Western European
WENRA RHWG
Nuclear Regulators Association

Guidance Document
Issue F: Design Extension of Existing Reactors

Guidance for the WENRA Safety Reference Levels for existing Reactors in their update in relation to lessons learned from the TEPCO Fukushima Dai-Ichi accident.

29 September, 2014

Western European
WENRA RHWG
Nuclear Regulators Association

Table of Content
Guidance Document
Issue F: Design Extension of Existing Reactors

00
Introduction

The purpose of this Guidance is to provide explanations of the intent of the Safety Reference Levels (RLs) of Issue F, to contribute to a consistent interpretation and to permit insights into the considerations which have led to their formulation. In addition, some background information is provided for easy reference. This Guidance does not define any additional requirements. Furthermore, it is important to recognize differences in national regulations and in reactor designs when using this document. However, the overall content and meaning is in all cases relevant.

Section 2 of this Guidance includes a listing for design extension conditions which are needed to be taken into account in the safety analyses. Furthermore, a listing of initiating and consequential events for design basis accidents has been included in this Guidance as an Annex, although it is relevant for Issue E (Design Basis Envelope for Existing Reactors). This is considered useful as it contributes to an overall picture of the foundation for both design basis accidents and design extension conditions (see also Figure 1).

01
Objective

F1.1 **As part of the defence in depth, analysis of Design Extension Conditions (DEC) shall be undertaken with the purpose of further improving the safety of the nuclear power plant by:**

- **enhancing the plant's capability to withstand more challenging events or conditions than those considered in the design basis**
- **minimising radioactive releases harmful to the public and the environment as far as reasonably practicable, in such events and conditions.**

Conditions more complex and/or more severe than those postulated as design basis accidents (DBAs) can occur. These conditions shall be investigated as Design Extension Conditions (DEC) so that any reasonably practicable[1] measures to improve the level of safety of a plant, compared to the level reached with the design basis (Issue E), are identified and implemented.

In Issue F, Design Extension Conditions are consistent with the definition in IAEA SSR-2/1:

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

This includes the cases in which, for existing reactors, such considerations occurred after the initial design of the plant has been completed.

The treatment of DECs in IAEA SSR-2/1 is also acknowledged, in particular requirement 20 and the following text:

> *A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences if they do occur. […]*
>
> *The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant is such as to prevent accident conditions not considered design basis conditions, or to mitigate their consequences, as far as is reasonably practicable.*

[1] Determining "reasonably practicable" implies weighing the efforts to reduce the risk against the benefits of risk reduction.

It should be noted that "further improving the safety" as stated in the reference level is not referring to the concept of "continuous improvement". This concept has been introduced in RL A2.3, which is referred to in F5.1. The improvement addressed in RL F1.1, on the other hand, is a process which is performed once by assessing whether the requirements laid down in the RLs of Sections 1 to 4 of Issue F are fulfilled, and implementing the necessary measures in those cases (if any) where they are not. (This process may be performed at different times for different fields.)

The main criterion for the implementation of improvements is reasonable practicability. What is reasonably practicable may change over time, for example because of developments in technology. Hence, there is a need for regular review of the DEC (see RL F5.1), which is a part of continuous improvement as addressed in RL A2.3.

All possible conditions exceeding the design basis events for which reasonably practicable measures can be identified to prevent accident sequences leading to severe fuel damage and/or to mitigate their consequences are included in DEC. Thus, DECs include sequences where severe fuel damage can be avoided (including multiple failure sequences), as well as severe accident sequences – corresponding to the two categories of DEC defined below (RL F1.2). This is presented schematically in Figure 1.

However, there may be conditions exceeding design basis events for which no additional measures are required to prevent severe accidents, due to the existence of margins in the design basis, or due to provisions which had been installed earlier.

The required capability of the plant to withstand the design basis events is determined based on conservative analyses. In addition, the licensee may decide to set design specifications exceeding the required capability, providing what can be called a design reserve. Furthermore, the actual capability of the SSCs may exceed this required capability, due to the chosen design and construction options (robustness). The use of conservative methodologies for analyses, the design reserve and robust design and construction of SSCs lead to a certain margin for the capability of the plant to withstand the design basis events.

Due to this margin, the plant will in reality be able to cope with some more challenging events than those covered by the design basis events and severe fuel damage could therefore be avoided in these cases. These more challenging events are belonging to the DEC A (DEC category for which severe fuel damage is to be prevented, see RL F1.2). It is one of the objectives of the DEC analysis to evaluate whether the extent to which the plant is capable to withstand more challenging events is sufficient. If this is not the case, reasonably practicable improvements should be implemented to enhance the plant's capability to withstand the DEC A.

In case of the more challenging events with postulated severe fuel damage, belonging to DEC B (DEC category with severe fuel damage, see RL F1.2), there will be conditions in the containment which can differ very markedly from those in case of design basis events. Therefore, mitigative provisions are likely to be needed for DEC B to minimize the radioactive releases harmful to the public and the environment as far as reasonably practicable.

The topic of margins is discussed further in the guidance to F3.1 (f).

There are a number of clear and basic differences regarding the treatment of DBA and DEC, e.g.:

- Methodology of analysis: Conservative or best estimate plus uncertainties for DBA, best estimate (with or without uncertainties) acceptable and, in some cases, preferred (see guidance to RL F3.1) for DEC; additional postulates like single failures for DBA, no systematic additional postulates for DEC.
- Technical acceptance criteria: Generally less restrictive and based on more realistic assumptions for DEC.
- Radioactive releases tolerated: Higher consequences are usually tolerated (if it is demonstrated that releases are limited as far as reasonably practicable) for DEC.

