Design Extension Conditions

A. Bujor, C. Harwood, Q. Lei, A. Viktorov
Canadian Nuclear Safety Commission (CNSC), Ottawa, Ontario, Canada
(christopher.harwood@cnsc-ccsn.gc.ca)

Abstract

The CNSC has introduced the term Design Extension Conditions (DEC) in regulatory document RD-337 version 2, "Design of New Nuclear Power Plants" which was issued for public consultation in July 2012. The primary drivers for this change compared with the earlier version of RD-337 are to maintain alignment with the equivalent International Atomic Energy Agency (IAEA) safety standard and to introduce changes resulting from lessons learned from the Fukushima Daiichi accident.

RD-337 version 2 and the accompanying guidance document GD-337 establish 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. Nevertheless, the currently available guidance specific to DEC is not comprehensive, while the practices just begin to emerge. CNSC and industry stakeholders are actively discussing how the high level requirements and expectations will be applied in various fields. This paper is a summary of a CNSC discussion paper that is being developed to encourage substantive stakeholder discussions. The topic of DEC is being advanced rapidly both nationally and internationally. With this in mind, this paper does not intend to provide a final established position, but rather to stimulate discussion on the subject of DEC.

This paper provides the definition of DEC, gives background information relating to the adoption of the term, describes the identification of DECs and the underlying principles associated with design, analysis, operational and procedural requirements.

As described in this paper, DEC and associated requirements apply to new NPPs. Applicability to existing NPPs is also discussed.

1. Introduction

In the context of nuclear power plant design and safety assessment, the term "design basis" 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 are typically very conservative and give a very high level of confidence that an NPP can meet safety requirements following any Design Basis Accident (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 RD-337 [1] introduces requirements for equipment, systems and components with role in management of these accidents. The design is expected to provide means to:

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

The definition of DEC is discussed in Section 2 below, and a process for selection of DEC is presented in Section 3. Figure 1 describes the plant design envelope and plant states, showing the relationship of DEC to other plant states.

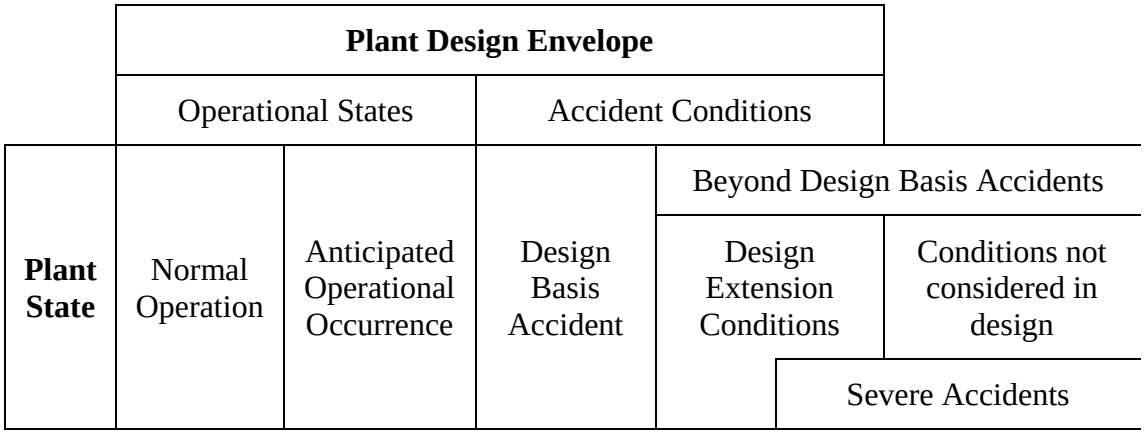

Figure 1: Plant Design Envelope and Plant States

It is important to keep in mind that DEC are not an extension of the design basis described above; they are a distinct subset of Beyond Design Basis Accidents (BDBA) that was referred to in RD-337 version 1 as "credible BDBAs".

Frequency ranges for Anticipated Operational Occurrences (AOO) and DBA are given in RD-310. CNSC does not intend to define a lower frequency boundary for DEC. Obtaining credible frequencies for low frequency events is difficult. The approach for identifying a set of BDBA to be treated as DEC inevitably involves a measure of judgement and may be subject to large uncertainties. In the past, major accidents in the nuclear industry have been complex, with many contributing factors, many of which are hard to quantify. For these reasons, no lower numerical frequency limit is being proposed for DEC.

