INTERNATIONAL NUCLEAR SAFETY JOURNAL

ISSN 2285 – 8717
ISSN–L 2248 – 8717
http://www.insj.info

vol. 4 issue 3, 2015, pages 13 - 23

Design Extension Conditions Concept and its Application to Operating Reactors in Canada

Alexandre VIKTOROV[1], **Christopher HARWOOD**[1]
[1]*Canadian Nuclear Safety Commission, Ottawa, Canada*
Corresponding author: alexandre.viktorov@canada.ca

==========

Abstract

The Canadian Nuclear Safety Commission (CNSC) formally introduced the term Design Extension Conditions (DEC) with the issue of regulatory document REGDOC-2.5.2, "Design of Reactor Facilities: Nuclear Power Plants". The primary drivers for this development were the desire to maintain alignment with the equivalent International Atomic Energy Agency (IAEA) safety standard and to reflect lessons learned from the Fukushima Daiichi accident.

The Canadian regulatory document for NPP design establishes high level design requirements and expectations for new Nuclear Power Plants (NPPs), including those pertaining to DEC. Other regulatory documents provide requirements for safety analysis and accident management as well as other aspect relevant to DEC. In the short time since this concept of DEC was made part of the regulatory framework in Canada, it has become apparent that it is reflective of the international best practices and will allow further strengthening of defence in depth but also requires further elaboration, in particular with respect to application to currently operating reactors.

The currently available guidance specific to DEC is not comprehensive, in particular, regarding the interface with the plant design basis, its role in the Defence-in-Depth, selection of requirements, impact on operating limits and conditions. Nevertheless, the practices begin to emerge, given that the topic of DEC is being advanced rapidly both nationally and internationally, in particular in the framework of IAEA. CNSC and Canadian stakeholders are actively discussing how the high level requirements and expectations are to be applied, and the emerging consensus will be captured in a new Canadian standard.

This paper provides an overview of recent deliberations by CNSC staff on the subject and an outline of the challenges that we still have to address. With this in mind, this paper does not aim to provide a final established position, but rather to stimulate international discussion on the subject of DEC, in particular its application to the older nuclear facilities. The paper provides the definition of DEC as currently used in Canada, describe interfaces with the other fundamental safety concepts such as Defence-in-Depth, explain the approach for identification of DECs and the underlying principles associated with design, analysis, operational and procedural requirements.

Keywords
Design Extension Conditions, design basis,nuclear safety requirements, operating NPP

==========

1.0 Introduction

In the context of nuclear power plant design and safety assessment, the term "design basis"[1] has been in use for many years and is applied through regulatory requirements and applicable national and international codes and standards. Requirements for the design basis have been

[1] IAEA definition of design basis: The range of conditions and events taken explicitly into account in the design of a facility, according to established criteria, such that the facility can withstand them without exceeding authorized limits by the planned operation of safety systems.

well established and are typically very conservative, aiming to give a very high level of confidence that an NPP can meet safety requirements, including following any design-basis accident (DBA). The experience has shown that the events categorized as being within the "design basis" can occur but their consequences are well within the acceptable limits. This success can be attributed to the robust design and operation practices, as well as adequate system of safety requirements. However, the experience also shows that tangible risks do arise from events that are outside of the "design basis". In the last decade or so, a new approach has emerged where an expanded scope of events is considered in the plant design and operation, albeit possibly with a different set of requirements aiming at "reasonable confidence" of success rather than the high confidence achieved for DBA.

To enhance protection to accidents beyond those considered in the design basis of the plant, in particular to severe accidents, the CNSC regulatory document REGDOC-2.5.2 "Design of reactor facilities: nuclear power plants" [1] introduces requirements for equipment, systems and components with role in addressing challenges posed by accidents, more severe that those included in the design basis. Such accidents are called "Design Extension Conditions" or DEC, in the Canadian terminology. For DEC, the design is expected to provide a degree of defence in depth and include means to:

- Explicitly consider plant-specific challenges to the safety functions and physical barriers
- Provide design features which help ensure safety goals are met, including provisions facilitating accident management
- Prevent significant releases of radioactive materials into environment.

