

ASSESSMENT OF EXTERNAL HAZARDS FOR DESIGN

José G. Sánchez Cabañero

jgsc@consultant.com

CONTENT

- 1.** Regulation and Safety Assessment Scope.
- 2.** General Requirements for Safety Assessment.
- 3.** Specific Requirements for Safety Assessment.
 - 3.1.** Specific for the Site,
 - 3.2.** Design Basis for External Events (DBEEs),
 - 3.3.** Protection Against DBEEs,
 - 3.4.** Design Extension Conditions (DEC),
 - 3.5.** Other Requirements for Design.
- 4.** Guidance for Plant Protection.


1 | REGULATION AND SAFETY ASSESSMENT SCOPE

REGULATION OF FIRST ORDER (1 of 2)


IAEA Safety Standards
for protecting people and the environment

Fundamental Safety Principles

Jointly sponsored by
Euratom FAO IAEA ILO IMO OECD/NEA PAHO UNEP WHO



Safety Fundamentals
No. SF-1


 **IAEA**
International Atomic Energy Agency

Nov. 2006

IAEA Safety Standards
for protecting people and the environment

Safety Assessment for Facilities and Activities

General Safety Requirements
No. GSR Part 4 (Rev. 1)

 **IAEA**
International Atomic Energy Agency

May 2009

IAEA Safety Standards
for protecting people and the environment

Safety of Nuclear Power Plants: Design

Specific Safety Requirements
No. SSR-2/1 (Rev. 1)

 **IAEA**
International Atomic Energy Agency

Feb. 2016

1 | REGULATION AND SAFETY ASSESSMENT SCOPE

REGULATION OF FIRST ORDER (2 of 2)

WENRARHWG

Report
WENRA
Safety Reference
Levels for Existing
Reactors

—

UPDATE IN RELATION TO LESSONS LEARNED FROM TEPCO
FUKUSHIMA DAI-ICHI ACCIDENT

30 May 2014

May 2014

WENRARHWG

Guidance Document
Issue T:
Natural Hazards
Head Document

—

Guidance for the WENRA Safety Reference Levels for Natural
Hazards introduced as lesson learned from TEPCO Fukushima Dai-
ichi accident.

21 April 2015

April 2015

WENRARHWG

Report
Safety of new NPP
designs

—

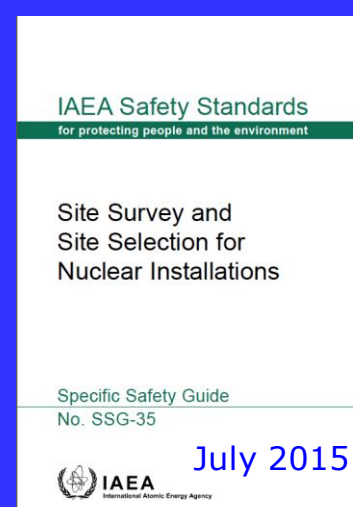
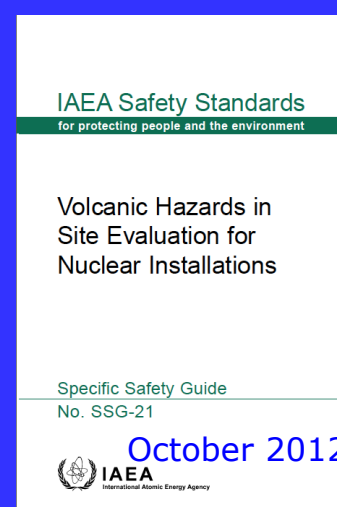
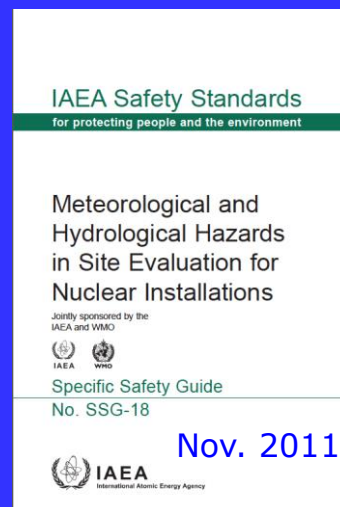
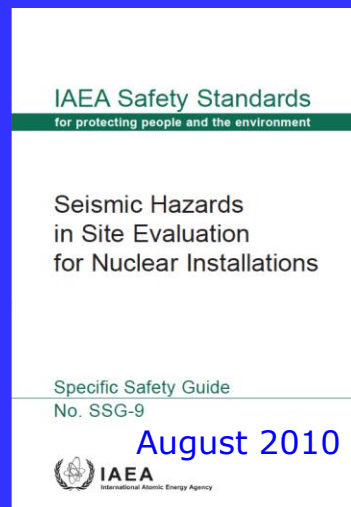
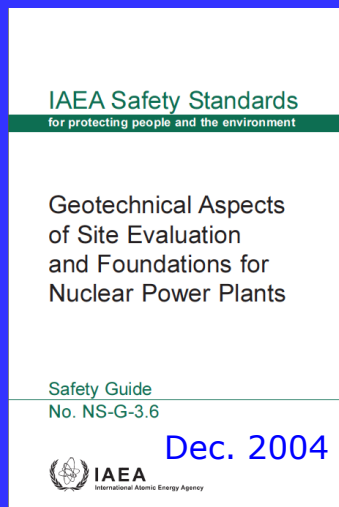
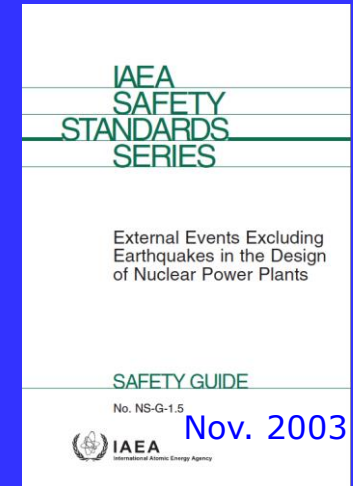
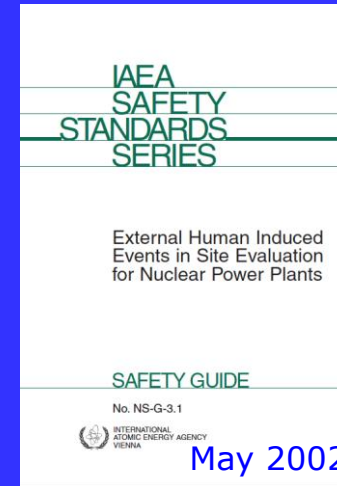
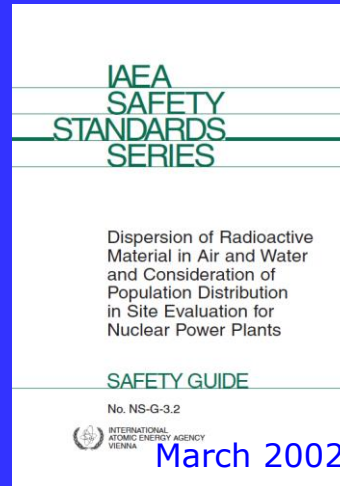
Study by Reactor Harmonization Working Group RHWG
March 2013

