Canadian Nuclear Safety Commission | Commission canadienne de sûreté nucléaire

Canada

Canadian Perspective on Risk-Informed Regulation of Small Modular Reactors

International SMR and Advanced Reactor Summit 2018, Atlanta, GA

New Major Facilities Licensing Division
Directorate of Regulatory Improvement and Major Projects Management

Canadian Nuclear Safety Commission
March 27–28, 2018

nuclearsafety.gc.ca

Outline

- View on Risk-Informed Regulatory Approach for SMRs
- Terminology
- Application of the Graded Approach to Address Fundamental Safety Principles

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

View on Risk-Informed Regulatory Approach for SMRs

Canada

Risk-Informed Regulation in Canada

- CNSC regulates in a risk-informed manner
  - CNSC allows proportionality through the articulation of requirements and guidance for activities
  - regulatory framework allows applicants/licensees to propose alternative methods to meet regulatory requirements
  - applicant/licensee needs to demonstrate their proposal meets requirements
- Supporting evidence plays a major role in making a regulatory decision
- A graded approach is established as a framework of decision-making tools and rules, and is supported by an organization's management system
  - documents the analyses supporting decision-making
  - supports robust and transparent regulatory processes

Use of the graded approach in Canada is consistent with International Atomic Energy Agency (IAEA) principles (IAEA Fundamental Safety Principles SF-1 and IAEA General Safety Requirements, Part 1)

Key Considerations in Regulatory Decision-Making

Section 24(4) of the *Nuclear Safety and Control Act* (NSCA)

No licence shall be issued, renewed, amended or replaced — and no authorization to transfer one given — unless, in the opinion of the Commission, the applicant:

(a) is qualified to carry on the activity that the licence will authorize the licensee to carry on; and

(b) will, in carrying on that activity, make adequate provision for the protection of the environment, the health and safety of persons and the maintenance of national security and measures required to implement international obligations to which Canada has agreed

The licensee is responsible for safety and is held accountable through their licence

Regulatory Decision-Making

- Decisions made by the Commission take into consideration
  - regulatory requirements
  - analyses and recommendations from CNSC staff, based on their assessment of both licensee and stakeholder submissions to the Commission
  - best available information, arising from regulatory research or credible research by third parties
  - public input, through the hearing process

Understanding risks and mitigating those risks play a significant role in the decision-making process

Graded Approach – Definition

- The **graded approach** is a method or process by which elements such as the level of analysis, the depth of documentation and the scope of actions necessary to comply with requirements are commensurate with
  - the relative risks to health, safety, security, the environment, and the implementation of international obligations to which Canada has agreed
  - the characteristics of a facility or activity (reactor specific)
    - reactor power, reactor safety characteristics, fuel design, source term
    - amount and enrichment of fissile and fissionable material
    - presence of high-energy sources, and other radioactive and hazardous sources
    - uncertainties associated with current level of knowledge
    - site characteristics (e.g., external hazards)

The use of a graded approach is a proportional application of requirements, not a relaxation of requirements

Application of the Graded Approach: Applicant's Perspective

- From an applicant/licensee perspective, **grading** is the **application** of the graded approach to a specific aspect of their licence application against specific regulatory requirements (e.g., a proposal to use only confinement instead of containment)
- An applicant or licensee may
  - demonstrate that specific design measures, analyses or other measures applied to their safety case are commensurate with the level of risks posed
  - propose that, since an overarching fundamental safety requirement is met, a detailed requirement may not have to be met
  - propose alternative methods to meeting requirements

The use of a graded approach is a proportional application of requirements, not a relaxation of requirements

Application of the Graded Approach: Regulator's Perspective

- From the CNSC's point of view, **grading** is the **application** of the graded approach to the overall review of a submission (e.g., acceptability of a safety case that employs confinement instead of containment)
- The regulator
  - applies technical requirements in a risk-informed manner to ensure fundamental safety objectives are met
  - carries out technical assessment and compliance activities for a project based on risk, complexity and novelty

Assessment of Applications: Fundamental Principles

- Assessment of a safety case for a proposed activity is carried out to ensure
  - regulatory requirements are met
  - high-level safety objectives are met
  - fundamental safety functions of “control, cool, contain” are met
- While demonstrating appropriate
  - defence in depth
  - safety margins in view of the uncertainties in the safety case and specific hazards over the lifecycle of the facility

Risk is demonstrated to be at a reasonable level

Characteristics of Suitable Information

- Facts and data have been derived through validated and quality assured (i.e., traceable and repeatable) scientific and engineering processes, such as
  - experimental or field-derived data
  - operating experience
  - computer modelling
- Uncertainties have been characterized and accounted for
- Information is demonstrated to be relevant to the specific proposal

The greater the uncertainty or safety significance, the greater the burden of evidence needed to support a proposal

Role of the Management System

- An organization needs processes and procedures to guide its staff on which tools to use when. Examples of risk-informing tools include
  - safety classification
  - safety analysis (deterministic and probabilistic)
  - process for reviews and approvals for specific decisions
  - specific risk-informed decision-making (RIDM) process
  - work instructions that specify specific approaches and/or guide the use of expert judgment (e.g., codes and standards)

