Canada's Nuclear Regulator

Design Extension Conditions for Nuclear Power Plants

Discussion Paper DIS-14-01

August 2014

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Canada

Design Extension Conditions for Nuclear Power Plants
Discussion Paper DIS-14-01

Également publié en français sous le titre : Conditions additionnelles de dimensionnement pour les centrales nucléaires.

Document availability

This document can be viewed on the CNSC website at nuclearsafety.gc.ca. To request a copy of the document in English or French, please contact:

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

Tel.: 613-995-5894 or 1-800-668-5284 (in Canada only)
Facsimile: 613-995-5086
Email: info@cnsc-ccsn.gc.ca
Website: nuclearsafety.gc.ca
Facebook: facebook.com/CanadianNuclearSafetyCommission
YouTube: youtube.com/cnscccsn

Publishing history

August 2014 Version 1.0

Preface

Discussion papers play an important role in the selection and development of the regulatory framework and regulatory program of the Canadian Nuclear Safety Commission (CNSC). They are used to solicit early public feedback on CNSC policies or approaches.

The use of discussion papers early in the regulatory process underlines the CNSC's commitment to a transparent consultation process. The CNSC analyzes and considers preliminary feedback when determining the type and nature of requirements and guidance to issue.

Discussion papers are made available for public comment for a specified period of time. At the end of the first comment period, CNSC staff review all public input, which is then posted for feedback on the CNSC website for a second round of consultation.

The CNSC considers all feedback received from this consultation process in determining its regulatory approach.

Table of Contents

Executive Summary

The Canadian Nuclear Safety Commission (CNSC) is mandated under the *Nuclear Safety and Control Act* to regulate the use of nuclear energy and materials to protect health, safety, security and the environment, and to implement Canada's international commitments on the peaceful use of nuclear energy; and to disseminate objective scientific, technical and regulatory information to the public.

Following the 2011 disaster in Fukushima, Japan, nuclear regulators around the world launched a comprehensive review of their major nuclear facilities. For its part, the CNSC established the CNSC Fukushima Task Force to review the capability of nuclear power plants (NPPs) and other nuclear facilities across the country to withstand conditions comparable to those that triggered the Fukushima accident. The task force concluded that Canadian nuclear power plants are safe and the risk posed to the health and safety of Canadians or to the environment is small.

The task force also reviewed the CNSC's regulatory framework and processes. It confirmed that the Canadian regulatory framework is strong and comprehensive. Nevertheless, it identified and outlined a series of recommendations aimed at further enhancing the safety of nuclear facilities in Canada. These recommendations are detailed in actions A.9.1 to A.9.3 of the *CNSC Integrated Action Plan on the Lessons Learned from the Fukushima Daiichi Nuclear Accident* [1].

Part of the ongoing international examination of the Fukushima accident has resulted in increased effort in developing prevention and mitigation strategies for accident situations and scenarios beyond those considered during the initial design of nuclear facilities. These accident scenarios are termed design extension conditions (DECs) and their consideration is becoming increasingly prevalent within the international nuclear community. DECs, or similar concepts, are being examined and adopted by nuclear regulators in a number of countries. Appendix B provides further details in this regard. The CNSC is working closely with the international nuclear community to identify and adopt best practices as considerations regarding DECs evolve. At the same time, the CNSC is committed to engaging in a meaningful domestic dialogue with all interested stakeholders regarding DECs.

The CNSC first publicly used the term DECs in draft regulatory document RD-337, version 2, *Design of New Nuclear Power Plants*, [2] issued for public consultation in July 2012. This document has now been finalized as REGDOC-2.5.2, *Design of Reactor Facilities: Nuclear Power Plants*, [3] and supersedes RD-337. This document establishes design requirements and expectations for new NPPs. It also includes high-level requirements and expectations related to DECs. As described in REGDOC-2.5.2, the safety objectives in DECs are to prevent core damage, mitigate accident consequences and protect containment integrity. Within Canada and around the world, opinions differ as to how DECs should be defined, characterized and selected. Additionally, there is no consensus on what prevention and mitigation plans should be created to address them.

Throughout this paper, DECs are described in relation to other plant states. It is important to emphasize that DECs are considered a subset of beyond-design-basis accident (BDBA) conditions. The rationale for this is that BDBA conditions extend to include accidents that, due to their extremely low probability of occurrence, are considered to be "practically eliminated". It is important to note that DECs would not include conditions that are considered to be "practically eliminated".

Another important premise of this paper is that DECs do not represent an extension of the conservative design basis or "high confidence" associated with other plant states. Instead, the principle of "reasonably high confidence" in the success of activities associated with DECs is introduced in this paper. It follows,

therefore, that this principle should be applied uniformly in DECs across various aspects of design, analysis and operation.

While the CNSC does not think a dedicated REGDOC on DECs is needed, the concept may be addressed in a number of draft and existing REGDOCs and Canadian standards. These documents potentially cover a range of subject areas, including design, analysis, construction, operation, procedures and radiation protection. The CNSC recognizes that requirements and guidance that would apply to equipment, analysis and procedures for DECs have not yet been fully developed.

This paper summarizes the CNSC's current understanding of DECs. Its intent is not to provide a CNSC position but to stimulate discussion on the subject of DECs.

Finally, it should be noted that several factors contribute to improving protection for the Canadian public against unlikely accidents at an NPP. Post-Fukushima upgrades to Canadian NPPs have extended the capabilities of plants to withstand very improbable events. The NPP's safety assessments have confirmed that increased safety is achieved. The CNSC Regulatory Framework has been updated to include appropriate requirements and guidance related to design, analysis and operation of NPPs. Several of these activities are still ongoing.

This document describes a consistent approach to establishing requirements and guidance related to DECs and although the paper presents a series of questions for the reader's consideration, comments and feedback should not be limited to these. Comments on any issue pertinent to the topic of DECs are encouraged.

Design Extension Conditions for Nuclear Power Plants

1. Introduction

Following the 2011 disaster in Fukushima, Japan, nuclear regulators around the world launched a comprehensive review of their major nuclear facilities. For its part, the CNSC established the CNSC Fukushima Task Force to review the capability of nuclear power plants (NPPs) and other nuclear facilities across the country to withstand conditions comparable to those that triggered the Fukushima accident. The task force concluded that Canadian nuclear power plants are safe and the risk posed to the health and safety of Canadians or to the environment is small.