March 2013

1 REGULATION AND SAFETY ASSESSMENT SCOPE

SAFETY GUIDES (1 of 2)

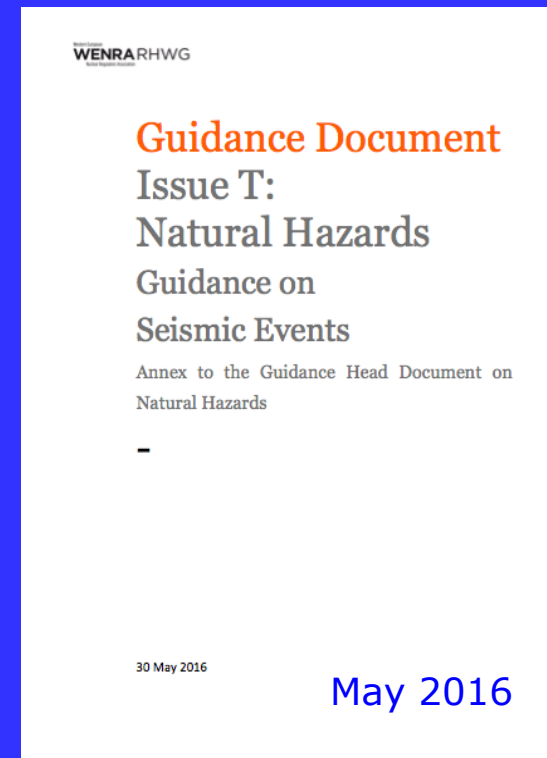
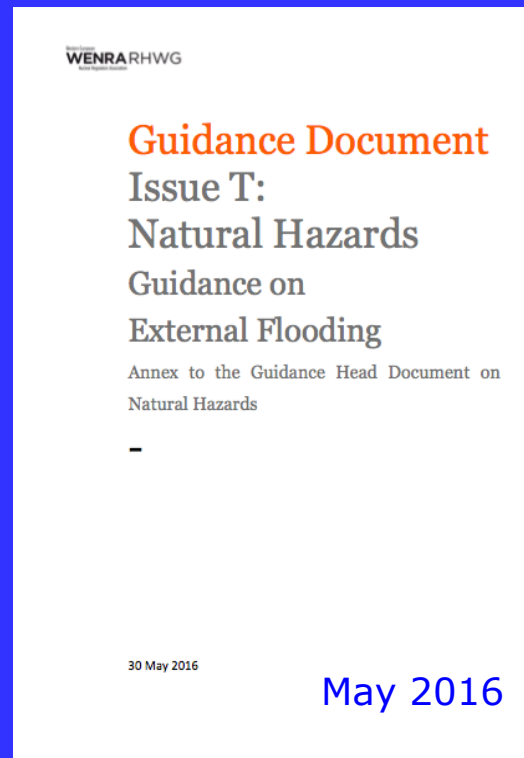
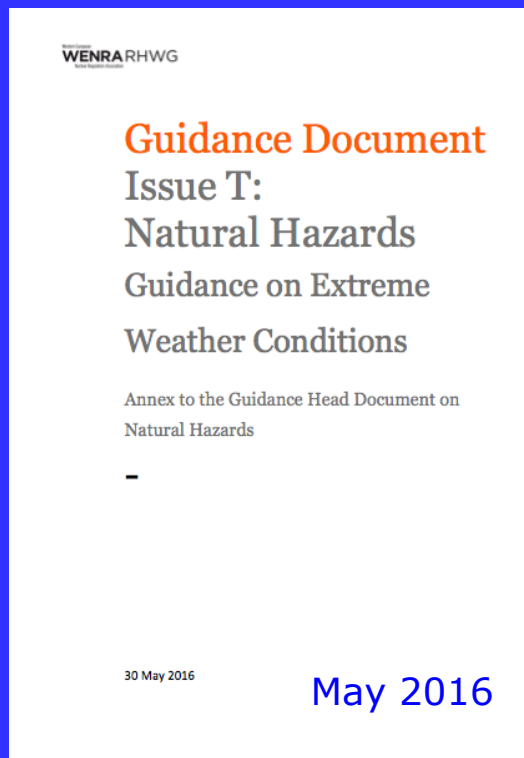
<http://www-ns.iaea.org/committees/files/CSS/205/status.pdf>



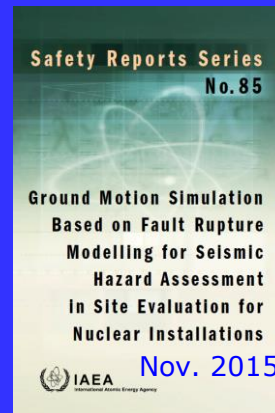
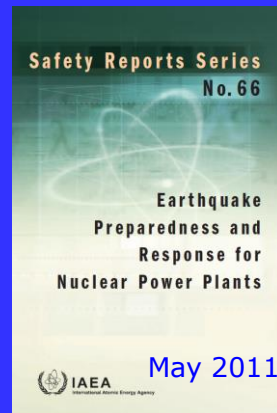
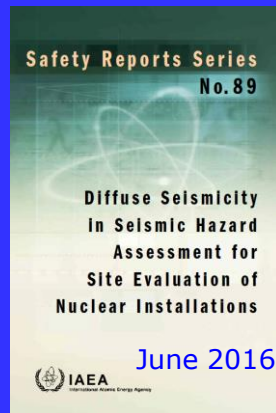
1 | REGULATION AND SAFETY ASSESSMENT SCOPE

SAFETY GUIDES (2 of 2)