The underlying philosophy governing regulatory requirements related to DEC is "reasonable confidence", unlike the "high confidence" applied to the design basis. This is consistent with international practice and is risk-informed, recognizing that BDBA and severe accidents have a very low likelihood of occurring. Until very recently there has

been little or no regulatory guidance on how "reasonable confidence" is to be achieved, however some directing lines on this aspect are presented for discussion in Section 4 of this paper. Specific regulatory expectations are also discussed in Section 4.

2. Definition of Design Extension Conditions

In addition to meeting probabilistic Safety Goals, RD-337 requires the design authority to consider mitigation of a broad range of accidents at the design stage. For this purpose, design features should be provided and designed such that they will operate as expected during a severe accident with a reasonable degree of confidence. In addition, the design authority is required to establish at the design stage, initial severe accident management guidelines, taking into account the plant design features and the understanding of accident progression and associated phenomena.

The Plant Design Envelope (PDE) concept is therefore introduced in section 7.2 of RD-337 version 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.*"

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 set forth in RD-337.

Considering the potential large uncertainties in quantifying failure probabilities during severe accidents (such as for failure rates for components operating beyond their level of qualification, or for human error probabilities), an appropriate level of confidence can be also justified by substantial defence in depth involving multiple layers of protection, application of the safety principles of independence, diversity, separation, full effectiveness, use of passive safety features, and use of multiple independent controls.

The concept of DEC was introduced as part of the PDE with the purpose of defining those conditions which should be considered in plant design with the purpose of further strengthening the plant defence in depth. The following definition is taken from Draft RD-337 version 2[1].

> **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

[1] Note that this definition is not the one used in the draft published for public comment; it was revised following comments received.

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. As used in RD-337, DEC is a complex concept, which encompasses a plant state, conditions, and events including external events, including those involving the reactor or the handling and storage of the irradiated fuel.

2.1 Fundamental concepts related to definition of DEC

Reasonable confidence – achieved through demonstration that the applicable requirements are met while applying a best estimate approach in defining the accident conditions. Certain degree of conservatism is still expected to address challenges for which the available knowledge is not sufficient to characterize the "best estimate" conditions.

Practically eliminated conditions – "practical elimination" refers to the implementation of specific design measures to either render such conditions physically impossible or reduce the possibility of such conditions to an extremely low level. To achieve practical elimination, each type of accident sequence that could lead to such conditions is examined and addressed. Demonstration of practical elimination of an accident sequence may involve deterministic and/or probabilistic considerations, and must take into account uncertainties due to the limited knowledge of important physical phenomena.

3. Identification of DEC

Identification and classification of events to be considered in design is the responsibility of the design authority as described in section 5.2 of RD-310, "Safety Analysis for Nuclear Power Plants", [3]. Development of a systematic process to identify the DEC considers the relations between design features, objectives, goals and strategies of severe accident management, and design-support deterministic analyses. The selection process is based on:

- understanding of severe accidents progression and associated phenomena
- identification of plant damage states, mechanistic conditions, processes, phenomena and challenges which must be addressed
- identification of the needs for success of:
  - recovery and long term reliable performance of safety functions
  - protect integrity of barriers
  - achieve controlled stable state
- identification of specific design features (such as complementary design features, containment systems, shielding provisions, instrumentation) and their roles for mitigation of severe accidents

An acceptable selection process for DECs is described below:

1. Identify all the design features considered to be used in mitigation of BDBA/severe accident and define their intended roles.
2. For each design feature considered to be used in mitigation of BDBA/severe accident and consistent with its intended role, identify the parameters needed for design. This may include: functional expectations, environmental conditions, actuation needs, support resources.
3. Identify those factors of the accident progression (i.e. mechanistic conditions in the plant, processes and phenomena which must be addressed by the accident management program) which are relevant for determining limiting values/range for the timing and amplitude of the parameters needed for design.
4. Identify those initiating events, human error, and operability (success, failure) of structures, systems and components (SSC), which are relevant for the factors determining limiting values/ranges of the parameters needed for design. In this step, the major uncertainties in the progression of an accident should be considered. Such uncertainties are:
    a) timing of failures and timing of recovery of SSC
    b) timing of operator actions
    c) partial success, partial failures, and partial recoveries of SSC
5. Identify individual accident scenarios which include combinations of such initiating events, human error and SSC success/failure.
6. Optimize this set of accident scenarios to reduce it to a manageable number of sequences. The optimized set of accident scenarios is the representative set of accidents which should be considered in design. These representative accident scenarios can be specific for different design features (systems, components). Deterministic analyses of these sequences will provide the numerical values for the set of the design parameters identified in step 2.