The CNSC Fukushima Task Force also reviewed the CNSC's regulatory framework and processes. It confirmed that the Canadian regulatory framework is strong and comprehensive. Nevertheless, it outlined a series of recommendations aimed at further enhancing the safety of nuclear facilities in Canada. These recommendations are detailed in actions A.9.1 to A.9.3 of the *CNSC Integrated Action Plan on the Lessons Learned from the Fukushima Daiichi Nuclear Accident*.

Several factors contribute to improving protection for the Canadian public against unlikely accidents (DECs) at a NPP. Post-Fukushima upgrades to Canadian NPPs have extended the capabilities of plants to withstand very improbable events. The NPP's safety assessments have confirmed that increased safety is achieved. The CNSC Regulatory Framework has been updated to include appropriate requirements and guidance related to design, analysis and operation of NPPs. Several of these activities are still ongoing. This document describes a consistent approach to establishing requirements and guidance related to DECs.

Part of the ongoing international examination of the Fukushima accident has resulted in increased effort in developing prevention and mitigation strategies for accident situations and scenarios beyond those considered during the initial design of nuclear facilities.

1.1 Design Basis

The term "design basis" is defined in REGDOC-2.5.2 *Design of Reactor Facilities: Nuclear Power Plants*, [3] as:

> [t]he range of conditions and events taken explicitly into account in the design of the facility, according to established criteria, such that the facility can withstand them without exceeding authorized limits by the planned operation of safety systems.

The design basis is applied through regulatory requirements and applicable national and international codes and standards. Requirements for the design basis are typically very conservative and rigorous. They provide a very high level of confidence that an NPP can meet safety requirements following any accident scenarios that were considered at the time of plant design and for which prevention and mitigation provisions were put in place. Design-basis accidents (DBAs) are accident conditions for which a reactor facility is designed, according to established design criteria (the design basis), and for which damage to the fuel and the release of radioactive material are kept to a minimum.

1.2 Considering Accidents beyond the Design Basis

The CNSC REGDOC-2.5.2 sets forth proposed requirements for structures, systems and components (SSCs) that have a role in the management of accidents beyond those considered in the design basis, particularly for severe accidents (SA). SAs are defined in REGDOC-2.3.2 *Operating Performance: Accident Management: Severe Accident Management Programs for Nuclear Reactors* [4] as:

> [a]n accident more severe than a design-basis accident, and involving significant core degradation or significant fuel degradation in the spent fuel pool (also called the irradiated fuel pool).

The term "design extension conditions" is used to describe those accidents, beyond the design basis, for which additional prevention and mitigation provisions are required.

According to REGDOC-2.5.2, the reactor design is expected to provide the means to:

- address plant-specific severe accident challenges
- provide design features that help ensure safety goals are met and accident management objectives and strategies are achieved
- prevent significant releases of radioactive materials into the environment

REGDOC-2.5.2 establishes the "plant design envelope" which comprises normal operation (NO), anticipated operational occurrences (AOO), DBAs and DECs. Figure 1 is taken from REGDOC-2.5.2. It shows the relationship of DECs to the other plant states.

In RD-337 version 1, DECs were referred to as "credible beyond-design-basis accidents (BDBAs)". Conditions and events that are practically eliminated are those with such a low probability of occurring that they are not considered to be DECs.

DECs may take into account accidents involving the reactor core, spent fuel pools and, where appropriate, multiple units at a site. Such accidents could be triggered by multiple failures of equipment, operator errors, internal or external events and, most probably, by a combination of events and failures. When major accidents occur they are complex with many contributing factors. The CNSC does not intend to define a lower frequency boundary for DECs, because of large uncertainties in obtaining credible frequencies for exceedingly rare events. The approach for identifying a set of BDBAs to be treated as DECs inevitably involves a measure of judgment.

It is important to note that DECs, as illustrated, are a selected subset of BDBAs conditions and not an extension of the design basis.

Figure 1: Plant states

<table>
<tr><td colspan="2">Operational states</td><td colspan="4">Accident conditions ➔</td></tr>
<tr><td rowspan="3">Normal operation</td><td rowspan="3">Anticipated operational occurrence</td><td rowspan="3">Design-basis accident</td><td colspan="3">Beyond-design-basis accidents ➔</td></tr>
<tr><td colspan="2">Design extension conditions</td><td>Practically eliminated conditions ➔</td></tr>
<tr><td>No severe fuel degradation</td><td colspan="2">Severe accidents ➔</td></tr>
<tr><td colspan="3">Design basis</td><td>Design extension</td><td>Not considered as design extension ➔</td></tr>
</table>

Reducing frequency of occurrence ➔

Appendix A offers a more complete description of the plant states diagram and shows the relationship between plant states and other aspects of NPP design, analysis and operation.

Question 1: Have DECs been characterized in a manner that is clear and logical?

2. Proposed Definitions and Key Concepts

2.1 Plant design envelope

REGDOC-2.5.2, *Design of Reactor Facilities: Nuclear Power Plants,* requires the plant design authority[1] to consider prevention and mitigation of a broad range of accidents at the design stage and to meet dose acceptance criteria and probabilistic safety goals. There should be reasonably high confidence that prevention and mitigation features should operate as expected in the unlikely event of a severe accident. The design authority should also exhibit an understanding of accident progression and associated phenomena, and is required to establish, at the design stage, initial severe accident management guidelines (SAMGs) that are based on an understanding of accident progression and that take plant design into account.

For this reason the plant design envelope is defined in REGDOC-2.5.2 as:

> [t]he range of conditions and events (including DEC) that are explicitly taken into account in the design of the nuclear power plant such that significant radioactive releases would be practically eliminated by the planned operation of process and control systems, safety systems, safety support systems and complementary design features.

[1] **Plant design authority** typically rests with the organization that has overall responsibility for the design. Prior to plant start-up, this authority must be transferred to the operating organization. The design authority may assign responsibility for the design of specific parts of the plant to other organizations, known as responsible designers. The tasks and functions of the design authority and any responsible designer need to be established in formal documentation; however, the overall responsibility remains with the design authority.