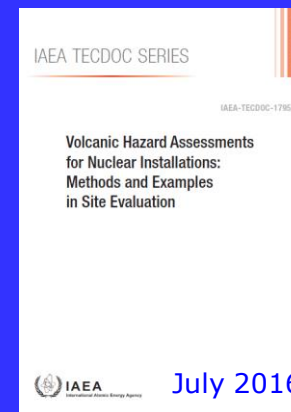
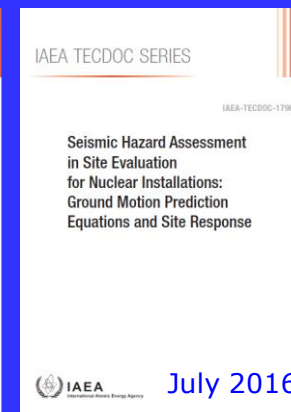
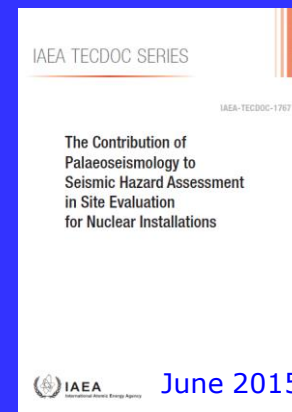
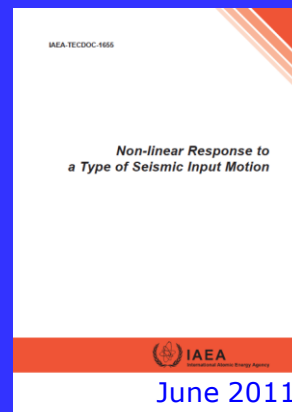
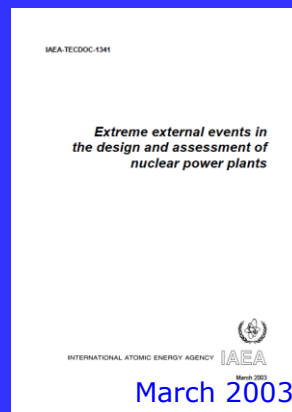
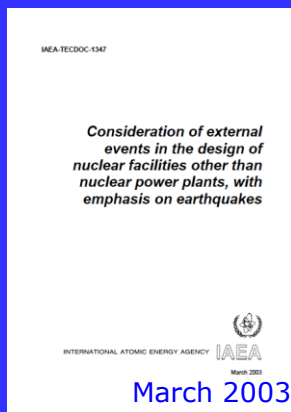
<http://www.wenra.org/publications/>



1 | REGULATION AND SAFETY ASSESSMENT SCOPE



SAFETY REPORTS AND TECDOCS



1 | REGULATION AND SAFETY ASSESSMENT SCOPE

SAFETY ASSESSMENT:

- ✓ **Concept** (IAEA Safety Glossary, 2007): The systematic process that is carried out to ensure that all the relevant safety requirements are met by the design, and cover of all aspects of a practice that are relevant to protection and safety, this includes siting, design and operation of the facility.

“Safety” means the protection of people and the environment against radiation risks, and the safety of facilities and activities that give rise to radiation risks. It is concerned with both radiation risks under normal states and as a consequence of incidents (initiating events, accident precursors, near misses, accidents), as well as with other possible direct consequences of a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation.

1 | REGULATION AND SAFETY ASSESSMENT SCOPE

SF-1:

- ✓ **§ 2.1.** The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation. To ensure this statement, measures have to be taken:
 - (a) To control the radiation exposure of people and the release of radioactive material to the environment;
 - (b) To restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation;
 - (c) To mitigate the consequences of such potential events.
- § 2.2.** This objective applies for all N.I. and activities and for all stages over the lifetime of a N.I. or radiation source, including planning, siting, design, manufacturing, construction, commissioning, and operation, as well as decommissioning and closure.

1 | REGULATION AND SAFETY ASSESSMENT SCOPE

SF-1. Principle 8. Prevention of accidents:

All practical efforts must be made to prevent and mitigate nuclear or radiation accidents.

- ✓ § 3.31. "Defence in depth" is the primary mean of preventing and mitigating the accident consequences. This concept is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to the people or the environment.
- ✓ § 3.32. Some elements of the *defence in depth* is an adequate site selection, a good design and engineering features providing safety margins, and to provide diversity, independency and redundancy in the design of safety systems.

1 | REGULATION AND SAFETY ASSESSMENT SCOPE

WENRA-SRLs for Existing Reactors:

All practical efforts shall be made to prevent and mitigate nuclear or radiation accidents.

- ✓ § E2.2. The defence in depth concept shall be applied to provide several levels of defence, including a design that provides a series of physical barriers, to prevent uncontrolled releases of radioactive material to the environment, as well as a combination of safety features that contribute to the effectiveness of the barriers.

The design shall prevent as far as practicable:

- Challenges to the integrity of the barriers;
- Failure of a barrier when challenged;
- Failure of a barrier as consequence of failure of another barrier.

1 | REGULATION AND SAFETY ASSESSMENT SCOPE

SSR-2/1 (Rev. 1). Defence in Depth (1 of 3):

- ✓ § 2.13. There are five levels of defence.

The first level of defence leads to requirements that the plant be soundly and conservatively sited and designed against external events;

In the second level is assumed that postulated initiating events are likely to occur over the operating lifetime of a NPP and cover the provision of specific systems and features in the design to prevent such events, or to minimize their consequences;

The third level assume that, although very unlikely, postulated initiating events might not be controlled at the second level and that an accident could develop. This leads to design requirements for to be capable of preventing damage to reactor core or radioactive releases requiring off-site protective actions.

