a confinement must demonstrate the adequacy of meeting the intended means of confinement. The accidents which a confinement function is needed are specified. Analyses for these accidents need to demonstrate that the confinement function has been fulfilled. When the SSCs that are essential for the proper operation of confinement are identified, the following design rules apply to the design of confinement:

- Component reliability, system independence, redundancy, fail-safe characteristics, diversity and physical separation of redundant systems;
- The use of material to withstand the postulated conditions of DBAs and selected BDBAs; and
- Provisions for inspection, periodic testing and maintenance to ensure that the confinement system continues to function.

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.

4.2 Utilization Aspects Associated with Small Reactor Facilities

For a small research reactor facility, attention needs to be paid 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 is 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; and

- 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 is designed in accordance with the same principles as applied to the reactor facility. In particular, all experimental devices using the reactor are designed to standards equivalent to those applied for the reactor itself and must be fully compatible in terms of the materials used, the structural integrity and the provision for radiation protection.

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

The safety case is also 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).

5. Implementation of Lessons Learned from the Fukushima Event

The original version of RD-367 and RD-337 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:

- Core damage frequency;
- Small release frequency; and
- 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, the original version of RD-367 and RD-337 include a number of deterministic design considerations for selected 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 original version of RD-367 and RD-337 expects that 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 include 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.

As per RD-367 and RD-337, 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 selected BDBAs.

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 selected BDBAs. Selected BDBAs are accident conditions not considered in DBAs, which are considered in the design process of the facility.

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 a select set of BDBAs including considerations of pressure, heat or combustible gases.

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

As discussed above, the original version of RD-367 and RD-337 published in 2008 and 2011, respectively, contain already the 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-367 and RD-337 have adequate design requirements at an overall level for severe accidents such as the Fukushima event, they are being updated 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 the CNSC design requirements to implement the lessons learned from the Fukushima event are discussed below. It should be noted that these regulatory documents are under revision and is subject to the CNSC regulatory document publication process which includes public consultation and approval by the Commission. They will be finalized once due publication process for these documents is completed.

5.1 Requirements for Multi-unit Site

It is proposed to include in the design requirements that the design consider any challenges to a multi-unit site such as AECL Chalk River research facilities. 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 facility 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 a select set of BDBAs; 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. It is proposed to include in the design requirements that means of estimating the core coolant inventory in selected BDBAs is provided to the extent practicable.

It is also proposed that the design includes 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. It is also proposed that 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 a select set of BDBAs.

The design of emergency power system (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.

It is proposed to include in the design requirements that the emergency support systems must support continuity of the fundamental safety functions until long term (normal or backup) service is re-established:

- Without the need for operator action to connect temporary onsite services for at least eight hours; and
- 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 all nuclear reactor facilities of small reactor facilities and NPPs regardless size:

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

This paper presents the key differences in the design requirements as applied to small reactor facilities in comparison with those applied to NPPs, in particular:

1) The application of a graded approach to make the documents applicable for a wide variety of designs, power levels and utilization associated with small reactor facilities; and
2) Utilization aspects associated with small reactor facilities.

Furthermore, this paper presents the proposed considerations in design requirements to implement specific details of the recommendations of the *CNSC Fukushima Task Force Report*. Major changes were found unnecessary since the original version of these documents already contained requirements to address most of the lessons learned from the Fukushima event of March 2011.

7. References

[1] Canadian Nuclear Safety Commission, Design of Small Reactor Facilities, RD-367, June 2011.
[2] Canadian Nuclear Safety Commission, Deterministic Safety Analysis for Small Reactor Facilities, RD-308, June 2011.
[3] Canadian Nuclear Safety Commission, Design of New Nuclear Power Plants, RD-337, 2008.
[4] Canadian Nuclear Safety Commission, Safety Analysis for Nuclear Power Plants, RD-310, 2008.
[5] IAEA Safety Standards, NS-R-4, Safety of Research Reactors, 2005.
[6] IAEA Safety Standards, SSR 2/1, Safety of Nuclear Power Plants: Design, 2012.
[7] IAEA Safety Standards, NS-R-1, Safety of Nuclear Power Plants: Design, 2000.
[8] CNSC Fukushima Task Force Report, INFO-0824, October 2011.