2.2 Design extension conditions

REGDOC-2.5.2 defines DECs as follows:

> [a] subset of beyond-design-basis accidents that are considered in the design process of the facility in accordance with best-estimate methodology to keep releases of radioactive material within acceptable limits. Design extension conditions could include severe accident conditions.

The concept of DECs is complex. It encompasses plant states, conditions and events, including external events, as well as those involving the reactor, or the handling and storage of the irradiated fuel.

2.3 Confidence

For DBAs, there is "high confidence" in the ability of the structures, systems and components (SSCs) to perform as designed. However, in DECs there should be "reasonably high confidence" that the SSCs will perform as designed. A certain degree of conservatism is still expected for addressing challenges where the available knowledge is not sufficient to characterize the best-estimate conditions.

Reasonably high confidence may be achieved through the adequate selection of the conditions considered in the design and of the rules governing such matters as design, testing, periodic inspection and maintenance of the SSCs intended to be used for the management of SAs.

2.4 Significant radioactive release

REGDOC-2.5.2 section 7.3.4 requires that:

> [t]he design shall be such that plant states that could lead to significant radioactive releases are practically eliminated. For plant states that are not practically eliminated, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public, and sufficient time shall be made available to implement these measures.

For DECs, protective measures must be limited in area and time. For example, a significant radioactive release could not be considered limited in location or time. Such a hypothetical release, if it were to lead to a long-term relocation of population would be classified as a "significant release". A radioactive release that requires only sheltering is unlikely to be considered "significant". However, a release that leads to short-term evacuation would be considered significant if the area to be evacuated were large or the duration long. Distinguishing requires a level of judgement.

2.5 Practically eliminated

The key design objective for NPPs is that significant releases are practically eliminated. This objective recognizes that the possibility of certain conditions or accidents is either physically impossible or judged with a high level of confidence to be extremely unlikely. Demonstration of practical elimination of an accident sequence may involve deterministic and probabilistic considerations. It should also take into account uncertainties associated with a limited knowledge of some of the important and applicable physical phenomena. REGDOC-2.5.2, section 7.3.4 provides guidance on demonstrating that accident sequences have been practically eliminated.

There are uncertainties in quantifying failure probabilities for SA scenarios. One is the failure rate for components that operate beyond their levels of qualification. Some tools that may help to achieve the appropriate level of confidence that severe releases have been practically eliminated include: defence in depth, the use of passive safety features, the use of multiple independent controls, and the application of the safety principles of independence, diversity and separation.

2.6 Identification of DECs

The design authority is responsible for identifying, selecting and classifying the events or conditions that comprise DECs. Currently, there is no formally agreed upon and recognized means for identifying DECs. An understanding of accident progression, processes and accident phenomena is relevant and examination of the following is suggested:

- identification and selection of representative events and accident sequences for determining actual design conditions
- identification of major design options and specific plant-design features for the mitigation of SAs and their roles in achieving severe accident management (SAM) goals
- identification of the conditions needed for the design of plant features to be used in preventing and mitigating consequences of SAs
- SAM strategies for mitigating challenges posed by SAs while at the same time ensuring reliable operation of safety functions and returning the plant to a stable controlled state
- deterministic accident analyses for design support

Considerations to identify and select DECs may include:

- accident scenarios that include combinations of initiating events, human error and SSC success/failure
- design features considered in the prevention or mitigation of a BDBA or an SA and defining their intended roles
- parameters for design features considered for use in preventing or mitigating a BDBA or an SA
- factors of the accident progression relevant for determining limiting values and ranges for the timing and amplitude of the parameters needed for design
- initiating events, human error and SSC operability (success, failure) , which are relevant for determining the limiting values and ranges of the parameters needed for design
- an optimal set of accident scenarios to reduce it to a manageable number of sequences

Underpinning identification and selection of DECs is the expectation that, in the DEC plant state, the practical elimination of significant releases is achieved. For a more in-depth discussion on the identification of DECs, please see Appendix C.

Question 2: Are the items included for the purposes of identifying DECs clear, logical, sufficient and/or required?

3. Objectives and Requirements for DECs

The safety objectives for DECs are to prevent severe core damage, mitigate accident consequences and protect containment integrity as long as possible. To meet these objectives, the CNSC believes that the following are key:

- inclusion of plant design features to be used for accident management

- specification of requirements for containment performance during DECs (such as maintaining the leak-tight barrier for a certain duration with no uncontrolled release thereafter)
- consideration of accident management needs and requirements

The underlying principle is to provide "reasonably high confidence" that SSCs will operate as intended during a DEC.

3.1 Design objectives and requirements

REGDOC-2.5.2 sets overall safety objectives for NPPs through dose acceptance criteria and safety goals. It sets specific design requirements for conditions and events within the plant design envelope. It does not set design requirements for BDBAs that are considered to be "practically eliminated".

3.1.1 Scope

Design objectives should be established for equipment that may be used in DECs. This equipment may include, but is not limited to:

- complementary design features[2], such as core catchers and containment-filtered venting systems that are dedicated to limiting or mitigating the effects of severe accidents
- fixed or portable equipment located onsite or offsite, such as mobile pumps or electric power generators
- safety or process SSCs that may be planned to be used beyond their design bases

The design requirements for safety systems should be very conservative for DBAs in order to provide very high confidence. Reasonably high confidence would be expected in the unlikely event of DECs.

3.1.2 Safety classification

Safety classification considers:

- the safety function(s) to be performed
- consequence(s) of failure
- the probability that the SSC will be called upon to perform the safety function
- the time following a postulated initiating event at which the SSC will be called upon to operate and the expected duration of that operation

These considerations allow the design authority to account for factors such as redundancy of equipment and the possibility of implementing alternative strategies. Although the probability of SSCs being called upon during DECs is very low, the failure of safety functions for the mitigation of DECs may lead to high-severity consequences. These safety functions should be assigned a safety category commensurate with their safety significance. Testing and maintenance requirements for equipment to be used in DECs would be established in accordance with their safety classification.

---

[2] **Complementary design feature**: An element added to the design as a stand-alone SSC or as an added capability to an existing SSC to cope with DECs.