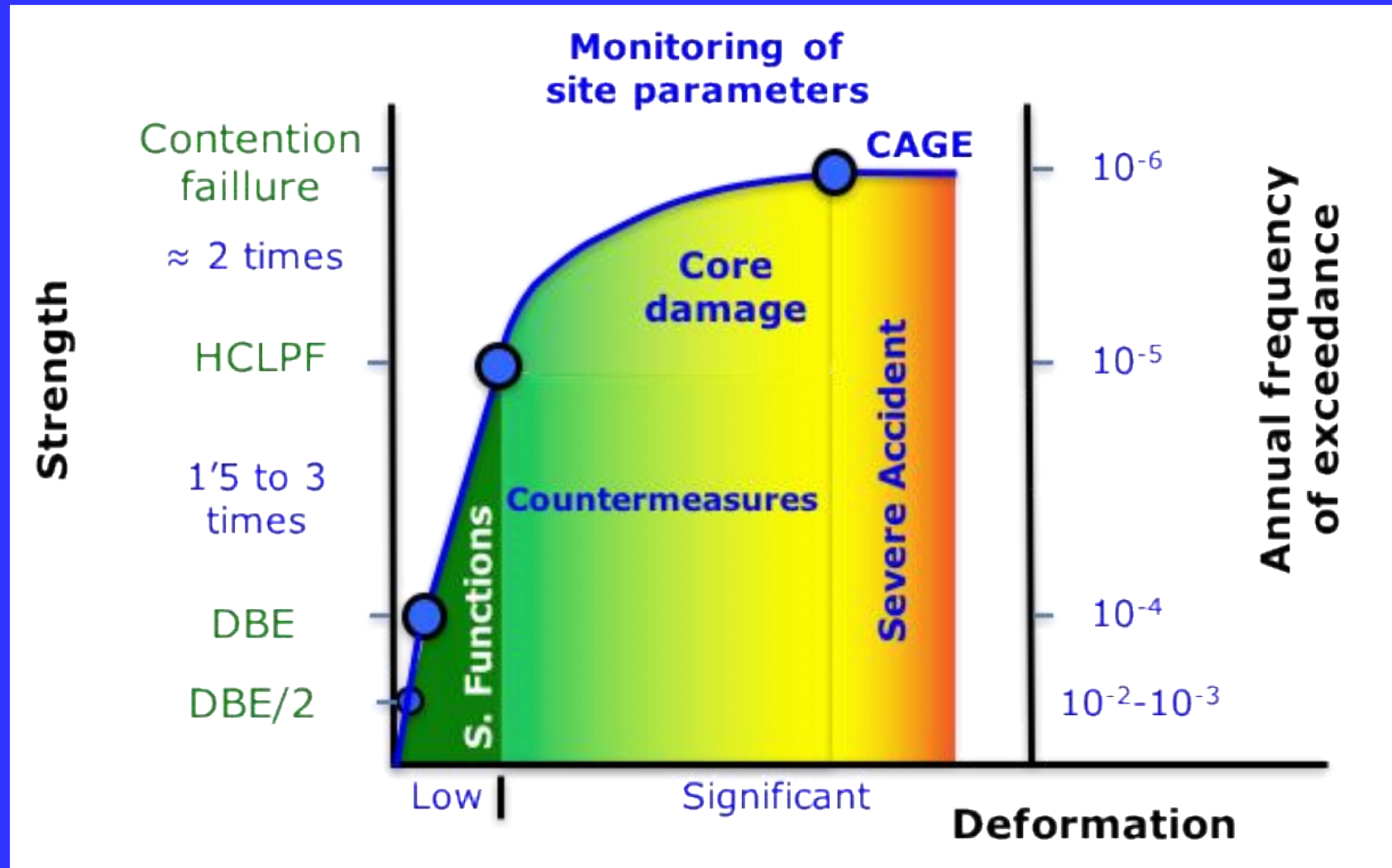
1 | REGULATION AND SAFETY ASSESSMENT SCOPE

SSR-2/3 (Rev. 3). Defence in Depth (2 of 3):

The fourth level purpose is to mitigate the consequences of accidents (DEC) that result from failure of the third level. Event sequences that would lead to an early radioactive release or a large radioactive release are required to be “practically eliminated” (with a high level of confidence to be extremely unlikely to arise or physically impossible).

The purpose of the fifth level of defence is to mitigate the radiological consequences of radioactive releases that could potentially result from accidents. This requires provision of adequately equipped emergency response facilities and emergency plans and emergency procedures for on-site and off-site emergency response.

1 REGULATION AND SAFETY ASSESSMENT SCOPE



1 | REGULATION AND SAFETY ASSESSMENT SCOPE

SSR-2/1 (Rev. 1). Defence in Depth (3 of 3):

- ✓ § 2.14. The number of provisions and measures that will be necessary will depend, among others, of the possible internal and external hazards and the potential consequences of failures.
- ✓ § 4.13. The design of the plant shall take due account of the results of deterministic and probabilistic safety analyses for external events, to ensure that due consideration is given to the prevention of accidents and to mitigation of the consequences of any accidents that do occur.
- ✓ § 4.13. The design shall be such as to ensure, as far as is practicable, that the first level of defence, or at most the second one, is capable of preventing an escalation to accident conditions for all failures or deviations from normal operation that are likely to occur over the operating lifetime of the NPP.

2 | GENERAL REQUIREMENTS FOR SAFETY ASSESSMENT

GSR, Part 4, Rev. 1:

Requirement 10. Assessment of Engineering Aspects (1 of 2):

- ✓ **§ 4.31.** The external events (natural and human induced) shall be addressed in the safety assessment, and it shall be determined if an adequate level of protection against their consequences is provided.

If a protection to withstand the effects of external events is required (referred to as DBEE) their severity (size) shall be established for each one; on the basis of a survey of the site and surrounding area for human induced events, and historical data for natural external events account taken for each event type, accuracy, quantity and period of time covered by the catalogue.

The safety assessment shall demonstrate that the design have available margins to withstand external events more severe than those selected for the design basis.

2 | GENERAL REQUIREMENTS FOR SAFETY ASSESSMENT

WENRA-SRLs for Existing Reactors.

- ✓ § **E5.2.** External hazards shall be taken into account in plant design:
 - Human made external hazards, including airplane crash, other nearby transportation, industrial activities and site area conditions which reasonably can cause fires, explosions or other threats to the safety of the NPP, shall as a minimum be taken into account in the design of the plant according to site specific conditions.
 - All natural hazards that might affect the site shall be identified, including any related hazards. Justification shall be provided that the compiled list is complete and relevant to the site. This list shall be included following hazards: Geological, Seismotectonic, Meteorological, Hydrological, Biological and Forest fire (Appendix 1 of Head Document).

2 | GENERAL REQUIREMENTS FOR SAFETY ASSESSMENT

WENRA-SRLs for Existing Reactors.

Objective:

- ✓ **§ T1.1.** Natural hazards shall be considered an integral part of the safety demonstration of the plant (including spent fuel storage). Threats from natural hazards shall be removed or minimized as far as reasonably practicable for all operational plant states.

