A Risk-Informed Approach To The Development Of Severe Accident Requirements

G. Rzentkowski and V. Q. Tang
Canadian Nuclear Safety Commission
280 Slater Street, Ottawa, K1P 5S9, Canada

Abstract

This paper describes the application of a risk-informed approach to the development of severe accident requirements. The aim is to ensure prevention of accident progression and mitigation of the consequences of severe plant conditions so that the risk to the public that originates from accidents outside the design basis is also addressed, and to demonstrate that power plant operation does not pose any significant additional risk in comparison with other risks to which the public is normally exposed. Some illustrative examples of relevant requirements under consideration are also provided.

1. Introduction

In response to the renewed interest in a nuclear energy option, the CNSC is reviewing the regulatory framework for licensing new nuclear power reactors, [1]. The intention underlying this work is to update the licensing basis for future power reactors; namely, a set of comprehensive requirements for design, siting, construction and operation of power reactors which are risk-informed and closely aligned with accepted international practices.

The first step in updating the licensing basis is the revision of the requirements for the design of nuclear power reactors, [2,3]. The IAEA Safety Standard NS-R-1, [4], was selected as the underlying template for the development of these requirements which, to a large extent, are technology neutral. Since the current regulatory framework has been largely constrained to the design basis accidents, particular emphasis is placed on severe accident aspects. Consequently, the design envelope[1] for new nuclear power plants has been extended to include not only the capabilities of the plant to successfully cope with various plant states -- ranging from normal operation, Anticipated Operational Occurrences (AOOs)[2] and Design Basis Accidents (DBAs)[3] -- but also complementary, practical measures to halt the

[1] A plant design envelope comprises design capabilities for all credible plant states considered in the design, including normal operating, AOO, DBA, and BDBA states.
[2] An operational process that deviates from normal operation without exceeding safety limits to result in an accident condition.
[3] Accident conditions against which a nuclear power plant is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.

progression of Beyond Design Basis Accidents (BDBAs)[4]. The proposed design requirements establish clear safety goals that a nuclear power plant design must meet to minimize any significant additional risk to the public in comparisons with other risks to which the public is normally exposed.

In the current regulatory framework the potential consequences from severe accidents are only implicitly addressed by considering dual failures events which, as reflected in the document known as the Siting Guide, [5], involve a process system failure coinciding with a safety system failure. (Besides specifying the radiological dose limits for dual failure events, the Siting Guide also suggests to minimize the likelihood of dual failures by setting limits on the frequency of the initiating single failure event and the frequency of failure on demand of protective devices.) As a result, unlikely combinations of events, such as a Loss of Coolant Accident with a consequent Loss of Emergency Coolant Injection, were included in the plant design. An application of the dual-failure approach has undoubtedly led to a robust reactor design and assurance of high reliability of reactor process and safety systems. Severe accidents, however, were not examined in a systematic manner to clearly demonstrate that the residual risk associated with multiple failures of protective barriers is minimized to the extent practicable.

2. General approach

The general approach to the development of the design requirements, [2], starts from the Nuclear Safety and Control Act as reflected in the CNSC Mission Statement and supported by the nuclear safety objectives. The safety objectives are focused on the radiation protection and technical safety. They can be defined as:

- ensure that in all operational states, public and station staff exposures to radiation are kept below prescribed limits, and as low as reasonably achievable;
- take all reasonably practical measures to prevent accidents and to mitigate their consequences should they occur;
- ensure with a high level of confidence that for all possible accidents taken into account in the design of the power reactor, including those of very low probability, any radiological consequences would be minor or below prescribed limits; and
- ensure that the likelihood of accidents with serious radiological consequences is extremely low.

The safety objectives can be achieved by the fundamental safety functions incorporated in the nuclear power plant design which can be expressed as:

- Control - control reactivity;
- Cool - remove heat from the core; and

[4] Accident conditions less frequent and more severe than DBAs. They include severe accidents, resulting from multiple failures of protective barriers that could potentially lead to severe degradation of the reactor core.

- Contain - confine radioactivity and shield radiation

The fundamental safety functions are necessary to maintain a sufficient number of physical barriers to confine the radioactive material. To ensure that the fundamental safety functions are effective, the design specific safety functions, corresponding to basic engineering processes (such as, for example, a reliable shutdown of the reactor or a heat removal from the fuel) are incorporated in the plant design. To the extent practicable, the basic engineering processes should rely on inherent safety characteristics of the reactor.