3.1.3 Survivability of equipment

REGDOC-2.5.2 requires that:

> [e]quipment and instrumentation credited to operate during DECs shall be demonstrated, with reasonable confidence, to be capable of performing their intended safety function(s) under the expected environmental conditions. A justifiable extrapolation of equipment and instrumentation behaviour may be used to provide assurance of operability, and is typically based on design specifications, environmental qualification testing and/or other considerations.

Survivability of equipment and instrumentation in DECs should consider the following:

- functions that need to be performed in the accident timeframe to achieve a safe shutdown state for DECs
- the accident timeframe for each required function
- the location and type of equipment used to perform necessary functions in each timeframe
- the harsh environmental conditions of DECs within each timeframe
- assurance that the equipment will survive to perform its function in the accident timeframes established in the DECs plant state

3.2 Analysis requirements

REGDOC-2.4.1, *Deterministic Safety Analysis*, [5] specifies requirements for deterministic safety analysis for AOOs, DBAs and BDBAs. Although the document refers to BDBAs, it does not specify requirements for DECs. This is because the analysis discussed in REGDOC-2.4.1, unlike the design process, might consider events of lower frequency than DECs. Section 4.3.3 of REGDOC-2.4.1, *Deterministic Safety Analysis*, states:

> A safety assessment for BDBAs shall be performed to demonstrate that:
>
> 1. The NPP as designed can meet the requirements for release limits established as the safety goals. A deterministic safety analysis provides consequence data for accident sequences to use in the PSA [probabilistic safety assessment].
> 2. The procedures and equipment put in place to handle the accident management needs are effective, taking into account the availability of cooling water, material and power supplies; consideration can be given to the plant's full design capabilities, including the possible use of safety, non-safety, and temporary systems beyond their originally intended function.

Deterministic BDBA analysis supports the evaluation of safety goals in conjunction with PSAs. It also demonstrates the adequacy of the design provisions and accident management programs. Therefore, deterministic safety analysis is also performed to demonstrate that the complementary design features will function as designed in DECs.

Deterministic analysis should be performed for an event leading to the highest challenge to maintaining the containment function.

The generally accepted principal for analysis of BDBAs is the best-estimate approach. This is consistent with International Atomic Energy Agency (IAEA) documents such as SSG-2, *Deterministic Safety Analysis for Nuclear Power Plants* [6] and SRS No. 56, *Approaches and Tools for Severe Accident Analysis for Nuclear Power Plants* [7]. Section 4.4.4 of REGDOC-2.4.1 states:

> [f]or the analysis of BDBA, it is acceptable to use a more realistic analysis methodology consisting of assumptions that reflect the likely plant configuration, and the expected response of plant systems and operators in the analyzed accident.

One of the reasons for using best-estimate methods and computer codes in BDBA analysis is related to accident management. Should an accident progress to the conditions beyond the design basis, accident management actions become an important part of defence-in-depth. The consequences of BDBAs are estimated so that the analysis reflects a realistic plant response and provides best-estimate information for accident management.

Analysis of BDBAs may use applicable[3] input from PSAs and may credit all the available SSCs, as long as it has been demonstrated with reasonably high confidence that they are able to perform their intended function. It is worth noting that the single-failure criterion, which applies to all safety groups credited in the DBA analysis, is not normally applied in the BDBA analysis.

3.3 Operational requirements

RD/GD-210, *Maintenance Programs for Nuclear Power Plants*, [8] covers maintenance, testing and inspection requirements. RD/GD-98, *Reliability Programs for Nuclear Power Plants*, [9] sets out the requirements for and provides guidance on reliability programs. Applicability of these regulatory requirements to DECs features should be based on their safety classifications.

3.4 Procedures

While design provisions are necessary to maintain and strengthen the existing multiple physical barriers to fission product release, it is also important that adequate procedures be in place to manage and mitigate DECs.

Procedural barriers relevant to DECs include those pertinent to accident management and emergency response. The accident management guidelines are symptom-oriented and do not depend directly on any predefined events. Operating manuals, emergency operating procedures (EOPs) and SAMGs provide a continuity of coverage between normal plant operation and severe accident conditions. Transitions between the types of procedures depend on measured conditions of the plant, not on an abstract definition of plant state.

Additional training requirements and plans may be contained in EOPs and SAMGs. The procedures and guidelines relevant to DECs should follow the principle of "reasonably high confidence" in their design, verification, validation and implementation. These procedures and guidelines should consider human factors and organizational performance to ensure that accident management actions are executed correctly and in a timely manner.

---

[3] **Applicability** is shown by demonstrating that the assumptions, models, rules, etc. used for generation of the information in the PSA are compatible with the use of that data.

SAMGs should provide guidelines for use of the complementary design features, including mobile onsite and offsite equipment and instrumentation to be used in DECs.

Draft REGDOC-2.3.2, *Accident Management*, [10] will respond to the CNSC Fukushima Task Force recommendation that the CNSC publish a dedicated regulatory document on accident management. According to draft REGDOC-2.3.2, an accident management program consists of an integrated set of plans, procedures, guidelines and arrangements to be used for accident management. They should address key issues such as identifying the challenges to plant and public safety, providing appropriate equipment and instrumentation, implementing guidance for personnel involved in accident management, and assuring adequate human and organizational performance.

Applicable regulatory documents for offsite emergency response include G-225, *Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills*, [11] and RD-353, *Testing the Implementation of Emergency Measures* [12]. While an emergency does not correlate with any particular plant state, by definition DECs would also be subject to the regulatory requirements for emergencies.

Draft REGDOC-2.10.1, *Nuclear Emergency Preparedness and Response*, [13] is currently under development. When published and incorporated into licensing, it will supersede G-225, *Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills*, and RD-353, *Testing the Implementation of Emergency Measures*. It will fulfill the recommendations of the CNSC Fukushima Task Force – and the External Advisory Committee – to strengthen regulatory requirements for licensees' emergency preparedness programs. Draft REGDOC-2.10.1 lists and discusses the requirements of an emergency-preparedness program and offers guidance for building such a program.

Guidance for human factors is provided in G-276, *Human Factors Engineering Program Plans*, [14], and G-278, *Human Factors Verification and Validation Plans* [15].

The CNSC will be reviewing the above documents to ensure that the principle of "reasonably high confidence" is applied consistently for events beyond the design basis.