It is important to keep in mind that DEC are not a simple increase in the scope of the traditional design basis; they are a distinct category of events, in the sense that a specific set of requirements is applicable to DEC. The Design Extension Conditions form a subset of a broad category of Beyond-Design-Basis Accidents (BDBA)[2].

Figure 1 describes the plant design envelope and plant states, showing the relationship of DEC to other plant states.

2.0 Definition of Design Extension Conditions

The Canadian REGDOC-2.5.2 requires the design authority to consider mitigation of a broad range of accidents while still at the design stage. For this purpose, design features should be provided such that they will accomplish their function during an accident with an appropriate degree of confidence. In addition, the design authority is required to provide the initial accident response guidance (such as abnormal incident manuals, emergency operating procedures, emergency mitigating equipment guidelines or severe accident management guidelines, etc.), taking into account the plant design features and the understanding of accident progression and associated phenomena.

The Plant Design Envelope (PDE) concept is introduced in section 7.2 of REGDOC-2.5.2 to represent „*The 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*."

[2] According to the IAEA glossary: Beyond design basis accident: Accident conditions more severe than a design basis accident.

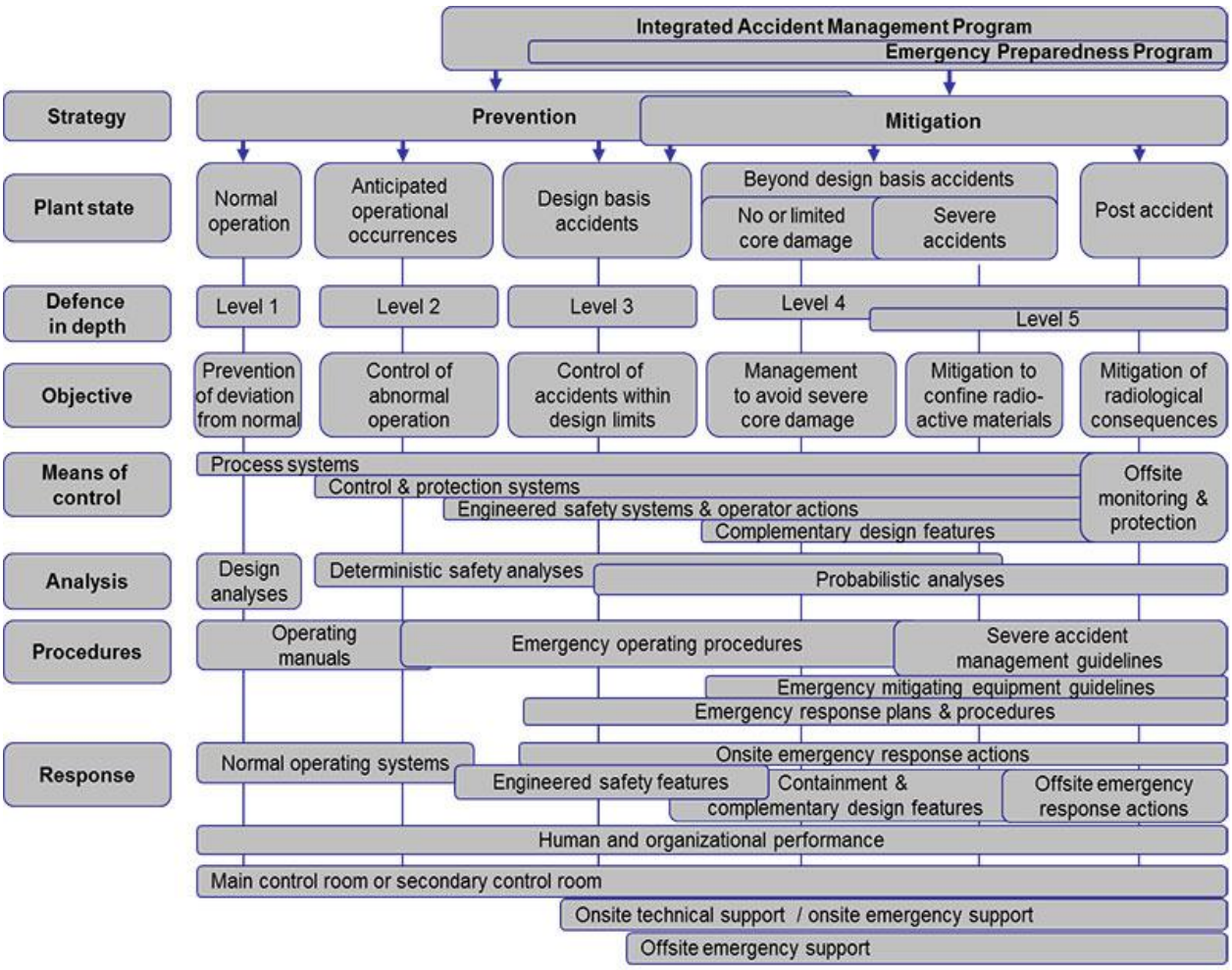

Fig. 1: Design Extension Conditions place in the Plant States

As specified in the definition of the PDE, the objective is that significant releases are practically eliminated for DEC. Recognizing that in the case of a severe accident a significant release cannot be avoided unless containment integrity is maintained and uncontrolled releases including unfiltered venting are precluded, design requirements for the containment system are explicitly set forth in REGDOC-2.5.2.

The concept of DEC has been introduced by CNSC as part of the Plant Design Envelope with the purpose of defining those conditions which should be considered in plant design, in addition to the Design Basis conditions, with the purpose of further strengthening the plant safety.