F1.2 There are two categories of DEC:

- **DEC A for which prevention of severe fuel damage in the core or in the spent fuel storage can be achieved;**
- **DEC B with postulated severe fuel damage.**

The analysis shall identify reasonably practicable provisions that can be implemented for the prevention of severe accidents. Additional efforts to this end shall be implemented for spent fuel storage with the goal that a severe accident in such storage becomes extremely unlikely to occur with a high degree of confidence.
In addition to these provisions, severe accidents shall be postulated for fuel in the core and, if not extremely unlikely to occur with a high degree of confidence, for spent fuel in storage, and the analysis shall identify reasonably practicable provisions to mitigate their consequences.

Objectives

To reach the objective of enhancing the plant's capability to withstand events or conditions which are more challenging than those considered for the definition of the design basis, and to minimise radioactive releases as far reasonably practicable, both prevention and mitigation of severe accidents are highly important. Category DEC A deals with prevention, whereas category DEC B concerns mitigation. Based on the principle of defence-in-depth, preventive measures have clear precedence over mitigative measures. There are differences regarding selection for analysis and objectives between DEC A where the aim is to avoid fuel damage, and DEC B where severe fuel damage is postulated.

The requirements in the RL differ for fuel in the reactor core and for spent fuel in storage:

- Despite all reasonable preventive measures, DEC with severe core damage have to be considered with the purpose of identifying reasonably practicable mitigative measures.
- Measures for sufficiently mitigating the consequences of severe accidents in spent fuel storages could be difficult to implement. Therefore, it is the goal that such accidents are extremely unlikely with a high degree of confidence.

Events extremely unlikely to occur

The demonstration that an accident is extremely unlikely with a high degree of confidence should take account of the assessed frequency of the condition and of the degree of confidence in the assessed frequency. The uncertainties associated with the data and methods should be evaluated, including the use of sensitivity studies, 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. Probabilistic and deterministic elements both are required for this demonstration.

It should be ensured that the provisions relied upon to demonstrate the extreme unlikeliness remain in place and valid throughout the plant lifetime. For example, in-service inspection and other periodic checks may be necessary.

All analytical methods applied should be validated against the specific phenomena in question, and verified.

The concept of "extremely unlikely with a high degree of confidence" constitutes an essential element of the concept of "practical elimination", as defined by IAEA.
According to IAEA SSR-2/1, *"[t]he possibility of certain conditions occurring is considered to have been practically eliminated if it is physically impossible for the conditions to occur or if the conditions can be considered with a high level of confidence to be extremely unlikely to arise"*. This is further discussed and elaborated in Position 5 of the RHWG Report "Safety of new NPP designs" of March 2013.

The term "practical elimination" has not been used in the RLs. It is usually applied almost exclusively in the context of severe accidents leading to large or early releases. In the safety reference levels, and also in this Guidance, "extremely unlikely with a high degree of confidence" refers in some cases also to large or early releases; in other cases it refers to severe accidents in the spent fuel pool, and also to certain events (F2.2).

Apart from Issue F, "extremely unlikely with a high degree of confidence" is also used in Issue T.

02
Selection of design extension conditions

–

F2.1 A set of DECs shall be derived and justified as representative, based on a combination of deterministic and probabilistic assessments as well as engineering judgement.

The DECs have to be selected and analysed for the purpose of further improving the safety of the nuclear power plant (see guidance to F1.1 regarding the meaning of "further improving") by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, events and accidents that compared to design basis events and accidents are either more severe or involve additional failures. Coverage of DECs can be provided by representative cases – analogous to the choice of a set of design basis events according to RL E4.2, which can serve as representative cases for design basis event analyses to cover all relevant events.

However, the approach of the analysis differs between design basis events and DEC. For the design basis events, the design and analysis are covered by considering conservative bounding cases. In the selection of representative cases for DEC analysis, where the aim is to identify reasonably practicable improvements, a more realistic approach should in general be used: Selecting a very demanding enveloping scenario for the DEC analysis, or setting a very low radiological target for mitigative measures, might lead to the conclusion that no reasonably practicable measures can be identified. Such an approach might not help to demonstrate that there are no reasonably practicable measures to achieve the plant's ability to withstand less demanding scenarios (still exceeding the design basis events). Therefore, the events which are considered in the selection of the representative DECs should cover a wide range of scenarios, from less demanding to more demanding (see also guidance to F2.2).

F2.2 The selection process for DEC A shall start by considering those events, and combinations of events, which cannot be considered with a high degree of confidence to be extremely unlikely to occur and which may lead to severe fuel damage in the core or in the spent fuel storage. It shall cover:

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

Where applicable, all reactors and spent fuel storages on the site have to be taken into account. Events potentially affecting all units on the site, potential interactions between units as well as interactions with other sites in the vicinity shall be covered.

This RL refers to the selection process for DEC A. It stipulates that a wide scope of events and combination of events exceeding the design basis events which may lead to severe fuel damage in the core or in the spent fuel storage are to be considered at the beginning of this process. This is followed by a process of narrowing down the range in the further course of the selection procedure.

The selection process of representative scenarios should notably make use of the PSA results, the overall understanding of the physical phenomena involved, the margins in the design and the systems' redundancy and diversity. In cases in which this does not provide a sufficient basis for the selection process, preliminary analyses of accident sequences triggered by events and combination of events should also be performed.

Only a sub-set of the events and combinations of events considered at the start will be selected for DEC A. From this sub-set the representatives DECs according to RL F2.1 are derived, which subsequently are subjected to the DEC analysis (see RL F3.1).