3.5 Radiation protection requirements

All plant states, including DECs, are subject to the CNSC's framework for radiation protection and the "as low as reasonably achievable" (ALARA) principle is applied in the control of radiological hazards and radiation exposures.

The CNSC has issued a discussion paper, DIS-13-01, *Proposals to Amend the Radiation Protection Regulations*, [16] detailing proposed amendments to address recommendation 8 of INFO-0824, *CNSC Fukushima Task Force Report* [17]. It advised that the *Radiation Protection Regulations* (RPR) [18] may be amended to be more consistent with current international guidance. To accomplish this, the RPR would be amended to set out in greater detail the regulatory requirements needed to address radiological hazards during the various phases of an emergency. These proposed regulatory amendments, should they receive approval from the Governor in Council, may impact the identification, design and analysis requirements of DECs.

Question 3: Does the above accurately define and cover the elements that should be included in the design objectives and requirements for DECs?

4. Applicability to NPPs in Canada

4.1 New NPPs

REGDOC-2.5.2, *Design of Reactor Facilities: Nuclear Power Plants* applies to the design of all new NPPs. As such, in considering DECs, the design authority for new NPPs must use a systematic approach to:

- address all known accident challenges within DECs
- have a balanced design between severe accident prevention and mitigation of accidents, with particular emphasis on prevention of containment failure
- integrate with the needs of the plant-specific accident management program to ensure the design provisions are available for management of accidents

4.2 Existing NPPs

Existing NPPs are outside of the scope of REGDOC-2.5.2. However, REGDOC-2.5.2 may be referenced in a review against modern standards prior to refurbishment or extended operation (e.g., via application of RD-360, *Life Extension for Nuclear Power Plants* [19]). For existing NPPs, the focus should be on:

- identifying and evaluating the existing design features that can be used to respond to challenges posed by DECs
- ensuring no vulnerability of the containment system, in conjunction with the accident management program
- implementing design upgrades where necessary to meet safety goals or accident management needs, or to counter specific challenges

It is noted that many upgrades have been made, planned, or are under consideration, at existing NPPs. These upgrades are a result of safety reviews performed at the time of refurbishment or following the Fukushima accident. Many of these upgrades address the ability to manage and mitigate DECs. Design requirements for these upgrades have been selected by licensees using best engineering judgment and reviewed by the regulator in a risk-informed manner. As part of implementing these upgrades, specific issues requiring regulatory guidance are being identified and addressed.

Further updates to the CNSC regulatory framework, identified in Section 3 and related CSA Group[4] standards, will take a number of years to develop. In the interim, it is suggested that industry stakeholders work closely with the CNSC to develop internal processes and to ensure greater clarity of the principles and concepts described in this discussion paper. Similarly, the CNSC, CSA Group and industry should work together to ensure that revised requirements and guidance documents follow the clarified principles and concepts. Extensive collaboration should enable industry practices and regulatory requirements to converge. Doing so will facilitate licensing and compliance verification once new requirements and guidance documents are issued.

Question 4: Are there other Canadian nuclear facilities, besides NPPs, that could potentially benefit from the application of DECs?

[4] **CSA Group:** Name by which the Canadian Standards Association is now known.

5. Research and Development in Support of DECs

Many physical phenomena associated with SAs are extremely complex. For some SAs, the current level of knowledge and modelling capabilities is limited. Quite frequently, the experimental studies required to augment such understandings cannot be conducted in fully representative conditions. This fact complicates the task of developing and validating models.

The high cost of experiments and the limited number of suitable facilities to perform studies of relevant phenomena necessitates wide international cooperation. While driven by considerations of efficiency, this approach is facilitated by the fact that many SA phenomena are common or similar in various reactor types. Domestic and international research activities in this area aim to reduce the uncertainties in available knowledge and allow more accurate modelling of accident progression and consequences.

Research should address the needs of the currently operating reactors as well as future reactors. Modifications of operating reactors are often limited and research in this area is primarily aimed at minimizing the potential impact of SAs. One of the key aspects to be addressed through research and development is the study of cliff-edge effects that may lead to non-linear and unexpected responses from existing plant SSCs. Cliff-edge effects may be described as a large increase in the severity of an event caused by a small change in conditions. They can be caused by changes in the magnitude of the event or changes in the plant or operator response.

6. Conclusion

The CNSC has published high-level requirements and guidance for design and analysis in REGDOC-2.5.2, *Design of Reactor Facilities: Nuclear Power Plants* and REGDOC-2.4.1, *Deterministic Safety Analysis*. However, detailed requirements and guidelines that apply to equipment, analysis and procedures for DECs are not fully developed. Nonetheless, the CNSC is of the opinion that the principle of "reasonably high confidence" should be applied to all activities associated with DECs. An ongoing dialogue between regulators, designers, operators, standards organizations and other interested stakeholders is necessary to define how "reasonably high confidence" can be achieved.

Although already stated, it is worth repeating that the CNSC does not think a dedicated regulatory document on DECs is necessary. The concept may be addressed in a number of draft and existing regulatory documents and Canadian standards. These documents potentially cover a range of subject areas, including design, analysis, construction, operation, procedures and radiation protection. They could be applicable to existing and future NPPs as well as to small reactor facilities.

The CNSC is committed to working with all interested stakeholders in developing prevention and mitigation strategies for accident situations and scenarios beyond those considered during the initial design of a nuclear facility. This paper has set out the CNSC's views regarding DECs in relation to other plant states in the hope of encouraging substantive stakeholder dialogue. Its intent is not to offer a definitive CNSC position, but to stimulate discussion on the subject of DECs.

Question 5: Should the CNSC consider revising its regulatory documents to account for DECs? If yes, should they be expanded to explicitly cover equipment and procedures that may be used in DECs?

Feedback

Comments or feedback may be submitted to the CNSC in one of the following ways:

By email: consultation@cnsc-ccsn.gc.ca

By fax: 613-995-5086

In writing: Canadian Nuclear Safety Commission
P.O. Box 1046, Station B
280 Slater Street
Ottawa, Ontario K1P 5S9

15

Appendix A: Plant States Diagram

Plant states impact several aspects of NPP design, analysis and operation. Figure 2 (see the following page) shows an approximate mapping between plant states and related topics.

Following the plant states diagram, explanatory notes are provided to elaborate on the content of the figure.