To identify needs and opportunities for improvement, the safety demonstration shall include assessments of the design basis and DEC (DEC could result from natural events exceeding the DBEE or from events leading to conditions not included in the design basis accidents).

2 | GENERAL REQUIREMENTS FOR SAFETY ASSESSMENT

WENRA-Head Document:

- ✓ § T1.1. Some natural hazards may not have been considered fully in the original design of plants, however in the re-evaluation under periodic reviews they should be treated as an integral part of the safety demonstration.

Assessment of natural events exceeding the design basis should be undertaken to identify if the plant has any disproportionate changes in safety performance for demands exceeding the design basis (cliff edge effects) and to identify the needs and opportunities to implement any reasonably practicable improvements to ensure that cliff edge effects are sufficiently remote from the design basis.

3 | SPECIFIC REQUIREMENTS FOR SAFETY ASSESSMENT

SSR-2/1 (Rev. 1):

Requirement 17. Internal and External Hazards (1 of 3):

All foreseeable external/internal hazards affecting the safety of the NPP, shall be identified and their effects shall be evaluated. These hazards shall be considered in designing the layout of the plant and in determining the postulated initiating events and generated loadings for use in the design of relevant items important to the plant safety.

- ✓ **§ 5.15A.** Items important to safety shall be designed and located, to withstand the effects of hazards or to be protected, in accordance with their importance to safety, against hazards and against common cause failure mechanisms generated by those hazards.
- ✓ **§ 5.15B.** For multiple unit plant sites, the design shall take due account of the potential for specific hazards to give rise to impacts on several or even all units on the site simultaneously.

3 | SPECIFIC REQUIREMENTS FOR SAFETY ASSESSMENT

SSR-2/1 (Rev. 1):

Requirement 17. Internal and External Hazards (2 of 3):

- ✓ **§ 5.17.** The design shall include those external events that have been identified in the site evaluation process. Severity and likelihood shall be considered in postulating potential hazards. In the short term, the safety of the plant shall not be permitted to be dependent on the availability of off-site services such as electricity supply and fire fighting services. The design shall take due account of site specific conditions to determine the maximum delay time by which off-site services need to be available.
- ✓ **§ 5.19.** Features shall be provided to minimize any interactions between buildings containing items important to safety (including power and control cabling) and any other plant structure as a result of external events considered in the design.

3 | SPECIFIC REQUIREMENTS FOR SAFETY ASSESSMENT

SSR-2/1 (Rev. 1):

Requirement 17. Internal and External Hazards (3 of 3):

- ✓ **§ 5.21.** The design of the plant shall provide for an adequate margin to protect items important to safety against levels of external hazards to be considered for design, derived from the hazard evaluation for the site, and to avoid cliff edge effects (sudden large variation in plant conditions in response to a small variation in a site parameter).
- ✓ **§ 5.21A.** The design of the plant shall also provide for an adequate margin to protect items ultimately necessary to prevent an early radioactive release or a large radioactive release, if measured levels of natural hazards exceed those considered for design.

3.1 | SITE SPECIFIC

WENRA-SRLs for Existing Reactors. Plant Design.

Site Specific Natural Hazard Screening and Assessment:

- ✓ **§ E6.1 / T3.1.** Natural hazards identified as potentially affecting the site can be screened out on the basis of being incapable of posing a physical threat or being extremely unlikely with a high degree of confidence.

Care shall be taken not to exclude hazards which in combination with other hazards (could include other natural hazards, internal hazards or human induced hazards. Consequential hazards and causally linked hazards shall be considered, as well as random combinations of relatively frequent hazards) have the potential to pose a threat to the facility. The screening process shall be based on conservative assumptions and supporting arguments shall be justified.

3.1 | SITE SPECIFIC

WENRA-Head Document:

- ✓ § T3.1. To demonstrate that an event is extremely unlikely with a high degree of confidence should take account of the assessed event frequency, and of the associated confidence degree. The uncertainties in data/methods should be evaluated in order to underwrite the degree of confidence claimed.

The demonstration should not be claimed solely based on compliance with a general cut-off probabilistic value. The compliance level should be proportionate to the remoteness of the hazard and the associated uncertainty or lack of data to support the screening.

More frequently hazards should not pose threats by themselves, but may contribute to the overall hazard by being coincident with other extreme events. Such events should be identified, kept during the screening and included in the site specific hazard assessment.

3.1 | SITE SPECIFIC

WENRA-SRLs for Existing Reactors. Plant Design.

- ✓ § T3.2. For all natural hazards that have not been screened out, hazard assessments shall be performed using deterministic and, as far as practicable, probabilistic methods taking into account the current state of science and technology.

In this hazard assessments shall take into account all relevant available data, and produce a relationship between the hazard severity (e.g. magnitude and duration) and exceedance frequency.

The maximum credible hazard severity, or maximum credible event (the most severe event considered to be extremely unlikely to be exceeded with a high degree of confidence) shall be determined where this is practicable.

3.1 | SITE SPECIFIC

WENRA-Head Document:

- ✓ § T3.2. A relationship between the hazard severity and frequency should be developed including mean and different confidence levels.

The extended duration of some natural events may give rise to increased severities and should be considered carefully.

The maximum credible event can be useful to define a DBE when probabilistic results have large uncertainties, and also provides a useful insight into the beyond design basis (DEC).

The determination of a maximum credible event is a difficult task for many hazards. In cases where a fully established scientific process is not available (due to few data or limited understanding of the physical processes) may be needed apply approaches with expert elicitation basis that should not be based on single experts, and the arguments should be thoroughly documented.

3.1 | SITE SPECIFIC

WENRA-SRLs for Existing Reactors. Plant Design.

- ✓ § **T3.3**. The following shall apply to hazard assessments:
 - Shall be based on all relevant site/regional data. Particular attention shall be given to extending available data to include historical data and events beyond recorded.
 - Special consideration shall be given to hazards whose severity changes during the expected lifetime of the plant.
 - The methods and assumptions used shall be justified. Uncertainties affecting the hazard assessments results shall be evaluated.

3.1 | SITE SPECIFIC

WENRA-Head Document:

- ✓ § T3.3. Efforts should be made to extend the site specific database (geomorphology, palaeoseismology, geophysics surveys), because of uncertainties can be reduced by new data. If there are shortage of reliable data for hazard assessment, information on the specific hazard from analogue regions may be used to refine uncertainties.