The initiating events considered as the basis for the selection of DECs of category A should be justified and take into account the following list[2]. In addition, a plant and site specific adjustment and justification will be necessary to demonstrate that a comprehensive set of DECs of category A has been compiled.

Thus, the final sets of conditions selected for DEC A analysis will be plant and site specific, developed on the basis of the following non-exhaustive list.

Initiating events for design extension conditions (DEC A):

- initiating events induced by earthquake, flood or other natural hazards exceeding the design basis events (see Issue T)[3]
- initiating events induced by relevant human-made external hazards exceeding the design basis events[3]
- prolonged station black out (SBO; for up to several days[4])
  - SBO (loss of off-site power and of stationary primary emergency AC power sources)
  - total SBO (SBO plus loss of all other stationary AC power sources), unless there are sufficiently diversified power sources which are adequately protected
- loss of primary ultimate heat sink, including prolonged loss (for up to several days)
- anticipated transient without scram (ATWS)
- uncontrolled boron dilution
- total loss of feed water

[2] The list mainly applies to PWR and BWR. For other designs used in WENRA countries (AGR and PHWR), the list will need to be adapted to the reactor type and justified to the regulatory authority of the relevant country.

[3] This could include subsequent loss of ultimate heat sink combined with station black out or combined with a total station black out.

[4] The prolonged loss of function should consider the time period until external help and/or recuperation of safety systems can be established.

- LOCA together with the complete loss of one emergency core cooling function (e.g. HPI or LPI)
- total loss of the component cooling water system
- loss of core cooling in the residual heat removal mode
- long-term loss of active spent fuel pool cooling
- multiple steam generator tube ruptures (PWR, PHWR)
- loss of required safety systems in the long term after a design basis accident

A listing of initiating and consequential events for the design basis is provided in the Annex to this Guidance. This listing is relevant for Issue E (Design Basis Envelope for Existing Reactors). It is included in the Guidance since it is considered useful to provide an overall picture of the foundation for both design basis accidents and design extension conditions in this Guidance.

Events and combinations of events that can be regarded as extremely unlikely with a high degree of confidence (see guidance to F1.2 for interpretation), based on information available prior to the DEC selection process or on deliberations performed during this process, do not need to be considered further for the DEC selection. For example, this can apply to a particular natural hazard that is extremely unlikely by appropriate site selection; or failure of the RPV, if it is considered extremely unlikely due to design, manufacturing, quality control etc. It may also concern some common cause failures (CCFs) which can be considered extremely unlikely with a high degree of confidence and thus are screened out, or large reactivity insertion.

For events or combinations of events, which cannot be considered with a high degree of confidence to be extremely unlikely to occur and which may lead to accident conditions more challenging than those included in the design basis accidents, the DEC A analysis should be carried out in order to ensure that they are already sufficiently covered (provisions or measures already realised by the design of the plant), or to identify reasonably practicable measures (additional provision or measure to be implemented) to prevent severe fuel damage.

It is conceivable that for an existing plant the analysis of a potential DEC A leads to the result that existing provisions are insufficient to prevent severe fuel damage and no further measures for improving the resistance of the plant on the prevention level are reasonably practicable. Although they are part of the DEC A analysis, the corresponding events or combinations of events will not be covered by the set of representative DECs of category A for the existing plant. In these cases, it has to be investigated if there are reasonably practicable means to mitigate their consequences within DEC B.

F2.3 The set of category DEC B events shall be postulated and justified to cover situations, where the capability of the plant to prevent severe fuel damage is exceeded or where measures provided are assumed not to function as intended, leading to severe fuel damage.

For DEC B (severe accidents) an approach different from that for the selection of DEC A has to be taken, since there will usually be a very large number of possible scenarios, based on a wide range of plant specific severe accident conditions and phenomena, which cannot all be

captured at the start of a selection process. Accordingly, no list of initiating events is provided for DEC B.

A set of severe fuel damage scenarios has to be identified for analysis according to RL F3.1, covering the different situations and conditions which can occur at the outset and during the course of a severe accident. The selection process of representative scenarios should notably make use of the PSA results, the overall understanding of the physical phenomena involved, the margins in the design and the systems' redundancy and diversity. As far as necessary, preliminary analyses of scenarios should be performed as part of the selection process.

Ensuring adequate confinement of radioactive substances, especially by protecting the containment integrity, is the main goal in DEC B. Special consideration should be given to the sequences that could lead to large or early releases to the environment (e.g. high pressure core melt), in order to attenuate the threats or to show that these sequences become very unlikely to occur with a high degree of confidence (to the extent this is required in RLs F4.8 to F4.14).

For existing plants, it cannot be excluded that there are states with severe fuel damage which have to be postulated according to RL F2.3 and which

- were not considered in the past, and
- cannot be considered extremely unlikely with a high degree of confidence, and
- do not lead to the identification of practicable additional measures of prevention (DEC A) and/or mitigation (DEC B) of severe accidents, and
- lead to radiological consequences which exceed the acceptable limits (in particular, to large or early releases).

These cases should be identified and judged by the licensee on a case-by-case basis to determine whether the associated risk is acceptable. For cases where additional measures have been identified as practicable, but are not sufficient to render large or early releases extremely unlikely with a high degree of confidence, a similar judgment has to be made, taking into account the practicable measures.