The reasons for risk-informed decisions need to be clear and documented

Terminology

Regulatory Requirements (1)

Regulatory framework element	Approach
• *Nuclear Safety and Control Act* and regulations • Federal and provincial acts and regulations • International obligations	• All clauses in the NSCA and associated regulations must be addressed • Some are prescriptive, but the majority are not – there is flexibility in how clauses are addressed

Regulatory Requirements (2)

Regulatory framework element	Approach
• CNSC regulatory documents and industry standards	• Requirements: "An applicant or licensee may put forward a case to demonstrate that the intent of a requirement is addressed by other means and demonstrated with **supportable evidence**." • Guidance: "…elaborate further on requirements or … provide direction to licensees and applicants on how to meet requirements. ….. Licensees are expected to review and consider guidance; should they choose not to follow it, they should explain how their chosen alternate approach meets regulatory requirements." • Can make a case for not addressing specific clauses in CNSC regulatory documents or industry standards.

High-Level Safety Objectives

- Qualitative safety objectives
  - section 3.1 (including all subsections) and section 4.3.1 in the CNSC's RD-367, *Design of Small Reactor Facilities*
  - section 4 (including all subsections) and the qualitative safety objectives in section 4.2.2 in the CNSC's REGDOC-2.5.2, *Design of Reactor Facilities: Nuclear Power Plants*
- Fundamental safety principles
  - control, cool, contain
  - independence, diversity, separation, redundancy
  - ALARA (as low as reasonably achievable)

Defence in Depth

- Level 1: Prevent deviations from normal operation and prevent failures of structures, systems and components (SSCs) important to safety
- Level 2: Detect and intercept deviations from normal operation, in order to prevent anticipated operational occurrences (AOOs) from escalating to accident conditions and to return the plant to a state of normal operation
- Level 3: Minimize the consequences of accidents by providing inherent safety features, fail-safe design, additional equipment and mitigating procedures
- Level 4: Ensure that radioactive releases caused by severe accidents are kept as low as practicable
- Level 5: Mitigate the radiological consequences of potential releases of radioactive materials that may result from accident conditions

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Application of the Graded Approach to Address Fundamental Safety Principles

Canada

Case Studies

- For the following:
  - Case Study #1 – Control
  - Case Study #2 – Cool
  - Case Study #3 – Contain

- What is needed to demonstrate that the **intent** of a requirement is addressed?

Case Study #1: Shutdown Requirements for SMRs (Control)

- For some new SMR designs, vendors claim that an automatic shutdown system is not required to prevent fuel failure because of inherent and new safety features
- As a result, no safety-grade shutdown system is provided (but considered as a process system)
- Given that some vendors claim an automatic shutdown system is not required for preventing fuel failure
  - What is needed to demonstrate that the **intent** of the shutdown requirements are met?

Case Study #2: Emergency Core Cooling Requirements for SMRs

- For some SMR designs, vendors claim that nuclear residual heat from the reactor unit can be removed passively (by thermal conduction, thermal radiation and natural convection) during normal operation, AOOs, design-basis accidents and beyond-design-basis accidents
- Some vendors claim that no emergency core cooling system (ECCS) in the traditional water-cooled reactor sense is required for ensuring nuclear safety of the plant
- Given that some vendors claim an ECCS is not required for preventing fuel failure
  - What is needed to demonstrate that the **intent** of the ECCS design requirements are met?

Case Study #3: Containment Requirements for SMRs

- For some SMR designs, vendors claim that traditional concrete containment structures are not needed for meeting safety objectives and dose limits in case of an AOO, design-basis accident or beyond-design-basis accident
- Some vendors claim that novel design features provide a containment function. Others claim that confinement is necessary for meeting regulatory requirements
- Given that some vendors claim that traditional containment structures are not needed
  - What is needed to demonstrate that the **intent** of the containment design requirements are met?

Case Study Results: Information Needed to Demonstrate That the Intent of a Requirement Is Addressed (1)

- Applicants to demonstrate that the reactor's design and operation are such, that
  - the probability of a loss of cooling, control and containment is so remote, and the consequences of such so low, that no nuclear worker or member of the public would receive a dose above normal levels
  - no offsite contamination would occur

Case Study Results: Information Needed to Demonstrate That the Intent of a Requirement Is Addressed (2)

- Applicants to
  - identify all phenomena or hazards, define failure modes and all postulated accident scenarios, and consider potential unknown phenomena
  - conduct deterministic and probabilistic analysis on all identified phenomena/hazards
  - analysis could be validated through research and development, modelling, small-scale experiments and/or prototypes
- Stakeholders suggested that the CNSC could consider the requirements of cool, control and contain to be met if the applicant can substantiate that the risks associated with a phenomenon are found to be very low

Case Study Results: Information Needed to Demonstrate That the Intent of a Requirement Is Addressed (3)