Hazard changes with time, (climate, sea level, or river changes) should be considered in the hazard assessment by take into account the plant lifetime.

The database of events are often short relative to the frequency of events that are being calculated. The treatment and incorporation of uncertainties in the hazard assessment is vital to ensure confidence in the resulting values.

3.2 | DESIGN BASIS FOR EXTERNAL EVENTS (DBEES)

WENRA-SRLs for Existing Reactors. Plant Design.

Definition of the DBEs:

- ✓ **§ T4.1.** DBEs definition shall be based on the site specific hazard assessment, from individual or combinations of natural hazards, causally or non-causally linked (due to a common root cause), and may be either the original basis or reviewed (e.g. following a PSR).
- ✓ **§ T4.2.** The exceedance frequencies of DBEs shall be low enough to ensure a high degree of protection. A common target value of frequency, not higher than 10^{-4} per annum, with due consideration of uncertainties, shall be used for each DBE. Where it is not possible to calculate these probabilities with reliable certainty, an event shall be chosen and justified to reach an equivalent level of safety.
- ✓ **§ T4.3 / T4.4.** Historical extreme events shall be enveloped by each plant DBE with a sufficient margin. Parameters of each DBE shall be defined from conservative basis of the hazard assessments results.

3.2 | DESIGN BASIS FOR EXTERNAL EVENTS (DBEES)

WENRA-Head Document:

- ✓ § T4.1. The simultaneous application of two independent low frequency hazards is considered as unreasonable.

The probability analysis of credible combinations of non-causally linked hazards should consider the duration of the events.

- ✓ § T4.2. The use of a confidence level higher than the median hazard curve is expected. Care should be taken where multiple parameters are used to define an event (e.g. to combine results of intensity storm and duration storm for an equal frequency of 10^{-4}).
- ✓ § T4.4. For each DBE (individual or combination of natural hazards), associated parameters should be readily applicable to engineering assessments, and should be defined to provide a basis for the safety demonstration of the plant.

3.2 | DESIGN BASIS FOR EXTERNAL EVENTS (DBEES)

SSR-2/1 (Rev. 1):

Requirement 14. Design Basis for Items Important to Safety:

The design basis for items important to safety shall specify the necessary capability, reliability and functionality for operational states, for accident conditions and for conditions arising from internal and external hazards, to meet the specific acceptance criteria over the lifetime of the NPP.

- ✓ § 5.3. The design basis for each item important to safety shall be systematically justified and documented. The documentation shall provide the necessary information to operate the plant safely.

3.3 | PROTECTION AGAINST DBEEs

WENRA-SRLs for Existing Reactors. Plant Design.

Protection Against Design Basis for External Events:

- ✓ **§ T5.1.** A protection concept shall be provided to cope with natural hazards. It shall encompass the protection against DBEs, events exceeding DBEs and the links in-to Emergency Operating Procedures (EOPs) and Severe Accident Management Guidelines (SAMGs).

If a exceedance frequency of 10^{-4} /year for seismic hazards were not used for the original DBE of the plant and if it is not reasonably practicable to do a level of protection equivalent, seismic margin methods (NS-G-2.13) may be used and current seismic capacity of the plant shall be quantified, and demonstrate that the plant is protected against a hazard level of probability 10^{-4} /year.

- ✓ **§ T5.2.** The protection shall be of sufficient reliability that the fundamental safety functions are conservatively ensured for any direct and credible indirect effects of the DBE.

3.3 | PROTECTION AGAINST DBEEs

WENRA-Head Document:

- ✓ § **T5.1 / T5.2**. For multiple unit sites, the protection concept should consider the simultaneous need for specific equipment and human resources and should further account for credible indirect effects, those should be identified with high conditional probability.

In addition, possible linked sequence of events following a natural event need careful consideration.

3.3 | PROTECTION AGAINST DBEEs

WENRA-SRLs for Existing Reactors. Plant Design.

- ✓ § **T5.3**. The protection concept shall:
 - (a) apply conservatism providing safety margins in the design;
 - (b) rely primarily on passive measures;
 - (c) ensure that measures to cope with a design basis accident remain effective during and following a design basis event;
 - (d) take into account the event predictability and the development over time;
 - (e) ensure that procedures and means are available to verify the plant condition during and following DBE;
 - (f) consider that events could simultaneously challenge several redundant or diverse trains of a safety system, multiple SSCs or several units at multi-unit sites, site and regional infrastructure, external supplies and others;
 - (g) ensure that sufficient resources remain available at multi-unit sites considering the use of common equipment or services;
 - (h) Not affect the protection against other DBE of different origin than natural.

3.3 | PROTECTION AGAINST DBEEs

WENRA-SRLs for Existing Reactors. Plant Design.

- ✓ § T5.4. For DBE, all SSCs identified as part of the protection concept against natural hazards shall be considered as important to safety.
- ✓ § T5.5. Monitoring and alert processes shall be available to support the protection concept. Where appropriate, intervention values shall be defined to facilitate the timely initiation of protection measures.

In addition, thresholds shall be identified to allow the execution of preplanned post event actions as inspections.

- ✓ § T5.6. During long-lasting natural events, arrangements for the replacement of personnel and supplies shall be available.

3.3 | PROTECTION AGAINST DBEES

WENRA-Head Document:

- ✓ § **T5.4.** The performance of non-safety SSCs should also be considered to avoid potential secondary damage to necessary SSCs.
- ✓ § **T5.5.** Administrative measures, monitoring and alert processes should be used besides permanent measures to provide warning in advance of the onset of natural hazard events or to monitor the development of the natural event.

Monitoring systems should be able to measure events more severe than the DBE without failing or saturating and should be qualified accordingly.

- ✓ § **T5.6.** means of transport and communication equipment should be available for use during and after a natural event.

3.4 | DESIGN EXTENSION CONDITIONS (DEC)

SSR-2/3 (Rev. 3):

Requirement 20. Design Extension Conditions:

- ✓ § 5.32. Where the results of engineering judgement, deterministic and probabilistic safety assessments indicate that combinations of events could lead to anticipated operational occurrences or to accident conditions, such combinations of events shall be considered to be design basis accidents or shall be included as part of design extension conditions, depending on their likelihood of occurrence.

Certain events might be consequences of other events, such as a flood following an earthquake. Such consequential effects shall be considered to be part of the original postulated initiating event.