Note that the diagram represents a number of complex concepts. The relationships described are not always as precise as the representation implies. The textual definitions of these concepts from the appropriate source documents should always be preferred.

Many of the transitions between states are actually broad boundaries. Often, overlaps exist between states or sharp boundaries do not apply. Even when numerical criteria are provided, the assessment of the design performance against the criteria may be subject to significant uncertainty.

Figure 2: Impact of plant design envelope and plant states

<table>
<tr><td></td><td colspan="6">Plant design envelope</td></tr>
<tr><td></td><td colspan="2">Operational states</td><td colspan="4">Accident conditions</td></tr>
<tr><td rowspan="2">Plant states</td><td rowspan="2">Normal operation</td><td rowspan="2">Anticipated operational occurrence</td><td rowspan="2">Design-basis accident</td><td colspan="2">Beyond-design-basis accidents</td></tr>
<tr><td>Design extension conditions</td><td>Practically eliminated conditions</td></tr>
<tr><td>Design rules</td><td colspan="3">Design basis</td><td>Design extension</td><td>Not considered as design extension</td></tr>
<tr><td>Core condition</td><td colspan="3">No core damage</td><td>No severe fuel degradation</td><td>Severe accidents</td></tr>
<tr><td>Classification frequency, 1/y</td><td>~1</td><td>$> 10^{-2}$</td><td>10^{-2} to 10^{-5}</td><td colspan="2">$<10^{-5}$</td></tr>
<tr><td rowspan="2">Radiological acceptance criteria</td><td colspan="5">Radiation protection regulations</td></tr>
<tr><td>ALARA</td><td>0.5 mSv</td><td>20 mSv</td><td colspan="2">No criteria</td></tr>
<tr><td>Deterministic acceptance criteria</td><td>Normal conditions of operation</td><td>Fitness for service</td><td>Integrity of physical barriers</td><td>Containment performance limits</td><td>No criteria</td></tr>
<tr><td>Probabilistic acceptance criteria</td><td colspan="2">No criteria</td><td>Reliability requirements for safety systems</td><td colspan="2">Safety Goals:
- core damage frequency
- large-release frequency
- small-release frequency</td></tr>
<tr><td rowspan="4">Systems, structures and components that play a role</td><td colspan="5">Process systems (defence in depth (DiD) level 1)</td></tr>
<tr><td colspan="5">Control systems (DiD level 2)</td></tr>
<tr><td colspan="2"></td><td colspan="3">Safety systems (DiD level 3)</td></tr>
<tr><td colspan="3"></td><td colspan="2">Complementary design features (DiD levels 4 and 5)</td></tr>
<tr><td rowspan="3">Operator procedures</td><td colspan="5">Operating manuals</td></tr>
<tr><td></td><td colspan="3">Accident management</td><td></td></tr>
<tr><td colspan="4"></td><td>Severe accident management</td></tr>
<tr><td>Confidence in preventing significant releases</td><td colspan="3">Design basis rules - high confidence</td><td>Reasonable confidence</td><td>Significant releases may occur</td></tr>
<tr><td>Offsite response</td><td colspan="3">Not required</td><td colspan="2">Graded response</td></tr>
</table>

Design rules: This describes the type of rules applied during the design process. Inside the design basis, well established codes and standards have been used for many years. This remains unchanged. For the design extension, less conservative rules are applied. Established codes and standards do not typically address this domain. Outside the plant design envelope, no specific design rules are required by REGDOC-2.5.2, *Design of Reactor Facilities: Nuclear Power Plants*. This does not mean that equipment will not function, but there may be a lower confidence in its functionality.

Core condition: The design should ensure that no core damage occurs in normal operation and AOOs. For DBAs, limited core damage (such as limited sheath failures or extensive fuel damage in a single channel) may occur. Severe core damage may occur in some DECs. Note that fuel in the spent fuel pools is not shown in Figure 2.

Classification frequency: REGDOC-2.4.1, *Deterministic Safety Analysis*, defines the expected frequency range for AOOs and DBAs, although frequency is not the only consideration in the classification of events. The CNSC does not set a lower frequency limit for DECs, as explained in Section 1.2 of the main text.

Radiological acceptance criteria: The *Radiation Protection Regulations* [17] establish the ALARA principle and set the dose limits for the public, and occupational and emergency dose limits for workers. Emergencies do not map uniquely to the plant states and are not described here. REGDOC-2.5.2 sets radiological dose acceptance criteria for AOOs and DBAs. More specifically, the dose acceptance criteria are design criteria. They apply only to committed whole-body doses that may be received by average members of the critical groups who are most at risk during the 30 days following an accident, as calculated in deterministic safety analyses.

Deterministic acceptance criteria: These criteria describe the role of the physical barriers to fission-product release. For normal operation, all barriers are expected to remain intact. For AOOs, all barriers (except those failed as the initiating event; e.g., a pipe leak) should remain intact and fit for return to normal operation. For DBAs, the barriers should remain intact to the extent practicable. For DECs, it is accepted that a severe core damage accident may occur. However, there will be reasonably high confidence that the equipment used for management of DECs will operate as intended and that containment integrity will be maintained to prevent significant radioactive releases.

Probabilistic acceptance criteria: REGDOC-2.5.2 defines the safety goals that apply to the overall design, in particular to events beyond the design basis. The three criteria used in the establishment of safety goals are: core damage frequency (CDF), small-release frequency (SRF) and large-release frequency (LRF).

Systems, structures and components that play a role: Process and control systems are designed primarily for levels 1 and 2 defence in depth and are not relied upon for DBAs. However, if functional, these systems may have a role in DECs and severe accidents. Safety systems are primarily designed to give very high confidence that DBAs do not lead to exceeding dose acceptance criteria. They may also have a role in DECs. Complementary design features are specific to DECs.

Operator procedures: Operator procedures do not map uniquely to plant states. Operating manuals, emergency operating procedures and SAMGs provide a continuity of coverage between normal operation and severe accident conditions. Switching between the types of procedures depends on measured conditions of the plant, not on an abstract definition of plant state. Note that

operating manuals may be needed even when the governing procedures are EOPs or SAMGs, since they provide directions for system operation.