- Participants indicated that the same type of information was needed for all three case studies
  - facts and data have been derived through validated and quality-assured (i.e., traceable and repeatable) scientific and engineering processes, such as
    - experimental or field-derived data
    - operating experience
    - computer modelling
  - uncertainties have been characterized and accounted for
  - information is demonstrated to be relevant to the specific proposal

Summary

- Assessment of a safety case for a proposed activity is carried out to ensure
  - regulatory requirements are met
  - high-level safety objectives are met
  - fundamental safety functions of “control, cool, contain” are met
- While demonstrating appropriate
  - defence in depth
  - safety margins in view of the uncertainties in the safety case and specific hazards over the lifecycle of the facility

Safety case to be supported by suitable information

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Additional Information: Defence in Depth

Canada

Defence in Depth (**Implementation of Defence in Depth at Nuclear Power Plants:** *Lessons Learnt from the Fukushima Daiichi Accident*, NEA 7248, 2016) **(1)**

LEVEL	IMPLEMENTATION
1. Normal operation: To prevent deviations from normal operation, and to prevent failures of structures, systems and components (SSCs) important to safety.	• Conservative design. • High-quality materials, manufacturing and construction (e.g. appropriate design codes and materials, design procedures, equipment qualification, control of component fabrication and plant construction, operational experience). • A suitable site was chosen for the plant with consideration of all external hazards (e.g. earthquakes, aircraft crashes, blast waves, fire, flooding) in the design. • Qualification of personnel and training to increase competence. • Strong safety culture. • Operation and maintenance of SSC in accordance with the safety case.

Provisions for level 1 commensurate with potential harm from accidents

Defence in Depth (**Implementation of Defence in Depth at Nuclear Power Plants:** *Lessons Learnt from the Fukushima Daiichi Accident*, NEA 7248, 2016) **(2)**

LEVEL	IMPLEMENTATION
2. **Operational occurrences**: To detect and intercept deviations from normal operation, to prevent AOOs from escalating to accident conditions and to return the plant to a state of normal operation.	• Inherent and engineered design features to minimise or exclude uncontrolled transients to the extent possible. • Monitoring systems to identify deviations from normal operation. • Operator training to respond to reactor transients
3. Design basis accidents: To minimise the consequences of accidents and prevent escalation to beyond design basis accidents.	• Inherent safety features. • Fail-safe design. • Engineered design features, procedures that minimise design basis accident (DBA) consequences. • Redundancy, diversity, segregation, physical separation, safety system train/channel independence, single-point failure protection. • Instrumentation suitable for accident conditions. • Operator training for postulated accident response.

Provisions for levels 2 and 3 commensurate with potential harm under accident conditions

Defence in Depth (Implementation of Defence in Depth at Nuclear Power Plants: *Lessons Learnt from the Fukushima Daiichi Accident*, NEA 7248, 2016) **(3)**

LEVEL	IMPLEMENTATION
4. **Beyond design basis accidents**: To ensure that radioactive releases caused by beyond design basis accidents, including severe accidents, are kept as low as practicable.	• Beyond design basis accidents guidance to manage accidents and mitigate their consequences as far as practicable. • Robust containment design with features to address containment challenges (e.g. hydrogen combustion, overpressure protection, core concrete interactions, molten core spreading and cooling). • Complementary design features to prevent accident progression and to mitigate the consequences. • Features to mitigate radiological releases (e.g. filtered vents).
5. **Mitigation of radiological consequences**: To mitigate the radiological consequences of potential releases of radioactive materials that may result from accident conditions.	• Emergency support facilities. • On-site and off-site emergency response plans and provisions. • Plant staff training on emergency preparedness and response.

Provisions for levels 4 and 5 commensurate with potential harm under accident conditions

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Additional Information: Requirements Relevant to the “Control”, “Cool” and “Contain” Case Studies

Canada

Case Study #1: Shutdown Requirements for SMRs (Control)

- Selected existing shutdown requirements in REGDOC-2.5.2 and RD-367
  - shutdown system is a safety system
  - two shutdown systems: SDS1 and SDS2 for CANDU
  - reliability: failure on demand from all causes < 1.0E-3 for each system
  - diversity: rod system (SDS1) and poison injection (SDS2) for CANDU
  - independence: two shutdown systems fully independent from each other and from process systems for CANDU
  - separation: physical separation between two shutdown systems
  - single-failure criterion
  - fail-safe design

Case Study #2: Emergency Core Cooling Requirements for SMRs

- Selected existing emergency core cooling (ECC) requirements in REGDOC-2.5.2 and RD-367
  - ECC system is a safety system
  - reliability: failure on demand from all causes < 1.0E-3
  - independence: ECC system independent from other safety systems and process systems
  - separation: sufficient physical separation between redundant ECC divisions, and other redundant safety or support systems
  - single-failure criterion
  - fail-safe design

Case Study #3: Containment Requirements for SMRs

- Selected existing containment requirements in REGDOC-2.5.2 and RD-367
  - containment is a safety system
  - in the event of an accident, containment boundary capable of allowing for sufficient time for the implementation of offsite emergency procedures
  - separation: sufficient physical separation between containment components
  - single-failure criterion
  - fail-safe design