3.4 | DESIGN EXTENSION CONDITIONS (DEC)

WENRA-SRLs for Existing Reactors. Plant Design.

Events more severe than the DBE:

- ✓ § T6.1. Events beyond DBE shall be identified as part of DEC analysis, and their selection shall be justified.

A representative set of DEC's shall be derived and justified, based on a combination of deterministic and probabilistic assessments as well as engineering judgment.

The selection process shall start by considering those events and combinations, which cannot be considered extremely unlikely with a high degree of confidence and which may lead to severe fuel damage in the core or in the spent fuel storage. It shall cover:

- Events occurrence during operational states of the plant;
- Events resulting from internal or external hazards;
- Common cause failures.

3.4 | DESIGN EXTENSION CONDITIONS (DEC)

WENRA-Head Document:

- ✓ § T6.1. Analysis of natural events exceeding the plant DBEs should be undertaken for several reasons:

To assure that events slightly exceeding the DBE cannot directly lead to severe fuel damage;

The estimation of plant capacity against individual natural hazards, is needed to understand the contribution of each natural hazard to the potential for severe fuel damage and to early or large releases;

To identify plant vulnerabilities and apply measures to improve plant robustness and enhancements to the protection concept, accident management strategies, emergency arrangements and provisions.

3.4 | DESIGN EXTENSION CONDITIONS (DEC)

WENRA-SRLs for Existing Reactors. Plant Design.

- ✓ § T6.3. When assessing effects of natural hazards included in the DEC analysis, and identifying practicable improvements against such events, analysis shall include:
 - (a) Demonstration of sufficient margins to avoid “cliff-edge effects” that would result in loss of a fundamental safety function;
 - (b) Identification and assessment of the most resilient means for ensuring the fundamental safety functions;
 - (c) Events could simultaneously challenge several redundant or diverse trains of a safety system, or multiple SSCs or several units at multi-unit sites, regional infrastructures, external supplies and other countermeasures.

3.4 | DESIGN EXTENSION CONDITIONS (DEC)

WENRA-Head Document:

- ✓ § T6.3. The identification of the value at which a loss of fundamental safety functions will occur is particularly important when the plant's robustness is only adequate to withstand events which are slightly more severe (or slightly more unlikely) than the DBE.

Estimating values at which a loss of safety functions will occur is preferred, but it is difficult to apply to all natural hazards, particularly when hazards are not described by probabilistic models.

An alternative approach to demonstrate sufficient margins before to loss the safety functions is the selection of one or several hazard-specific loading values which are higher than the DBE loads (either in terms of return period or hazard severity) and prove that the fundamental safety functions are not endangered by these loads.

3.4 | DESIGN EXTENSION CONDITIONS (DEC)

WENRA-Head Document:

- ✓ **§ T6.3a.** A margin to cliff-edge effects is defined as the difference between a DBE, and a natural event at which the fundamental safety functions can no more be ensured.

The justification that a loss of fundamental safety functions of heat removal and control of reactivity is only temporary may not be possible for an external event due to the extent damage.

The conservatism applied when establish the design (design reserve) and requirements for construction of safety-related SSCs will usually lead to a margin for plant capability to withstand natural events more severe than the design basis.

3.4 | DESIGN EXTENSION CONDITIONS (DEC)

WENRA-Head Document:

To quantify this margin it is necessary to determine the severity of the event at which fundamental safety functions cannot be assured. The margin can be measured by different ways:

- As a gap in exceedance frequency of the natural hazard used for defining the DBE and the occurrence frequency of an event that leads to a cliff edge effect;
- As a gap in the severity of the events expressed in the physical units of the design basis parameters;
- As a ratio between events severity.

3.4 | DESIGN EXTENSION CONDITIONS (DEC)

WENRA-Head Document:

- ✓ § **T6.3b**. It is needed to identify what is the weakest SSCs of the most resilient line of protection, and this will give an indication of the limiting levels of demand that will challenge the protection concept.
- ✓ § **T6.3c**. DEC assessment should include a scenario in which the site is completely isolated and all external resources are lost (including blackout). Such assessments should determine the duration over which the safe shutdown can be maintained without external support.
- ✓ § **T6.3e**. The verification of as-built conditions of SSCs is seen as a key part of any DEC. It will provide information over the current condition, identify all modifications since installation and any features which may reduce the SSCs resilience not evident from a paper based review. Walkdown process should be structured, undertaken by qualified and experienced individuals, and documented.

3.5 | OTHER REQUIREMENTS FOR DESIGN

SSR-2/1 (Rev. 1):

Requirement 15. Design limits:

A set of design limits consistent with the key physical parameters for each item important to safety for the NPP shall be specified for all operational states and for accident conditions.

- ✓ **§ 5.4.** The design limits shall be specified and shall be consistent with relevant national and international standards and codes, as well as with relevant regulatory requirements.

3.5 | OTHER REQUIREMENTS FOR DESIGN

SSR-2/1 (Rev. 1):

Requirement 30: Qualification of Items Important to Safety:

- ✓ § 5.49. The qualification programme for items important to safety shall include the consideration of ageing effects caused by environmental factors (conditions of vibration, irradiation, humidity or temperature) over the expected service life of those items.

When items important to safety are subject to natural external events and are required to perform a safety function during or following such an event, the qualification programme shall replicate as far as is practicable the conditions imposed on the items important to safety by the natural external event, either by test or analysis, or by a combination of both.

3.5 | OTHER REQUIREMENTS FOR DESIGN

SSR-2/1 (Rev. 1):

Requirement 36: Escape Routes from the Plant:

A NPP shall be provided with a sufficient number of escape routes, clearly and durably marked, with reliable emergency lighting, ventilation and other services essential to the safe use of these escape routes.

- ✓ **§ 5.65.** At least one escape route shall be available from workplaces and other occupied areas following an internal or and external event or following combinations of events considered in the design.

3.5 | OTHER REQUIREMENTS FOR DESIGN

SSR-2/3 (Rev. 3):

Requirement 53. Heat Transfer to an Ultimate Heat Sink:

The capability to transfer heat to an ultimate heat sink shall be ensured for all plant states.

- ✓ **§ 6.19A.** Systems for transferring heat shall have adequate reliability for all plant states in which they have to fulfill the heat transfer function. This may require the use of a different ultimate heat sink or different access to the ultimate heat sink.
- ✓ **§ 6.19B.** The heat transfer function shall be fulfilled for levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.