The following definition is adopted in REGDOC-2.5.2 for Design Extension Conditions: „*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 definition is based on that from IAEA SSR-2/1, "Safety of Nuclear Power Plants: Design", [2] but has been slightly modified to clarify that DEC is a subset of BDBA; it does not include DBAs that can be considered to be "practically eliminated". As used in REGDOC-2.5.2, DEC is a complex concept, which relates to plant states, conditions, and diverse events including external events, those involving the reactor, and/or the handling of the irradiated fuel.

3.0 Fundamental principles applied to consideration of DEC

The Canadian standard CSA N290.16 [3] includes the following principles, originally developed by the Canadian industry, to be followed when incorporating the concept of DEC into the design, analysis and operation practices:

- Focus on stopping accident progression prior to a severe accident
- Provide multiple barriers to accident progression and multiple means to supply necessary water or electricity to ensure adequate defence-in-depth
- Give primary and early priority on methods and actions to initiate reactor cool-down and maintain fuel cooling
- Maintain containment integrity to minimize radioactive releases
- Control containment venting through a filtered system
- Confirm that necessary SSCs (systems, structures and components) will survive rare yet credible conditions arising from internal and external hazards
- Maintain wet storage bay water levels sufficient to mitigate high radiation fields, hydrogen production, and fuel damage
- Provide emergency mitigating equipment, which is robust, readily available, easily deployable within required timeframes, and has adequate redundancy.

4.0 Identification of DEC

In the Canadian approach, frequency ranges for AOO (Anticipated Operational Occurrences) and DBA are given in REGDOC-2.4.1, "Deterministic Safety Analysis", [4]. However, CNSC has not defined a lower frequency boundary for DEC. Obtaining credible frequency values for low frequency events, which may include multiple failures of equipment and human errors, is difficult due to the large inherent ambiguities. The approach for identifying events to be considered as DEC inevitably involves a measure of judgement and is characterized by notable uncertainties. For these reasons, the regulator does not impose any lower frequency limit for DEC; however, the designer may select sensible values to the convenience of decision making during the design development.