03
Safety analysis of design extension conditions

F3.1 The DEC analysis shall:

(a) rely on methods, assumptions or arguments which are justified[37], and should not be unduly conservative;

(b) be auditable, paying particular attention where expert opinion is utilized, and take into account uncertainties and their impact;

(c) identify reasonably practicable provisions to prevent severe fuel damage (DEC A) and mitigate severe accidents (DEC B);

(d) evaluate potential on-site and off-site radiological consequences resulting from the DEC (given successful accident management measures);

(e) consider plant layout and location, equipment capabilities, conditions associated with the selected scenarios and feasibility of foreseen accident management actions;

(f) demonstrate, where applicable, sufficient margins to avoid "cliff-edge effects"[38] that would result in unacceptable consequences; i.e. for DEC A severe fuel damage and for DEC B a large or early radioactive release;

(g) reflect insights from PSA level 1 and 2;

(h) take into account severe accident phenomena, where relevant;

(i) define an end state, which should where possible be a safe state, and, when applicable, associated mission times for SSCs.

[37] These methods can be more realistic than for DBA, including best estimate. Modified acceptance criteria may be used in the analysis.

[38] A cliff edge effect occurs when a small change in a condition (a parameter, a state of a system…) leads to a disproportionate increase in consequences.

The DECs which have been selected according to RLs 2.1 to 2.3 are to be subjected to the DEC analysis.

Point (a):

Justified methods depend on the type of analysis which is performed. The purpose of analyses performed for a DEC can be:

(1) to review whether the fundamental safety functions can be guaranteed by existing equipment (installed for design basis accidents) for the selected set of DEC A events; or otherwise

(2) to identify and to evaluate reasonably practicable preventive (DEC A) or mitigative (DEC B) measures for enhancing safety or enlarging margins to avoid possible cliff edge effects (see also (f)).

For (1), conservative approaches or best estimate methodology may be used. In case of (2), best estimate methodology should be preferred to avoid missing reasonably practicable improvements due to an unduly conservative approach (see also Guidance to F2.1 above).

Point (b):

In principle, it could be admissible to perform an analysis without considering uncertainties (see guidance to F1.1). However, the consideration of uncertainties is useful to ensure that the results of a best estimate analysis constitute a meaningful basis for the planning of reasonably practicable improvement measures.

Point (c):

The outcomes of the DEC analyses should be used for:

- Identification of SSCs that are important to prevent severe fuel damage (DEC A) or to prevent large or early releases (DEC B).
- Identification of administrative and procedural measures (operator actions, EOPs, SAMGs etc.) that are important to prevent severe fuel damage (DEC A) or to prevent large or early releases (DEC B).
- Identification of reasonably practicable additional provisions (regarding SSCs as well as administrative and procedural features) to prevent severe fuel damage (DEC A) or to prevent large releases and/or to allow sufficient time for protective actions for the public to be implemented (DEC B).

In addition, the general principle that radioactive releases harmful to the public and the environment have to be minimized as far as reasonably practicable has to be followed.

Point (f):

Within the analysis of DEC, cliff-edge effects should be identified and a sufficient margin to avoid cliff-edge effects should be demonstrated wherever applicable.

The onset of severe fuel damage would be the cliff-edge effect for a DEC A. What is considered as a sufficient margin to avoid a cliff-edge effect is to be decided on a case-by-case basis.

Different kinds of margins may have to be considered, depending on the nature of the DEC. The following examples illustrate this point for DEC A:

- For multiple failure events, the margin to avoid cliff-edge effects could be seen in various ways:
    - The capacity of required SSCs to achieve functional capability beyond their design basis needed to avoid severe fuel damage.

  - The number (or probability of occurrence) of additional failures, beyond a design basis accident, for which it remains possible to avoid severe fuel damage.

- For certain multiple failure events like total SBO, loss of primary ultimate heat sink and many other cases, the margin could be expressed in terms of the period of time available for measures to avoid severe fuel damage. The probability of these sequences may be taken into account.

- For events related to reactivity or loss of coolant, the margin could be expressed in terms of fuel temperature or enthalpy release.

- For external hazards within DEC, margins could in addition be expressed in terms of frequency or severity (see Guidance on Issue T for more information on natural hazards).

For postulated DEC B, the cliff edge effect should be understood in terms of a large increase of radiological consequences due to containment failure. A margin could be expressed in terms of likelihood or time delay of containment failure to occur.

Point (i):

When analysing a sequence in the framework of DEC analysis, an end state should be defined and justified for this analysis. For DEC A, the "defined end state" could be a "safe state" as defined in IAEA SSR-2/1:

> *Plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time.*

However, in case of DEC B, it is unlikely to reach such a safe state. Therefore, the DEC B analysis should cover a reasonable period of time, until some other defined end state is reached. This could be a "controlled state after severe accident". This is a state after a severe accident where decay heat removal is ensured, the damaged or molten fuel is stabilized, re-criticality is prevented and long term confinement is ensured to the extent that there is limited release of radioactive nuclides.

04
Ensuring safety functions in design extension conditions

General

F4.1 **In DEC A, it is the objective that the plant shall be able to fulfil, the fundamental safety functions:**

- **control of reactivity[39],**
- **removal of heat from the reactor core and from the spent fuel, and**
- **confinement of radioactive material.**

In DEC B, it is the objective that the plant shall be able to fulfil confinement of radioactive material. To this end removal of heat from the damaged fuel shall be established[40].

[39] Preferably, this safety function shall be fulfilled at all times; if it is lost, it shall be re-established after a transient period.
[40] For the fulfilment (or re-establishment) of the fundamental safety functions in DEC A and DEC B, the use of mobile equipment on-site can be taken into account, as well as support from off-site, with due consideration for the time required for it to be available.