A defence-in-depth strategy, as recommended by the IAEA, [4], provides a conceptual platform for effective implementation of safety functions. There are five levels to the defence in depth:

- prevention of abnormal operation and failures;
- control of abnormal operation and detection of failures;
- control of accidents within the design basis;
- control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents; and
- mitigation of radiological consequences of significant releases of radioactive materials.

The defence-in-depth strategy is supported by emphasis on inherent safety characteristics of the reactor, and insights from deterministic and probabilistic safety analyses to evaluate and optimize the overall plant design. In principle, an application of the defence-in-depth strategy assures prevention and control of incidents and accidents at several engineering and procedural levels in order to ensure the effectiveness of the protection of physical barriers.

The risk perspective is utilized to ensure a high level of independence of the different levels of protection which is a prerequisite to avoid cascading failure propagation from higher to lower levels of defence-in-depth. This includes identification of initiating events, strategies to prevent initiating events from occurring and from progressing to accidents, and strategies to mitigate the consequences of events and accidents should they occur. The risk perspective is thus essential in balancing strategies of accident prevention and mitigation; that is, higher frequency initiating events and event sequences rely more on prevention, whereas lower frequency initiating events and event sequences rely more on mitigation.

2.1 Design Basis

The design basis of the plant includes various plant states, ranging from normal operation, AOOs and DBAs. The design safety strategy is largely based on the deterministic approach which relies on the sound engineering concepts such as, for example, redundancy, diversity, independence and separation. The aims include ensuring that no single failure prevents the safety systems from carrying out their function, and minimizing the potential for common cause and common mode failures. The design basis challenges to physical barriers are assessed by posing the most severe demands on the safety systems under pre-determined

initial and boundary conditions and analysis rules; typically, with the use of conservative assumptions and safety margins to address uncertainties in the safety analysis.

It is important to recognize that such an analysis approach may, in certain cases, lead to a prediction of unrealistic plant conditions due to the overlapping conservatism used in the modeling of the design basis challenges. In this case, it is not possible to show that an application of the deterministic approach results in a balanced design, providing approximately the same level of protection for all postulated initiating events. The deterministic approach is therefore complemented by the probabilistic analysis which is based on a systematic and comprehensive assessment of risk: that is, the product of the probability of the design basis challenges, leading to an undesired system or reactor state, and its consequences. The risk perspective is thus used, rather implicitly, to evaluate and optimize the overall defence-in-depth strategy by identifying the design basis challenges to physical barriers and by judging their acceptability based on the derived acceptance criteria.

2.2 Beyond design basis

An application of the defence-in-depth extends the design envelope for nuclear power plants to include not only the capabilities of the plant to successfully cope with various design plant states, as discussed in the previous section, but also complementary, practical measures to halt the progression of severe plant conditions. The aim is to ensure mitigation of the consequences of severe plant conditions, either technical (reactor core damage) or radiological (release of radioactive material), to demonstrate that power plant operation does not pose any significant additional risk to the public in comparison with other risks to which the public is normally exposed. The safety goals are thus formulated in addition to deterministic design requirements so that risk to the public that originates from accidents outside the design basis is considered. These safety goals are linked to potential health effects to people in the vicinity of the plant, and are expressed in terms of the risk of a fatality caused by the operation of the nuclear power plant being a small percentage (typically less than 1%) of the risk posed by other industrial activities and societal risks.

There are two fundamental safety goals; one relating to early fatalities and the other relating to late or delayed fatalities. Early fatalities are linked to accident rates (e.g. industrial, traffic, etc.) while late fatalities are linked to cancer rates. The actual numerical safety goal limits that are typically used in the nuclear power industry are conservative surrogates of these goals to simplify their calculation. They are:

- the Severe Core Damage Frequency Goal, and
- the Large Release Frequency Goal.

The Large Release Frequency Goal refers to the frequency of an off-site release that would result in the need for long-term, or even permanent, evacuation of the surrounding population as a result of extensive ground contamination. This requirement is more restrictive than that needed to meet the fatality goals. A numerical value of once every million years for such events is widely accepted in the international nuclear community.