The vendor/applicant is expected to explicitly consider DEC in the design of the plant, such that it can be reasonably expected that significant radioactive releases would be practically eliminated by the planned operation of process and control systems**, s**afety systems, safety support systems and complementary design features. The final 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. Therefore, the DEC should be selected by the designer, and not imposed by the regulator.

4. Requirements for DEC

The high level safety objectives that apply in the DEC plant state are to prevent severe core damage, mitigate accident consequences and maintain containment integrity as long as possible.

The applicable acceptance criteria for DEC are related to:

- requirements to include in the plant design features to be used for accident management
- requirements for containment performance during DEC (such as maintaining the leak tight barrier for a certain duration, and no uncontrolled release thereafter)
- accident management needs and requirements

The underlying principle is to provide "reasonable confidence" that these design features will operate as intended during a DEC.

4.1 Design Requirements

RD-337 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 would always exist that may be considered as "practically eliminated" conditions due to the extremely low likelihood of their occurrence.

4.1.1 Scope

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

- complementary design features[2]. Examples of complementary design features are core catcher and containment filtered venting system dedicated to severe accidents
- fixed or portable equipment onsite or offsite that do not form part of the plant itself, such as mobile pumps, or electric power generators
- safety or process SSCs that may be planned to be used beyond their design basis

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.

4.1.2 Safety Classification

Safety classification considers:

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

These requirements allow the design authority to take into consideration factors such as redundancy of equipment and the possibility of implementing alternative strategies, for

[2] **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.

example, there may be adequate time to replace a portable generator should it fail during operation.

4.1.3 Survivability of Equipment

RD-337 version 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. 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

4.2 Analysis Requirements

RD-310, *Safety Analysis for Nuclear Power Plants,* specifies high level requirements for deterministic safety analysis for AOO, DBA, and BDBA. RD-310 does not include the term DEC and still retains reference to BDBA which is appropriate as the analysis, unlike design process, might consider events of vanishingly small likelihood. Section of 5.3.3 of RD-310 states that:

> "*Analysis for BDBAs shall be performed as part of the safety assessment to demonstrate that:*
> 1. *The nuclear power plant as designed can meet the established safety goals; and*
> 2. *The accident management program and design provisions, put in place to handle the accident management needs, are effective.*"

Clearly, deterministic BDBA analysis is required not only to support the evaluation of safety goals in conjunction with probabilistic safety assessment (PSA), but to demonstrate the adequacy of the accident management program and design provisions. Therefore, deterministic safety analysis is 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", [4] and SRS No. 56 "Approaches and Tools for Severe Accident Analysis for Nuclear Power Plants", [5]. Section 5.4.4 of RD-310 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.*"

One of the reasons for using best-estimate methods and computer codes in DEC analysis is related to accident management. As the accident progresses to the conditions beyond the design basis, accident management actions become an important part of defence in depth. Determination of DEC and the associated challenges to the fission product barriers are less certain than that for design basis events because DEC-induced SSC degradation is more severe and the degradation mechanism is more complex. It would be challenging or even impractical to bound the DEC consequences using a highly conservative approach in the same way as the analysis for DBA. More importantly, it is desired that the consequences of DEC are best estimated so that the analysis results reflect a realistic plant response and provide best-estimated accident conditions for accident management.

Deterministic analysis should be performed for an event leading to the highest challenge (e.g., the largest hydrogen source term) to ensure that the complementary design features are capable of coping with the DEC. In this case, the hydrogen mitigation measures (e.g., PAR and/or igniters) should be demonstrated to function under DEC to prevent the potential challenge to the integrity of the containment due to most challenging hydrogen burn modes.

Analysis of DECs may use applicable[3] input from PSAs and may credit all the available SSCs as long as they have been demonstrated with reasonably high confidence to be able 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.

4.3 Operational Requirements

RD/GD-210, "Maintenance Programs for Nuclear Power Plants", [6] covers maintenance, testing and inspection requirements. RD/GD-98, "Reliability Programs for Nuclear Power Plants", [7] gives requirements and guidance on reliability programs. Applicability of these regulatory requirements to DEC features should be based on their safety classification. These documents could be expanded to include equipment that may be used in DEC.

[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.

4.4 Procedural Requirements

While the complementary design features offer necessary design provisions 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.

Procedural 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.