Level of confidence in preventing significant releases: As described in detail in the main text, a high level of confidence is required in meeting requirements within the design basis. For DECs, reasonably high confidence is expected. For very unlikely conditions and events, it is acknowledged that significant releases may occur.

Offsite response: Offsite response should not be needed for any event within the design basis, although it is acknowledged that precautionary measures may be taken if a release is considered possible should further failures occur. For increasing severity of events, emergency measures such as sheltering, administration of potassium iodine, short-term relocation or long-term evacuation may be implemented.

Appendix B: How DECs are Defined Outside Canada

International Atomic Energy Agency

The International Atomic Energy Agency (IAEA) approach is found in IAEA SSR–2/1 [1]. It contains the following definition of DECs:[5]

> Accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions could include severe accident conditions.

Finland

The Finnish Centre for Radiation and Nuclear Safety (STUK) has issued Draft YVL B.1 *Safety Design of a Nuclear Power Plant* [2] containing the following definition:

> Design extension condition shall refer to a situation caused by a rare external event, or a situation where the initiating event of an anticipated operational occurrence or Class 1 postulated accident involves a common-cause failure in the safety systems, or a combination of failures, and which the facility is required to withstand without sustaining severe fuel damage.

STUK's definition appears to overlap that for a postulated accident which states that a:

> [p]ostulated accident shall refer to such a deviation from normal operation that can be assumed to occur less frequently than once over a span of one hundred operating years; and which the nuclear power plant is required to withstand without sustaining severe fuel damage, even if individual components of systems important to safety are rendered out of operation due to servicing or faults.

United States of America

The following proposal was made by the United States Nuclear Regulatory Commission Risk Management Task Force [3] to deal with design-enhancement categories for BDBAs:

> The NRC should establish through rulemaking a design-enhancement category of regulatory treatment for beyond-design-basis accidents. This category should use risk as a safety measure, be performance-based (including the provision for periodic updates), include consideration of costs, and be implemented on a site-specific basis.

This proposal was recently rejected by the Nuclear Regulatory Commission [4], though it may be subsumed into the U.S. NRC's Risk Management Regulatory Framework.

France and Germany

The French and German regulators do not use the term DEC. Instead, they use a similar concept: risk reduction categories (RRCs). The French and German regulators jointly prepared *Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors* [5]. These guidelines are based on common work of the French

---

[5] SSR-2/1 has been under review since the Fukushima accident. Changes are anticipated in requirements for DECs, spent fuel pools, multiple units and provisions for external events.

Institut de Protection et de Sûreté Nucléaire[6] (IPSN) and of the German Gesellschaft für Anlagen- und Reaktorsicherheit (GRS). The guidelines define RRCs, the applicable analysis rules and associated acceptance criteria.

The RRCs are divided into two classes:

- RRC-A – multiple failures that must be analyzed using deterministic methods in order to design additional measures to prevent core melt
- severe accidents – sometimes referred to as RRC-B

RRC accidents are analyzed with less conservative assumptions than those applied to DBAs. For example, all systems (except those implicated in the failure) can be assumed operational, the single-failure criterion does not have to be met and equipment is not assumed to be unavailable due to maintenance.

Japan

The Japanese Nuclear Regulation Authority is currently developing new safety standards that incorporate the lessons learned from the Fukushima Daiichi accident. Its new safety standards do not use the term DEC. Instead, in setting design requirements, the term "postulated BDBAs" is frequently used, indicating that a subset of BDBAs is considered in design. In the requirements for analysis and for severe accident management, the qualifier "postulated" is not normally used, indicating that all BDBAs are to be considered.

References to Appendix B

1. IAEA Safety Report Series SSR-2/1, *Safety of Nuclear Power Plants: Design*, 2012

2. STUK draft YVL B.1, *Safety Design of a Nuclear Power Plant*, 2011

3. U.S. NRC Risk Management Task Force, *A Proposed Risk Management Regulatory Framework*, 2012

4. U. S. NRC SECY-13-0132, *U.S. Nuclear Regulatory Commission Staff Recommendation for the Disposition of Recommendation 1 of the Near-Term Task Force Report*, ML14139A273, 2014-05-19

5. ASN, *Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors*, adopted during the GPR/German experts plenary meetings held on October 19th and 26th, 2000 (please note that this webpage downloads automatically)

[6] IPSN is now part of the Institut de Radioprotection et de Sûreté Nucléaire (IRSN)

Appendix C: Identification of DECs

The design authority is responsible for identifying, selecting and classifying events or conditions that comprise DECs. Currently, there is no recognized means for identifying DECs. An understanding of accident progression, processes and accident phenomena is relevant and examination of the following is suggested:

- major design options and specific plant design features for mitigation of SAs and their roles in achieving severe accident management (SAM) goals
- conditions needed for the design of plant features to be used in preventing and mitigating consequences of SAs
- SAM strategies for mitigating challenges posed by SAs while at the same time ensuring reliable operation of safety functions and returning the plant to a stable controlled state
- selection of representative events and accident sequences for determining actual design conditions
- appropriate deterministic accident analyses for design support

Selection of DECs may also be aided by:

- the elements found in the CNSC regulatory framework (such as REGDOC-2.5.2, *Design of Reactor Facilities: Nuclear Power Plants* and REGDOC-2.4.1, *Deterministic Safety Analysis*)
- an understanding of accident progression, processes and phenomena
- the expectation that the end goal is to practically eliminate significant releases

A proposed process for identification and selection of DECs is described in the following six steps. Note that the identification of DECs is likely to be an iterative process; the starting point is not particularly important.

1) Identify the design features considered in prevention or mitigation of a BDBA or an SA and defining their intended roles.

These features may include:

- barriers to delay or arrest the progression of the accident and migration of the corium[7]
- containment and containment systems
- shielding provisions
- other equipment or instrumentation used in SAM

As part of the overall strategy for addressing challenges and plant conditions and for restoring and maintaining safety functions, the roles of each design feature should be clearly defined. The objective is to illustrate that the planned operation of these systems can be reasonably expected to practically eliminate significant radioactive releases. This objective is essential for determining the conditions for these features which must be designed and the rationales for selecting these conditions.

2) Identifying the parameters of the design for design features considered for use in preventing or mitigating a BDBA/SA defined above.

---

[7] **Corium**: A lava-like molten mixture consisting of portions of the nuclear reactor core.