The Severe Core Damage Frequency Goal is a defence-in-depth measure designed to limit reliance on the containment system. The frequency of accidents that could lead to severe core damage is very low, i.e., less than once every hundred thousand years and also is widely accepted in the international nuclear community.

The main tool for demonstrating that the proposed design meets safety goals is the probabilistic safety assessment; Level 1 for the assessment of plant failures and responses of reactor systems (core damage frequency), and Level 2 for the assessment of containment response (large release frequency). The risk perspective is thus explicitly required for the evaluation and optimization of the defence-in-depth strategy for severe plant conditions.

3. Design requirements for severe accidents

The general risk-informed approach outlined above provides a structured, hierarchical framework for the development of the design requirements for severe accidents, namely:

- the plant design shall be capable of meeting established safety goals, setting the limits for the cumulative frequency of core damage and the frequency of radioactivity releases, and
- the design shall include practicable measures to mitigate consequences of severe accidents.

In principle, plant states that could potentially result in high radioactive releases shall be restricted to a very low likelihood of occurrence, and the potential radiological consequences from severe accidents shall be limited as far as practicable.

3.1 General design principles and high-level requirements

The plant designer shall identify and classify possible conditions deviated from normal operation as AOOs, DBAs or BDBAs. The latter category includes severe accidents.

For BDBAs, the plant design must include practicable measures to halt accident progression, return the plant to a controlled state, and mitigate accident consequences. The following relatively high-level requirements can be stated:

- a balanced design shall be demonstrated such that no particular event or design feature makes a disproportionately large or significantly uncertain contribution to the total frequency of severe accidents;
- radiological and combustible gas accident source terms shall be identified for the use in design of systems, structures and components credited for the control of severe plant conditions (fourth level of defence in depth) to practically eliminate the possibility of containment damage in the early phase of an accident;
- the equipment designated for use in severe accident management shall be assessed for its operability under the accident conditions and be shown, with reasonable confidence, to be capable of achieving the design intent; and

- instrumentation shall be provided to monitor plant variables and systems over the entire range of parameters for normal operation, transients and accidents in order to ensure that adequate information on the plant status is available to plant operators.

To determine feasible preventive and mitigating measures, the design approach may rely on either probabilistic or deterministic (phenomenological) analysis with the use of realistic assumptions and criteria.

3.2 Design of containment

The containment shall maintain its role of a leak-tight barrier for a period of approximately 24 hours following the onset of severe core damage. After this period, the containment shall continue to provide a barrier against uncontrolled releases of radioactivity by withstanding potential challenges associated with severe accidents. For example, the containment system shall have a design capability to:

- remove heat and to reduce pressure inside the containment structure to minimize the pressure-induced release of fission products to the environment and to preserve containment integrity,
- control hydrogen concentration to prevent deflagration or detonation which could jeopardize the integrity of the containment structure or penetrations, and
- prevent a melt-through or failure of the containment floor in the reactor vault due to the thermal impact of the core debris (facilitate cooling of the core debris), and
- minimize generation of non-condensable gases and radioactive products as a result of concrete/core interaction..

An important aspect of ensuring the reliability of containment as a leak-tight barrier is prevention of bypass through penetrations, air-locks and interfacing systems. To this end, strict requirements are imposed on leak-tightness, testability and isolation of containment penetrations and piping.

3.3 Design of barriers to arrest or mitigate accident progression

The plant designer shall identify potential barriers at which core degradation in the course of a severe accident can be halted, and consider features that can assist in termination of a core degradation at such barriers. In particular, the redundant capabilities to remove residual heat from the core debris and transfer it to an ultimate heat sink shall be provided. Systems for control and removal of fission products, hydrogen and other combustible gases shall also be provided in the design.

4. Severe accident management

A regulatory guide [7] has been recently issued by the CNSC, describing the elements of a Severe Accident Management (SAM) Program and establishing regulatory expectations.

Accordingly, the licensee should identify the goals of SAM and practical actions to achieve these goals, namely:

- establishing and maintaining reactivity control;
- ensuring availability of heat sink for heat generated in the reactor core;
- depressurizing the primary heat transport system;
- maintaining coolant inventory in the primary heat transport system;
- controlling pressure and water inventory in steam generators;
- ensuring containment isolation;
- controlling the containment pressure and temperature;
- controlling flammable gases concentrations; and
- controlling radioactive product releases.