RD/GD-306, "Accident Management Programs for Nuclear Reactors", [8], which is currently under development, will fulfil CNSC Fukushima Task Force recommendations on 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 RD/GD-306, 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 include G-225, "Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills", [9] and RD-353, "Testing the Implementation of Emergency Measures", [10].

RD/GD-225, "Emergency Preparedness Programs", [11], is currently under development and will supersede G-225 and RD-353. It will fulfil CNSC Fukushima Task Force and the External Advisory Committee recommendation to strengthen licensees' emergency preparedness programs. RD/GD-225 lists and discusses 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.

Guidance for Human Factors aspects are provided in G-278, "Human Factors Verification and Validation Plans", [12] and G-276, "Human Factors Engineering Program Plans", [13]. These documents may need revision to ensure that the principle of "reasonable confidence" is applied consistently for events beyond the design basis.

4.5 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.

An emergency does not correlate with any particular plant state; however, by definition, DEC would also be subject to the regulatory requirements for emergencies. It is important to note that the CNSC is issuing a discussion paper on proposed amendments to Sections 15, 16 and 17 of the *Radiation Protection Regulations*, [14]. These proposed amendments will address recommendation 8 of INFO-0824, *CNSC Fukushima Task Force Report*, [15], 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 impact DEC design and analysis requirements in the consideration of achieving general nuclear safety objectives.

5. Applicability to NPPs in Canada

5.1 New NPPs

For new designs, RD-337 applies fully. In considering DEC, the design authority must use a systematic approach to:

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

5.2 Existing NPPs

For existing NPPs, RD-337 does not apply directly. Application will be consistent with overall applicability of RD-337 to existing plant, e.g. via application of RD-360, "Life Extension for Nuclear Power Plants", [16], in an integrated safety review for refurbishment or extended operation. For existing NPPs, the focus is on:

- identifying and evaluating the existing design features that can be used to respond to challenges posed by DEC
- 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, or are under consideration at existing NPPs, as a result of safety reviews performed at the time of refurbishment 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 best engineering judgement, based on risk informed considerations. As part of implementation of these upgrades, specific issues requiring regulatory guidance are being identified and addressed.

6. 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 more accurate modeling of the accident progression and consequences.

The research should address needs of the currently operating reactors as well as future reactors. However, for existing plants, severe accidents were not a design consideration. Consequently, modifications of the operating reactors are often limited and the research in this area is primarily aimed at minimizing the potential impact of 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.

7. Conclusion

Design Extension conditions have been described. We have outlined the relationship to other plant states and 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. However, the principle of “reasonable confidence” should be applied to all activities. An ongoing dialogue between regulators, designers, operators and standards organizations will be necessary to define how this reasonable confidence is to be achieved.

8. References

1. CNSC Regulatory Document Draft RD-337 Version 2, "Design of New Nuclear Power Plants", issued for public comment 2012.
2. IAEA Safety Standard SSR-2/1, "Safety of Nuclear Power Plants: Design", 2012.
3. CNSC Regulatory Document RD-310, "Safety Analysis for Nuclear Power Plants", 2008.
4. IAEA Specific Safety Guide SSG-2, "Deterministic Safety Analysis for Nuclear Power Plants", 2009.
5. IAEA Safety Report Series SRS No. 56 "Approaches and Tools for Severe Accident Analysis for Nuclear Power Plants", 2008.
6. CNSC Regulatory Document RD/GD-210, "Maintenance Programs for Nuclear Power Plants", 2012.
7. CNSC Regulatory Document RD/GD-98, "Reliability Programs for Nuclear Power Plants", 2012.
8. CNSC Regulatory Document RD/GD-306, "Accident Management Programs for Nuclear Reactors", under development.
9. CNSC Regulatory Document G-225, "Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills", 2001.
10. CNSC Regulatory Document RD-353, "Testing the Implementation of Emergency Measures", 2008.
11. CNSC Regulatory Document RD/GD-225, "Emergency Preparedness Programs", to be issued.
12. CNSC Regulatory Document G-278, "Human Factors Verification and Validation Plans", 2003.
13. CNSC Regulatory Document G-276, "Human Factors Engineering Program Plans", 2003.
14. Government of Canada, SOR/2000-203, "Radiation Protection Regulations", 2000.
15. CNSC Information Document INFO-0824, *CNSC Fukushima Task Force Report*, 2011
16. CNSC Regulatory Document RD-360, "Life Extension for Nuclear Power Plants", 2008.