Typical design parameters may include:

- environmental conditions, such as:
  - process parameters and local conditions – pressure, temperature, humidity, chemical conditions and radiation conditions
  - local environmental conditions that could be caused by a fire, flood or earthquake
  - other environmental conditions induced by external events
- functional expectations to meet the needs of performing their intended roles during an accident; for example, for the design of passive autocatalytic recombiners (PARs) (i.e., determining the number and location of PARs units), information would be needed on hydrogen source term, rate and location of release, and distribution patterns
- access, actuation, timing, as applicable
- support resources (such as power or water) as applicable, such as:
  - makeup of water, including inventory and injection point
  - power, including loads and duration of availability

These design parameters are derived with best-estimate methodology from analysis of the representative set of accidents to be considered in plant design. This is discussed further in step 6, below.

3) Identifying factors of the accident progression (i.e., mechanistic conditions in the plant, processes and phenomena which must be addressed by the SAM program) relevant for determining limiting values and range for the timing and amplitude of the parameters needed for design.

For example, determining the number and the location of PARs requires data on hydrogen source term as well as the rate and location of the hydrogen release. These parameters are influenced by the specific accident progression pattern. The rate of hydrogen generation is primarily affected by the following conditions:

- surface area of contact between steam and metal, which depends on fuel temperature and on the timing of core collapse
- temperature of metal in contact with steam, which depends on fuel temperature and on the timing and rate of water injection
- extent, duration and location of corium-concrete interaction, which depends on movement of corium, and on corium cooling before and after initiation of corium-concrete interaction

These are some of the conditions that are not considered in the design basis, but that would apply in the design process of the plant for DECs.

4) Identifying initiating events (IE), human error (HE), and SSC operability (success, failure) which are relevant for determining limiting values/ranges of the parameters needed for design.

It is necessary to identify the combinations of individual events (IE including external events; HE and SSC successes or failures) whose occurrence during an accident will generate the limiting conditions to be used in the design process of the plant.

The combinations of events listed above should be identified based on an understanding of the influence of the combination of various individual events on the progression of accidents. Other conditions that may be relevant, such as initial plant conditions, should also be

identified here. Major uncertainties in the progression of an accident should be considered, including:

- timing of failures and timing of recovery of SSCs
- timing of operator actions
- partial successes, partial failures and partial recoveries of SSCs

5) Identify individual accident scenarios that include combinations of identified IE, HE and SSC success/failure.

These accident scenarios contain conditions (step 3) and events (step 4) needed for the design. Identification of individual accident sequences may use PSA results of event-tree analyses, if applicable. It must be recognized that PSA methodology has inherent limitations, such as lack of a time scale for human errors, failures and recoveries; lack of capability to consider partial success or partial failures; or lack of adequate human reliability models for SAM-specific decision-making processes. Care must be taken to ensure that these limitations are considered and compensated by supplementary rationales, means and sensitivity cases.

6) Optimize the set of accident scenarios to reduce it to a manageable number of sequences.

The optimized set of accident scenarios is the set that should be considered in design. The accident scenarios in this set contain conditions and events needed for the design of mitigation strategies. Deterministic analyses of these sequences will provide the numerical values for the set of the design parameters identified. These analyses will follow the requirements and guidance in REGDOC-2.4.1, *Deterministic Safety Analysis.*

Abbreviations

ALARA	as low as reasonably achievable
AOO	anticipated operational occurrence
BDBA	beyond-design-basis accident
CNSC	Canadian Nuclear Safety Commission
CSA	Canadian Standards Association
DBA	design-basis accident
DECs	design extension conditions
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit
HE	human error
IAEA	International Atomic Energy Agency
IE	initiating event
IPSN	Institut de Protection et de Sûreté Nucléaire
IRSN	Institut de Radioprotection et de Sûreté Nucléaire
NPP	nuclear power plant
NRA	Japanese Nuclear Regulation Authority
PARs	passive autocatalytic recombiners
PSA	probabilistic safety assessment
R&D	research and development
RRC	risk reduction categories
SA	severe accident
SAM	severe accident management
SAMGs	severe accident management guidelines
SSCs	structures, systems and components
STUK	Finnish Centre for Radiation and Nuclear Safety
USNRC	United States Nuclear Regulatory Commission

References

1. *Canadian Nuclear Safety Commission (CNSC), Integrated Action Plan on the Lessons Learned from the Fukushima Daiichi Nuclear Accident*, 2013

2. CNSC draft RD-337 version 2, *Design of New Nuclear Power Plants*, 2012

3. CNSC REGDOC-2.5.2, *Design of Reactor Facilities: Nuclear Power Plants*, 2014

4. CNSC REGDOC-2.3.2 *Operating Performance: Accident Management: Severe Accident Management Programs for Nuclear Reactors*, 2013

5. CNSC REGDOC-2.4.1, *Deterministic Safety Analysis*, 2014

6. International Atomic Energy Agency (IAEA) Safety Specific Guide SSG - 2, *Deterministic Safety Analysis for Nuclear Power Plants*, 2009

7. IAEA Safety Report Series SRS No. 56, *Approaches and Tools for Severe Accident Analysis for Nuclear Power Plants*, 2008

8. CNSC RD/GD-210, *Maintenance Programs for Nuclear Power Plants*, 2012

9. CNSC RD/GD-98, *Reliability Programs for Nuclear Power Plants*, 2012

10. CNSC draft REGDOC-2.3.2, *Accident Management*, 2014

11. CNSC G-225, *Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills*, 2001

12. CNSC RD-353, *Testing the Implementation of Emergency Measures*, 2008

13. CNSC draft REGDOC-2.10.1, *Nuclear Emergency Preparedness and Response*, to be issued Fall 2015

14. CNSC G-276, *Human Factors Engineering Program Plans*, 2003

15. CNSC G-278, *Human Factors Verification and Validation Plans*, 2003

16. CNSC DIS-13-01, *Proposals to Amend the Radiation Protection Regulations*, 2013

17. CNSC INFO-0824, *CNSC Fukushima Task Force Report*, 2011

18. Government of Canada, SOR/2000-203, *Radiation Protection Regulations*, 2000

19. CNSC RD-360, *Life Extension for Nuclear Power Plants*, 2008