For DEC A, the fundamental safety function of heat removal can be regarded as fulfilled if operation of the corresponding systems is interrupted for some time, but their function is restored without any relevant fuel damage occurring. In particular, when assessing the residual heat removal from the spent fuel pool, the thermal inertia which is provided by the water inventory of the pool has to be taken into account. However, all relevant cases of fuel inventory and decay heat power which are possible in the pool have to be duly considered, including the case of the reactor core being completely unloaded into the pool.

For DEC B, maintaining the fundamental safety function of confinement has the highest priority. The other fundamental safety functions are of importance insofar as they are required to support the confinement function. The irreversible loss of the confinement function, and the associated uncontrolled consequences, should be avoided. Severe accident management actions to prevent this irreversible loss of the confinement function which are leading to limited and controlled releases to the environment, are not considered as a loss of the confinement function if they are temporary, associated with specific predefined requirements (such as filtering of the releases) and do not lead to unacceptable off-site consequences[5], and thus are part of DEC B measures.

[5] However, consequences may justify the implementation of protective measures in the immediate vicinity of the plant, like evacuation of the public.

F4.2 It shall be demonstrated that SSCs[41] (including mobile equipment and their connecting points, if applicable) for the prevention of severe fuel damage or mitigation of consequences in DEC have the capacity and capability and are adequately qualified to perform their relevant functions for the appropriate period of time.

[41] SSCs including their support functions and related instrumentation.

Regarding the demonstration of the ability of SSCs to perform their functions under DEC:

- The verification of assured flow paths (in particular regarding the state of valves) and accessibility to critical SSCs in station black out conditions should be considered as an integral part of the demonstration of the capability of SSCs to perform their function relevant for safety.
- The "appropriate period of time" refers to the time after the event which is required to reach and sustain and end state according to RL F3.1 (i).

F4.3 If accident management relies on the use of mobile equipment, permanent connecting points, accessible (from a physical and radiological point of view) under DEC, shall be installed to enable the use of this equipment. The mobile equipment, and the connecting points and lines shall be maintained, inspected and tested.

Plant management under DEC may rely on the use of mobile equipment. This equipment and its storage place has to remain unaffected by the DEC (including the external hazards) in which the equipment is relied upon to meet the safety functions. This equipment should be able to operate under the conditions to be expected in this DEC. Consideration should be given to the location and number of connection points to guarantee their availability and timely accessibility under the conditions to be expected in this DEC, so that mobile equipment can be connected to the plant and provide the expected service.

A program for inspections, periodic testing and maintenance on mobile equipment should be established, in accordance with the requirements in Issue K.

F4.4 A systematic process shall be used to review all units relying on common services and supplies (if any), for ensuring that common resources of personnel, equipment and materials expected to be used in accident conditions are still effective and sufficient for each unit at all times. In particular, if support between units at one site is considered in DEC, it shall be demonstrated that it is not detrimental to the safety of any unit.

No further guidance is needed.

F4.5 The NPP site shall be autonomous regarding supplies supporting safety functions for a period of time until it can be demonstrated with confidence that adequate supplies can be established from off site.

The autonomy of the NPP site regarding supplies should be guaranteed for a period of time permitting transport of additional supplies on the site, taking into account the circumstances

in case of design extension conditions, including external hazards exceeding the design basis and related potential damage to infrastructure. The period of time available should be justified by analysis, and then shown to be adequate by demonstrating that the supplies or materials can be delivered and utilised within this timescale[6].

Long-term sub-criticality

F4.6 In design extension conditions, sub-criticality of the reactor core shall be ensured in the long term[42] and in the fuel storage at any time.

[42] It is acknowledged that in case of DEC B, sub-criticality might not be guaranteed during core degradation and later on during some time in a fraction of the corium.

Regarding footnote 42, in case of core melt accidents (DEC B) re-criticality during the on-going core degradation in parts of a (previously) molten core may be difficult to model with any accuracy. Temporary re-criticality in a fraction of the corium is considered to be admissible as long as it is demonstrated that the confinement function is not threatened at any time.

Heat removal functions

F4.7 There shall be sufficient independent and diverse means including necessary power supplies available to remove the residual heat from the core and the spent fuel. At least one of these means shall be effective after events involving external hazards more severe than design basis events.

To secure the cooling of the core and the spent fuel, either an alternative ultimate heat sink (including a complete chain of systems providing a link to it) or a chain of independent and diverse systems of using the primary ultimate heat sink (if the primary ultimate heat sink is available for all events within the DEC involving external hazards[7]) should be in place. If there is an alternative ultimate heat sink, it should be independent as far as practicable from the primary ultimate heat sink (for example, water from river/water from pond, or seawater/air).

The alternative ultimate heat sink or the chain of diverse systems should be able to secure the cooling of the core and the spent fuel for an extended period of time in case of a design extension condition (beyond the point at which a defined end state (see guidance to RL F3.1) has been reached).

In case where the primary means to remove the decay heat from the core and the spent fuel in DEC are not effective anymore, the diverse means of decay heat removal shall be put into service, consistent with the timeframe defined in the safety analysis and actions described in EOPs and SAMGs.

Means which are used for design basis events and which are sufficiently robust to be available in DEC can be credited here, providing there is sufficient independence and diversity.

[6] Several WENRA countries stipulate a duration of 72 hours for this period of time.

[7] An example of a heat sink which is likely to be formally available in all cases is the atmosphere. However, some influences (temperature, moisture, volcanic or fire ashes, duststorm etc.) may impact its cooling efficiency, and hence its availability.

Confinement functions

In case severe spent fuel damage is considered in DEC B (RL F1.2), the RLs on confinement function should be applied, where relevant, to the spent fuel storages.

F4.8 Isolation of the containment shall be possible in DEC. For those shutdown states where this cannot be achieved in due time, severe core damage shall be prevented with a high degree of confidence.