Identification and classification of events to be considered in design is the responsibility of the design authority. The set of DEC is specific to the reactor technology and to particular design options. From the perspective of external events, selection of DEC is also site-dependent, and must account for the natural and human-induced hazards. For these reasons, and at least until more experience is accumulated with consideration of DEC it is viewed that the DEC must be selected by the designer or the applicant for a licence, and not imposed by the regulator.

Identification of DEC can be seen as a two-step process:

- Firstly, the probabilistic safety assessment would help identifying dominant contributors to the overall core damage frequency and large release frequency, as well as event that come close to challenging the core and containment integrity.
- Secondly, regardless of the specific scenario, the designer should consider the known physical phenomena, which could challenge the fundamental safety functions.

5.0 Requirements for DEC

There are markedly less specific requirements for design extension conditions than for design basis. In the development of DEC requirements, the fundamental principles described in

Section 3.0 above serve as a starting point for developing requirements and appropriate acceptance criteria.

The underlying philosophy governing requirements related to DEC is "reasonable confidence", unlike the "very high confidence" applied to the design basis. This is risk informed, recognizing that BDBA and severe accidents have a very low likelihood of occurring and are characterized by large uncertainties. The formal definition of the concept is provided below.

Reasonable confidence: „*Reasonable confidence is a higher than average expectation that the action will achieve at least the minimum functionality required for success. Reasonable confidence can be shown through evaluation of conditions under which the action is to take place and assessing the likelihood of the system or personnel to successfully perform the action while applying a best estimate approach. Where the available knowledge is not sufficient to characterize the "best estimate" conditions then a certain degree of conservatism is still expected."*

5.1 Design Requirements

The Canadian regulatory document REGDOC-2.5.2 sets design requirements only for events within the plant design envelope (including both the design-basis conditions and design extension conditions), i.e. there are no design requirements for BDBAs of very low frequency. It is important to recognise that certain BDBAs may always be considered as "practically eliminated" conditions due to the extremely low likelihood of their occurrence.

Design requirements are established for equipment that may be used in DEC. This equipment may include:

- complementary design features[3]. Examples of complementary design features are core catcher and containment filtered venting system dedicated to severe accidents;
- safety or process SSCs that may be envisaged to be used beyond their design basis;
- fixed or portable equipment onsite or offsite that do not form part of the plant itself, such as mobile pumps, or electric power generators;
- connection points, that become part of the permanently installed equipment.

The design requirements for safety systems will be the most restrictive of those needed to provide high confidence in DBA or reasonable confidence in DEC.

REGDOC-2.5.2 requires that "*equipment and instrumentation credited to operate during DECs shall be demonstrated, with reasonable confidence, to be capable of performing their intended safety function 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, or other considerations.*"

A demonstration of equipment and instrumentation operability should include the following:

1. the functions credited in the accident timeframes that need to be performed to achieve a safe shutdown state for DECs
2. the accident timeframes for each function

[3] **complementary design feature**: A design feature added to the design as a stand-alone structure, system or component (SSC) or added capability to an existing SSC to cope with design extension conditions.

3. the equipment type and location used to perform necessary functions in each timeframe
4. the bounding harsh environment of DECs within each timeframe
5. a reasonable assurance that the equipment will survive to perform its function in the accident timeframes, in the DEC environment

5.2 Analysis Requirements

The Canadian regulatory document REGDOC-2.4.1, "Deterministic Safety Analysis", specifies high-level requirements for deterministic safety analysis for AOO, DBA, and BDBA. REGDOC-2.4.1 does not include the term DEC and still retains reference to BDBA which is appropriate as the analysis, unlike the design process, might consider events of vanishingly small likelihood. Section of 4.3.3 of REGDOC-2.4.1 states that:

"*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.

2. The accident management program and design provisions put in place to handle the accident management needs are effective, taking into account the long-term availability of cooling water, material and power supplies."

Clearly, deterministic BDBA analysis is required not only to support the evaluation of safety goals in conjunction with probabilistic safety assessment (PSA), but also to demonstrate the adequacy of the accident management and design provisions. Therefore, deterministic safety analysis is to be performed to demonstrate that the complementary design features are capable of coping with DECs.