3.4 | OTHER REQUIREMENTS FOR DESIGN

SSR-2/1 (Rev. 1):

Requirement 54. Containment System for the Reactor:

A containment system shall be provided to ensure, or to contribute to, the fulfillment of the following safety functions at the NPP:

- (a) Confinement of radioactive substances in operational states and in accident conditions;
- (b) Protection of the reactor against external events; and
- (c) Radiation shielding in operational states and in accident conditions.

3.5 | OTHER REQUIREMENTS FOR DESIGN

SSR-2/§ (Rev. §):

Requirement 55. Radioactive Releases from the Containment:

The design of the containment shall be such as to ensure that any radioactive release from the NPP to the environment is as low as reasonably achievable, is below the authorized limits on discharges in operational states and is below acceptable limits in accident conditions.

- ✓ § 6.21. The number of penetrations through the containment shall be kept to a practical minimum and all penetrations shall meet the same design requirements as the containment structure itself. The penetrations shall be protected against reaction forces caused by pipe movement or accidental loads such as those due to missiles caused by external or internal events, jet forces and pipe whip.

3.5 | OTHER REQUIREMENTS FOR DESIGN

SSR-2/1 (Rev. 1).

Requirement 65. Control Room (1 of 2):

A control room shall be provided at the NPP from which the plant can be safely operated in all operational states, either automatically or manually, and from which measures can be taken to maintain the plant in a safe state or to bring it back into a safe state after anticipated operational occurrences and accident conditions.

- ✓ **§ 6.39.** Appropriate measures shall be taken, including provision of barriers between the control room and the external environment, and adequate information shall be provided for the protection of workers of the control room, for a protracted period of time, against hazards such as high radiation levels resulting from accident conditions, releases of radioactive material, fire, explosive or toxic gases. This requirement also apply for the supplementary control room at the NPP (Requirement 66, § 6.41).

3.5 | OTHER REQUIREMENTS FOR DESIGN

SSR-2/1 (Rev. 1).

Requirement 65. Control Room (2 of 2):

- ✓ § 6.40. Special attention shall be paid to identifying those events, both internal and external to the control room, that could challenge its continued operation, and the design shall provide for reasonably practicable measures to minimize the consequences of such events.
- ✓ § 6.40A. The design of the control room shall provide an adequate margin against levels of natural hazards more severe than those considered for design, derived from the site hazard evaluation.

4 | GUIDANCE FOR PLANT PROTECTION

NS-G-1.5. Designing for Protection Against EE.

Safety Analysis for DBEE (1 of 3):

- ✓ **§ 2.19.** For each proposed external event to be considered should be evaluate their effects on the plant, including all credible secondary effects, following the single failure criterion.
- ✓ **§ 2.20.** The common cause failures are typically associated with EE that are expected to have adverse effects over relatively large plant areas, and this type of failures should also be taken into account (the single failure criterion is only capable of dealing with random failures and therefore the redundancy, which is the ultimate outcome of such an analysis, may be defeated by a common cause failure.

4 | GUIDANCE FOR PLANT PROTECTION

NS-G-1.5. Designing for Protection Against EE.

Safety Analysis for DBEE (2 of 3):

- ✓ § 2.21 / 2.22. A DBEE should be assumed coincident with any extreme event if a direct or indirect causal relationship cannot be excluded 2.21; otherwise, a DBEE should not be considered in combination with events that may occur independently, such as other external human induced events or natural phenomena, unless a combination of these events is shown to have a sufficiently high probability of occurrence.
- ✓ § 2.25. Special consideration should be given in the safety analysis to postulate long lasting extreme conditions on site, particularly from extreme weather and flooding events that could delay the feasibility of providing any backup measure from outside the site.

4 | GUIDANCE FOR PLANT PROTECTION

NS-G-1.5. Designing for Protection Against EE.

Safety Analysis for DBEE (3 of 3):

- ✓ **§ 2.29.** The EE may challenge many levels of defence in depth., and basic plant protection should be addressed in the first level, either by design, physical barriers or by component qualification. Probabilistic evaluations should be carried out for the definition of suitable design combinations between EE and internal accidents, addressing both their potential correlation and their joint probability.
- ✓ **§ 2.29.** If a challenge to a level of defence in depth is envisaged, dedicated operational procedures should be put in place with reference to limits and conditions for normal operation, and supported by adequate warning systems and monitoring.

4 | GUIDANCE FOR PLANT PROTECTION

NS-G-1.5. Designing for Protection Against EE.

Design Safety Features for DBEE (1 of 2):

- ✓ § 2.34. There are two basic forms of plant protection against EE:
 - (1) The causal influences of an external event are reduced by means of a passive barrier (dry site concept, site protection dam, external shield, barriers, or building base isolation),
 - (2) The ability of the safety systems to resist the effects of EE is assessed by means of adequate item qualification (including redundancy, diversity and independency, speciality for the UHS).

4 | GUIDANCE FOR PLANT PROTECTION

NS-G-1.5. Designing for Protection Against EE.

Design Safety Features for DBEE (2 of 2):

- ✓ § 2.37. To provide additional plant protection from some EE, administrative measures based on forewarning can also provide safety benefits (e.g. reduction of fire loading materials adjacent to or on the site, installation of additional barriers or closure of watertight gates before flooding, inspection of drainage and trough channels).
- ✓ § 2.41. Adequate robustness should be used in design to provide the plant with some additional capacity for beyond design basis values for conditions in the selected external event scenarios.
- ✓ § 2.42. A evaluation should be carried out to avoid cliff edge effects according to the specific nature of the EE scenario. In this case, additional engineering provisions should be implemented on safety systems at least for a safe shutdown mode.

4 | GUIDANCE FOR PLANT PROTECTION

NS-G-1.5. Designing for Protection Against EE.

Interface with Operational Safety Features (2 of 2):

- ✓ § 2.43. Particular Operating Limits and Conditions (OLC) should be defined for any EE that proves to be important for plant design, in terms of relevance of the hazard, contribution to sizing of safety related items and contribution to the results of probabilistic safety assessment (PSA).

The OLCs should be associated with dedicated surveillance procedures, a plant safe state (possibly a reactor shutdown) that is to be reached after such 'abnormal' events and a post-event revalidation procedure for any item important to safety that may have been challenged.

4 | GUIDANCE FOR PLANT PROTECTION

THANK YOU FOR YOUR ATTENTION !