If an event leads to bypass of the containment, severe core damage shall be prevented with a high degree of confidence.

Isolation of the containment penetrations should not impede vital functions which are needed for severe accident management (e.g. containment heat removal).

Special attention needs to be given to situations with an open containment during certain shutdown states. In this case, a core damage accident could more easily lead to large or early releases. Therefore, timely containment isolation should be guaranteed, or measures to prevent core damage with a high degree of confidence shall be available. Specific consideration has to be given to the time needed for the restoration of containment isolation and effective leak-tightness or for implementing the measures to prevent core damage, taking into account factors such as the progression of the accident sequences.

The reference to bypass of the containment in RL F4.8 is not to be interpreted as concerning failing isolation of a containment penetration or deliberate venting of the containment after the occurrence of an event. Rather, F4.8 refers to cases in which the event itself creates a pathway for leakages from the containment (for example, interfacing system loss of coolant accidents). In these cases, core damage could lead more easily to large or early releases and shall therefore be prevented with a high degree of confidence.

F4.9 Pressure and temperature in the containment shall be managed.

This RL covers all types of over-pressurization as well as risks related to under-pressure where relevant.

The following RLs F4.10 and F4.11 could be seen as special, important cases concerning different mechanisms of over-pressurization.

F4.10 The threats due to combustible gases shall be managed.

The threats due to combustible gases (including but not limited to hydrogen) should be understood to cover combustible gases which may originate from the reactor core, spent fuel storage (if applicable) or from the interaction of corium (from reactor core or spent fuel) with concrete. They also include combustible gases which migrate from the building where they were produced, for example into the containment venting system.

Furthermore, the threats due to combustible gases include high temperature resulting from combustion as well as pressure waves and formation of high-energy fragments (missiles) created by explosions.

F4.11 The containment shall be protected from overpressure. If venting is to be used for managing the containment pressure, adequate filtration shall be provided.

Over-pressurization by non-condensable gases and/or steam has to be taken into account. Venting of the containment may be one option to avoid the irreversible loss of the confinement function due to overpressure.

Should venting be used to protect against over pressurization of the containment, adequate filtering should be implemented so that:

- For off-site consequences, RL F4.14 is met;
- For on-site consequences, anticipated conditions referred to in LM3.5 and LM4.1 are not exceeded.

As a consequence, for some DEC A situations, filtration during venting may not be needed provided that the radiological consequences of the venting are acceptable (see F3.1 (d)).

For multi-unit sites, conditions at other units should be taken into account. Venting systems should be resistant to the relevant external events and DEC B environmental conditions for the time frame for which they are required to operate.

F4.12 High pressure core melt scenarios shall be prevented.

High-pressure core melt scenarios could lead to the irreversible loss of the confinement function. Therefore, it should be demonstrated that such scenarios are extremely unlikely with a high degree of confidence (according to the interpretation in the guidance to RL F1.2).

F4.13 Containment degradation by molten fuel shall be prevented or mitigated as far as reasonably practicable.

The RLs of Issue F do not require that fuel melt is generally rendered extremely unlikely with a high degree of confidence. Therefore, measures against containment degradation in case of fuel melt are required.

RL F4.13 applies to all situations with molten fuel spreading outside the reactor vessel and can concern for example the risks of steam explosions, direct containment heating or the basemat penetration by the corium. Instability of the reactor building caused by the mass of the water injected into this building as part of efforts to control the molten fuel should also be taken into account.

The advantages and disadvantages of different strategies have to be carefully weighed (for example, “dry cavity”, early cavity flooding).

F4.14 **In DEC A, radioactive releases shall be minimised as far as reasonably practicable.**

In DEC B, any radioactive release into the environment shall be limited in time and magnitude as far as reasonably practicable to:

(a) allow sufficient time for protective actions (if any) in the vicinity of the plant; and
(b) avoid contamination of large areas in the long term.

The delay of releases in time in DEC B is not only relevant for protective actions in the vicinity of the plant; it can also be important for the implementation of any additional measures in the plant (or neighboring units) to delay releases further, or to prevent them altogether.

This RL also implies that the leak tightness of the containment and its penetrations should be maintained in the long term in case of DEC A. Furthermore, it sets limits for the degradation of the containment leak tightness due to exposure to DEC temperatures, pressures and radiation (e.g. degradation of rubber seals), differentiating between DEC A and DEC B.

Instrumentation and control for the management of DEC

F4.15 **Adequately qualified instrumentation shall be available for DEC for determining the status of plant (including spent fuel storage) and safety functions as far as required for making decisions[43].**

[43] This refers to decisions concerning measures on-site as well as, in case of DEC B, off-site.

The status of the plant and the safety functions, as far as required, should be monitored or at least ascertainable in case of DEC. In particular, the instrumentation should reliably provide adequate information both on reactor core and spent fuel as well as containment status. The instrumentation should have been demonstrated to be able to perform its safety-related functions in DEC environmental conditions, in order to manage such accidents according to EOPs and SAMGs. Instrumentation for key parameters should also be able to perform its functions for a sufficient period of time in case of a total SBO (see guidance to F4.18).

The lighting at key locations for operators should also remain operational under DEC environmental conditions, for a sufficient period of time in case of a total SBO.

In case of DEC B, it has to be noted that information on the plant status (in particular, concerning the possibility of future releases) is also relevant for deciding on emergency measures off-site.

F4.16 **There shall be an operational and habitable control room (or another suitably equipped location) available during DEC in order to manage such situations.**

Habitability of the control room (or another suitably equipped location) should by preference be achieved by control room design features. In addition, temporary use of personal protection equipment may be taken into account while acknowledging the associated limitations of such equipment.