The general rule for DEC analysis is the acceptability of a best-estimate approach, which is consistent with IAEA documents such as SSG-2, "Deterministic Safety Analysis for Nuclear Power Plants", [5] and SRS No. 56 "Approaches and Tools for Severe Accident Analysis for Nuclear Power Plants", [6]. REGDOC-2.4.1 states that, "*For the analysis of BDBA, it is acceptable to use a more realistic analysis methodology consisting of assumptions which reflect the likely plant configuration, and the expected response of plant systems and operators in the analysed accident.*" Nevertheless, in situations of large, poorly quantified uncertainties, it would be prudent to apply a degree of conservatism in the analysis assumptions.

Deterministic analysis should be performed at least for events leading to the highest challenges for all relevant hazards (e.g., the largest hydrogen source term, highest pressure, largest water level inside containment, etc.) to ensure that the accident management and design features are available to cope with the DEC. Using hydrogen as an example of a challenge, the hydrogen mitigation measures (e.g., PARs – passive autocatalytic recombiners and/or igniters) should be demonstrated to function to maintain integrity of the containment even due to most challenging hydrogen releases into containment expected under those conditions.

Analysis of DECs may use applicable[4] input from PSAs and may credit all the available SSCs as long as they have been demonstrated with reasonable confidence to perform their intended function in DECs. It is worth noting that the single failure criterion, which applies to all safety groups credited in the DBA analysis, does not have to apply in DEC analysis.

[4] 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.

Should safety analysis of an accident considered to be part of DEC indicate significant challenges to the fundamental safety functions then appropriate measures are expected to be taken, to reduce such challenges to acceptable levels.

5.3 Operational and Procedural Requirements

While the complementary design features offer additional design capabilities to maintain and strengthen the existing multiple physical barriers to fission product release, adequate procedural barriers should be also in place to cope with DEC.

Operational requirements relevant to DEC include those pertinent to accident management and emergency response. The accident management guidelines are symptom-oriented and they do not depend directly on any pre-defined events. These procedures and guidelines follow the principle of "reasonable confidence" in their design, verification and implementation.

REGDOC-2.3.2, "Accident Management", [9], which has been recently published, fulfils action A.9.2 of the "CNSC Integrated Action Plan on the Lessons Learned from the Fukushima Daiichi Nuclear Accident", [10] regarding the development of a dedicated regulatory document on accident management. Accident management is an important element of a commitment to the defence-in-depth approach. According to this document, an accident management program consists of an integrated set of plans, procedures, guidelines, and arrangements designed to be used for accident management. The key requirements address such aspects 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 are documented in CSA Standard N1600 "General Requirements for Nuclear Emergency Management Programs", [11] and REGDOC-2.10.1, "Emergency preparedness programs", [12] which follow through on the CNSC Fukushima Task Force and External Advisory Committee recommendation to strengthen licensees' emergency preparedness programs. These documents define the requirements and guidance for an Emergency Preparedness Program. The EP Program is based on four components: Planning Basis; Program Management; Response Plan and Procedures; and Preparedness. These components are considered in the development of emergency response plans and procedures to maintain an adequate level of readiness to respond to any emergency and prevent or mitigate the effects of accidental releases from a Class I nuclear facility or a uranium mine or mill.

Several other CNSC regulatory documents and CSA standards, which were developed prior to the formalization of the DEC concept in REGDOC-2.5.2, deal with safety areas that will likely require adjustment to incorporate consideration of DEC. One can mention the following:

- RD/GD-210, "Maintenance Programs for Nuclear Power Plants", [7]
- RD/GD-98, "Reliability Programs for Nuclear Power Plants", [8]
- G-278, "Human Factors Verification and Validation Plans", [13] and G-276, "Human Factors Engineering Program Plans", [14] which provide guidance for Human Factors aspects

Of particular interest is the question whether the design extension conditions and challenges associated with those should be considered in setting the operational limits and conditions. In the Canadian regulatory framework, CSA Standard N290.15 sets requirements for the safe

operating envelope for NPPs and the discussion is ongoing to what extent, if at all, DECs should play a role in setting limits on the normal operating equipment.