These high level actions form a starting point for identifying detailed, station specific activities. As appropriate, procedural guidance should be developed for operators and emergency teams to implement such activities.

5. Safety analysis requirements for severe accidents

The deterministic and probabilistic safety analyses shall include consideration of selected severe accidents. These analyses are necessary to:

- demonstrate that safety goals are met;
- show compliance with specific safety requirements;
- assess alternative design solutions;
- provide input for development and verification of SAM programs; and
- provide input for environmental assessment and emergency preparedness planning.

The specific objectives of deterministic analysis include:

- identify the key phenomena and determine the timing of events and conditions during the accident progression;
- specify the criteria that would indicate the onset of a severe accident;
- assist in evaluation of measures and systems required to arrest the accident progression and to mitigate the consequences;
- evaluate performance of plant systems under accident conditions;
- identify the symptoms for use in accident management that allow determining the reactor core condition and state of protective barriers;
- evaluate challenges to fission product barriers and their timing in order to improve the potential for successful human intervention;
- help identify the material resources that may be needed for SAM purposes; and
- verify that SAM actions are effective to counter challenges to protective barriers.

In addition to the demonstration that the safety goals are met, results of probabilistic safety analyses can be used for a number of purposes, such as:

- demonstrate that a balanced design has been achieved such that no particular feature or event makes a disproportionately large or significantly uncertain contribution to the total frequency of severe accidents;
- identify specific systems for which design improvements can be justified on the basis of reduction of probabilities of severe accidents;
- provide basis for cost-benefit assessments of any potential design or operational modifications;
- identify credible accident scenarios for SAM validation purposes; and
- select accident scenarios for personnel training and drill purposes.

6. Summary

The application of the risk-informed approach to the development of severe accident requirements for new nuclear power plants in Canada has been presented.

The approach is based on fulfilling the safety objectives (focused on the radiation protection and technical safety), assuring the fundamental safety functions (cool, control and contain), and fully implementing all levels of defence in depth. An implementation of the defence-in-depth strategy assures prevention and control of incidents and accidents at several engineering and procedural levels in order to ensure the effectiveness of the protection of physical barriers. The defence-in-depth strategy is supported by emphasis on inherent safety characteristics of the reactor, and insights from deterministic and probabilistic safety analyses to evaluate and optimize the overall plant design.

The proposed design requirements establish clear safety goals, in addition to deterministic considerations, that a nuclear power plant design must meet to minimize any significant additional risk to the public in comparisons with other risks to which the public is normally exposed. In principle, the likelihood of accidents with serious radiological consequences shall be extremely low, and the potential radiological consequences from severe accidents shall be limited as far as practicable. Effectively, the proposed requirements extend the plant design envelope to include not only the capabilities of the plant to successfully cope with various plant design states, but also practical measures to halt the progression of severe accidents.

9. References

1. G. Rzentkowski, I. Grant, T. Viglasky, “Development of Licensing Basis for Future Power Reactors in Canada”, Proceedings of the 26th Annual Canadian Nuclear Society Conference; June, 2005.

2. G. Rzentkowski, A. Banas, D. Miller, "An approach to the Development of Licensing Basis for New Power Plants in Canada", Proceedings of the 25th Annual Canadian Nuclear Society Conference, Toronto, Canada, June 2004
3. CNSC Pre-consultative Draft Document, "*Requirements for Design of Nuclear Power Plants*", March 2005.
4. IAEA, "Safety of Nuclear Power Plants: Design Safety requirements", IAEA Safety Standard Series No. NS-R-1, October 2000.
5. G. C. Laurence, "Reactor Siting Criteria and Practice in Canada", AECB # 1010, Presented at the American Nuclear Society National Topical meeting on Nuclear Reactor Power Siting, Los Angeles, February, 1965.
6. IAEA, "Guidance for the Evaluation of Innovative Nuclear Reactors and Fuel Cycles", IAEA-TECDOC-1362, June 2003.
7. CNSC, "Severe Accident Management Programs for Nuclear Reactors", Regulatory Guide G–306, Published by the Canadian Nuclear Safety Commission, May 2006.