The “other suitably equipped location” could be a supplementary control room or local control panel, if they are adequately equipped and protected for management of the DEC (A and/or B).

Necessary information from instrumentation should be relayed to the operational control room (or another suitably equipped location) and be presented in such a way to enable a timely assessment of the plant status (including spent fuel storage) and safety functions as far as required in DECs.

Emergency power

F4.17 Adequate power supplies during DEC shall be ensured considering the necessary actions and the timeframes defined in the DEC analysis, taking into account external hazards.

There should be adequate means (stationary and/or mobile) to ensure the required power supply to support fundamental safety functions in case of DEC, including the external events within the DEC, as defined – for natural hazards – in Issue T.

This RL could be fulfilled by providing a stationary diverse AC power supply to account for common cause failures (for example: due to component failure or loss of primary emergency diesel generators’ cooling system) as part of DEC A provisions.

F4.18 Batteries shall have the adequate capacity to provide the necessary DC power until recharging can be established or other means are in place.

DC power supply should be provided during DEC for all functions that are required. For example, where appropriate:

- to guarantee uninterrupted power supply for needed I&C (accident instrumentation – see also RL F4.15),
- for valve drives required for containment isolation,
- to start emergency diesel generators.

DC power supply could be enhanced, for example, by improving battery discharge times, implementing load shedding strategies and preparing dedicated on-time recharging options.

05
Review of the design extension conditions

F5.1 The design extension conditions shall regularly[44], and when relevant as a result of operating experience and significant new safety information, be reviewed, using both a deterministic and a probabilistic approach as well as engineering judgement to determine whether the selection of design extension conditions is still appropriate. Based on the results of these reviews needs and opportunities for improvements shall be identified and relevant measures shall be implemented.

[44] See RL A2.3.

This RL emphasizes that the regular assessment of the overall safety of a nuclear power plant, as required in RL A2.3, has to include the design extension conditions. Reasonably practicable measures for improvement which have been identified shall be implemented in a timely manner, in accordance with A2.3.

List of Acronyms

AC	alternating current
AGR	advanced gas-cooled reactor
AM	accident management
AOO	anticipated operational occurrence
ATWS	anticipated transient without scram
BWR	boiling water reactor
DB	design basis
DBA	design basis accident
DBE	design basis event
DC	direct current
DEC	design extension conditions
DiD	defence in depth
EOPs	emergency operating procedures
HPI	high pressure injection
IAEA	International Atomic Energy Agency
LOCA	loss of coolant accident
LPI	low pressure injection
NPP	nuclear power plant
PHWR	pressurized heavy water reactor
PIE	postulated initiating event
PMF	postulated multiple failure
PWR	pressurized water reactor
PSA	probabilistic safety assessment
RHWG	Reactor Harmonization Working Group
RL	(safety) reference level
RPV	reactor pressure vessel
SAMGs	severe accident management guidelines
SBO	station blackout
SSCs	systems, structures and components
WENRA	Western European Nuclear Regulators' Association

Figure 1:
Scheme of means, events and plant conditions

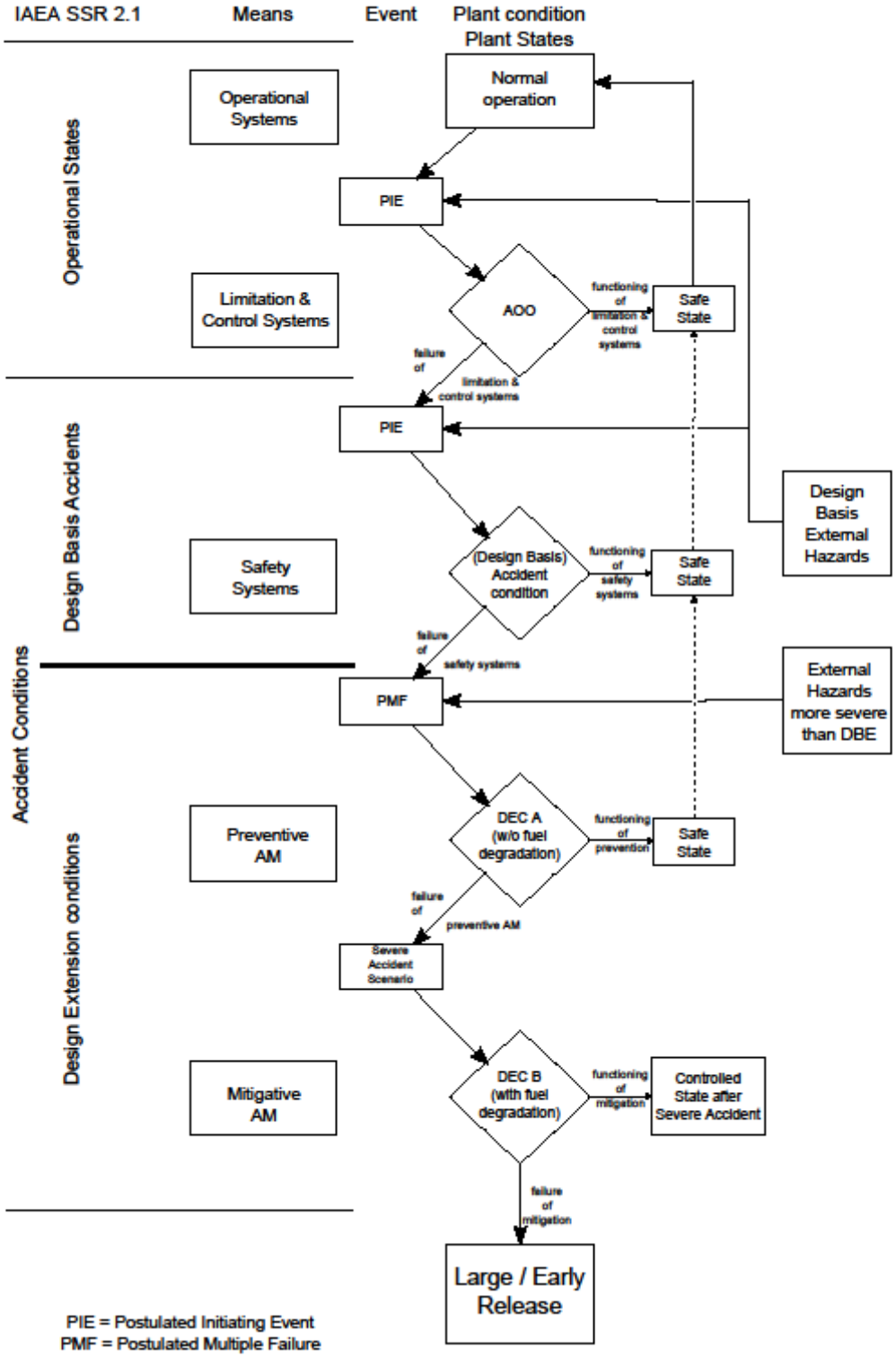
The Figure 1 gives a schematic, simplified overview of the means, events and plant conditions for the operational states and accidental conditions of an NPP. The goal of the figure is not to capture all details but to support the text in the Guidance. Human error, for example, is not mentioned explicitly in the figure. However, 'failure of safety systems', 'failure of preventive AM'… also include failures due to human error, where appropriate.