5.4 Radiation Protection Requirements

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

DEC would also be subject to the regulatory requirements for radiation protection. Recently CNSC has issued a discussion paper, "Proposals to Amend the Radiation Protection Regulations" [15] on proposed amendments to Sections 15, 16 and 17 of the Radiation Protection Regulations [16]. These proposed amendments will address action A.8.1.1 of the "CNSC Integrated Action Plan On the Lessons Learned From the Fukushima Daiichi Nuclear Accident", which identified that the Radiation Protection Regulations should be amended to be more consistent with current international guidance and to describe in greater detail the regulatory requirements needed to address radiological hazards during the various phases of an emergency. These regulatory amendments may influence DEC operational, design and analysis requirements.

6.0 Applicability to NPPs in Canada

6.1 New NPPs

For new designs, REGDOC-2.5.2 and other regulatory documents apply fully. In considering DEC, the design authority must use a systematic approach to:

- address all known accident challenges to safety functions arising during DEC
- have a design which ensures balance between severe accident prevention and accident mitigation with particular emphasis on prevention of failures of the final barrier, i.e., the containment
- consider the needs of the plant-specific accident management to ensure the appropriate design and procedural provisions are in place for management of accidents.

6.2 Existing NPPs

For existing NPPs, REGDOC-2.5.2 is not meant to be applied directly as it is not feasible to satisfy at least some of the design requirements for facilities that have already been constructed.

On the other hand, it is the older plants that could benefit the most from the recent advancements in the science and technology of safety. Given the expectation of important safety gains, there is also an expectation of a corresponding effort to back-fit some of the novel concepts to existing facilities.

Application of new design, analysis and operational DEC requirements to existing NPP is consistent with the Canadian practices concerning the application of recently formalized requirements to plants built and licenced in conformance with earlier standards. New requirements are introduced in a risk-informed way as part of re-licensing of the operating facilities and, most notable during Periodic Safety Reviews for refurbishment or extended operation.
For existing NPPs, the focus is on:

- identifying and evaluating existing design features that can be used to respond to challenges posed by DEC,

- addressing any potential challenges to the containment system,
- implementing design upgrades where necessary to meet safety goals or accident management needs, or to counter specific challenges,
- assuring provisions, both design, procedural and human, for execution of accident management.

When applying the concept of Plant Design Envelope (that is, the Design Basis conditions combined with Design Extension conditions) to the currently operating plants designed to earlier standards, several different outcomes are possible regarding the re-categorization of events (i.e., transient and accidents):

(a) Events previously not considered in the Design Basis (and thus not considered at all) may now be recognized as DEC. A current example includes station transients triggered by external events exceeding (to a certain likelihood, beyond which the event may be considered practically eliminated) the design basis levels.

(b) An event previously considered as part of design basis, could be considered as DEC with the new approach, based on the demonstrably low likelihood of the event. Examples:

(i) Large Break Loss of Coolant Accident with the Loss of Emergency Core Cooling (LBLOCA + LOECC). This event was previously considered as a dual failure or Class 5 accident, and nowadays is viewed as a Beyond Design Basis Accident.

(ii) Loss of Coolant Accidents with the break size above a certain size. Based on experimental evidence and theoretical understanding of phenomena, certain LOCA could be now considered part of Design Basis, while the largest breaks could be categorized as DEC.

The key driver for re-classification of an event, previously considered part of design basis, as DEC is the burden on operation which is deemed to be out of proportion with the risk posed by such an event.

For the regulator to accept such re-classification, several questions need to be answered:

- Is it possible to adequately support claim of low likelihood of an event, such that its predicted frequency falls below the DBA range?
- If an event is re-classified, what would be the acceptance criteria?
- Are there any implications for the operating limits and conditions?
- Will there be any impacts on the existing design, maintenance and testing requirements?
- How will compliance activities change?

It is noted that many upgrades have been made, or are under consideration at existing Canadian NPPs, for example, as a result of Integrated Safety Reviews or following the Fukushima Daiichi accident. Many of these changes address DEC. Design requirements for these upgrades have been selected by licensees and reviewed by the regulator, using the current standards and codes, best engineering judgement, and invoking risk-informed and cost-benefit considerations. As part of implementation of these upgrades, specific issues requiring regulatory guidance are being identified and addressed. Implementation of safety enhancements to address DECs should not compromise robustness of the existing plant design basis.

7.0 R&D in support of DEC

Many physical phenomena associated with severe accidents are extremely complex; and for some of those, the current level of knowledge and modeling capabilities is limited. Quite frequently, the experimental studies cannot be conducted in the fully representative conditions, a fact that additionally complicates the task of development of models and their validation. The research activities in this area aim to reduce the uncertainties in available knowledge, thus allowing more accurate modeling of the accident progression and consequences.

The research aims to address needs of the currently operating reactors as well as future reactors. However, for existing plants, severe accidents were not a design consideration. The extent of design modifications of the operating reactors are often limited and consequently the research in this area is primarily aimed at better understanding of the capabilities of the plant systems to cope with challenges posed by severe accidents. One of the key aspects to be addressed through the R&D effort is the study of cliff-edge effects that may lead to non-linear and unexpected response of the existing plant systems, structures and components.

The high cost of experiments and limited number of suitable facilities to perform studies of relevant phenomena necessitates wide international cooperation in this area of nuclear safety research. While driven by considerations of efficiency, this approach is also facilitated by the fact that many severe accident phenomena are common or similar in various reactor types.

8.0 Conclusion

Design Extension Conditions and the guiding principles as emerging in Canada have been described. We have outlined the relationship to other plant states and explained that DEC is a subset, and not a substitute, of BDBA. We stress that DEC does not represent an extension of the conservative design basis.

We note that detailed requirements and guidelines that apply to equipment, analysis and procedures for DEC are not yet fully developed or tested in practice. However, the principle of "reasonable confidence" should be applied to most DEC activities to make safety improvements feasible. An ongoing dialogue between regulators, designers, operators and standards organizations will be necessary to define how this reasonable confidence is to be achieved.

9.0 References

1. CNSC Regulatory Document "Design of new nuclear power plants", REGDOC-2.5.2, 2014
2. IAEA Safety Standard "Safety of nuclear power plants: design", SSR-2/1, 2012
3. CSA Standard N290.16 "Requirements for beyond design basis accidents", draft
4. CNSC Regulatory Document "Deterministic safety analysis", REGDOC-2.4.1, 2014
5. IAEA Specific Safety Guide "Deterministic safety analysis for nuclear power plants", SSG-2, 2009
6. IAEA Safety Report Series, "Approaches and tools for severe accident analysis for nuclear power plants", SRS No. 56, 2008
7. CNSC Regulatory Document, "Maintenance programs for nuclear power plants", RD/GD-210, 2012

8. CNSC Regulatory Document, "Reliability programs for nuclear power plants", RD/GD-98, 2012
9. CNSC Regulatory Document, "Accident management", REGDOC-2.3.2, 2014
10. CNSC publication, "CNSC Integrated Action Plan On the Lessons Learned From the Fukushima Daiichi Nuclear Accident", 2013
11. CSA Standard N1600 "General Requirements for Nuclear Emergency Management Programs", 2014
12. CNSC Regulatory Document, "Emergency preparedness programs", REGDOC-2.10.1, 2014
13. CNSC Regulatory Document, "Human factors verification and validation plans", G-278, 2003
14. CNSC Regulatory Document, "Human factors engineering program plans", G-276, 2003
15. CNSC Discussion Paper, "Proposals to Amend the Radiation Protection Regulations". DIS-13-01, 2013
16. Government of Canada, "Radiation protection regulations", SOR/2000-203, 2000