For clarity, the figure links in a simplified way postulated initiating events (PIEs) to design basis accidents (DBAs) and postulated multiple failures (PMFs) to design extension conditions (DECs), although for some plants some PMFs may be taken into account in the DBA list.

At the right hand side, the external hazards (including natural hazards and human made hazards) are shown as events leading to PIEs or PMFs. Other events (e.g. internal events) could have been added as well. However, the revision of the WENRA Safety Reference Levels contains a new Issue on natural hazards (Issue T). Therefore, only external hazards are shown in the figure 1 in order to illustrate how the natural hazards (and more generally the external hazards) do fit in the more general requirements on design basis (Issue E) and design extension conditions (Issue F).

The figure contains arrows and lines connecting the different plant conditions and events in a top down manner. This is a simplification for clarity as accident scenarios often will not follow such kind of gradual degradation. For example, there can be scenarios going directly from a PIE during normal operation to a design basis accident condition, and a common cause failure added to an AOO generally leads to DEC A. However, adding more possible arrows and lines to the figure would not have been beneficial for the purpose of the figure as illustration supporting the text in this Guidance.

Figure 1: Scheme of means, events and plant conditions



Annex:
Non-Exhaustive List of Initial and Consequential Events for the Design Basis

This listing is relevant for Issue E (Design Basis Envelope for Existing Reactors). It is included in the Guidance for Issue F since it is considered useful to provide an overall picture of the foundation for anticipated operational occurrences, design basis accidents and design extension conditions in this Guidance. In particular, DBAs and DECs of category A are connected and should be seen as complementary.

Like the list for DEC A, this list mainly applies to PWR and BWR. For other designs used in WENRA countries (AGR and PHWR), the list will need to be adapted to the reactor type and justified to the regulatory authority of the relevant country.

As in the case of the listing for DEC A, an adequate justification should be provided if items from this list were not included in the corresponding analyses, and a plant and site specific adjustment and justification will be necessary to demonstrate that a comprehensive list of anticipated operational occurrences and design basis accidents has been compiled.

Events for design basis (anticipated operational occurrences and design basis accidents)

Initiating events

- initiating events induced by earthquake, flood or other natural hazard (see Issue T)
- initiating events induced by aircraft crash, other nearby transportation, industrial activities and site area conditions which reasonably can cause fires, explosions or other threats to the safety of the nuclear power plant, or other human made hazards
- small, medium and large LOCA (up to break of the largest diameter piping of the Reactor Coolant Pressure Boundary)
- breaks in the main steam and main feed water systems
- forced decrease of reactor coolant flow
- forced increase of reactor coolant flow (BWR)
- forced increase or decrease of main feed water flow
- forced increase or decrease of main steam flow
- inadvertent opening of valves at the pressurizer (PWR)
- inadvertent operation of the emergency core cooling system
- inadvertent opening of valves at the steam generators (PWR)
- inadvertent opening of main steam relief/safety valves (BWR)
- inadvertent closure of main steam isolation valves
- steam generator tube rupture (PWR, PHWR)

- inadvertent turbine trip (due to loss of main heat sink, loss of external load etc.)
- uncontrolled movement of control rods
- uncontrolled withdrawal/ejection of control rod
- boron dilution in the reactor coolant system or spent fuel pool (PWR)
- core instability (BWR)
- chemical and volume control system malfunction (PWR)
- pipe breaks or heat exchanger tube leaks in systems connected to the reactor coolant system and located partially outside containment (Interfacing System LOCA)
- fuel handling accidents
- loss of off-site power
- load drop by failure of lifting devices

Initiating events as well as consequential events (could be both types) resulting from internal hazards

- fire
- explosion
- flooding

Consequential events

- missile generation, including turbine missiles
- release of fluid (oil etc.) from failed systems
- vibration
- pipe whip
- jet impact