DRAFT TECDOC

Considerations on the Application of the IAEA Safety Requirements for Design of Nuclear Power Plants

Rev 7b, 22 Sept. 2014

THIS DRAFT IS FOR COMMENTS

Please provide your comments to Mr. Javier Yllera (SAS/NSNI) j.yllera@iaea.org
by October 23, 2014

FOREWORD

CONTENTS

1. INTRODUCTION

BACKGROUND

In 2012, a new IAEA Specific Safety Requirements known as No. SSR-2/1 "Safety of Nuclear Power Plants: Design" [1] was published with the objective to reflect safety developments and experience accumulated in the area of NPP design until that time. Although this publication was primarily developed prior to the Fukushima Daiichi accident, it has been shown that it is affected to a limited extent by the lessons learned from this accident and some changes are currently being proposed to reinforce particular aspects. SSR-2/1 was intended to ensure higher level of safety of NPPs taking into account the achieved state of technological and scientific knowledge and to reflect large consensus. Among the most significant changes as compared with the previous IAEA Safety Requirements (NS-R-1) published in year 2000, are the extension of plant states to consider in the plant design, which should also include multiple failures potentially leading to severe accidents and the strengthened independence of different levels of defence in depth. In accordance with the new requirements, the design should also address the necessary provisions for the mitigation of severe accidents. It should be convincingly demonstrated that all conditions potentially leading to early or large releases are practically eliminated.

In addition, the lessons learned from the Fukushima accident have led to the identification of important topics for safety enhancement, such as the consideration of site specific external natural hazards exceeding the design basis, the possible loss of ultimate heat sink and the capability for using of mobile sources of electric power and coolant.

The indicated issues are currently discussed and addressed in different countries. The complexity of the issues can lead to different interpretations. By having developed this TECDOC the IAEA intends to contribute to the harmonization of opinions and prevent diverging views and implementation means.

This TECDOC can be used as a guidance document to help the regulatory bodies, designers and vendors as well as operating organizations to understand the new IAEA Safety Requirements, to harmonize their implementation and to provide feedback for the preparation of relevant Safety Guide(s).

OBJECTIVE

The main purpose of this TECDOC is to provide interpretation of the new requirements introduced in SSR-2/1 including the amendments to SSR-2/1 produced to incorporate the lessons learned from the Fukushima event. This TECDOC is also intended to propose a revision of the definitions of some relevant terms included in the Safety Glossary to make them more consistent with the new requirements. The document is intended to provide guidance mainly for new reactors and as far as reasonably achievable, also for existing nuclear power plants. However, since the issues discussed are quite general in nature, the document is also applicable, taking into account the graded approach, to other types of nuclear installations. In addition, it should be pointed out that under the scope of nuclear power plant, are also included all facilities associated with the plant operation or containing the fissile materials, in

particular spent fuel pools, located either in the reactor containment or in a separate building.

SCOPE

This TECDOC provides guidance on the following selected topics:

- Categories of plant states, including both reactor and spent fuel pool: the interpretation of the terms such as design basis, beyond design basis, design basis accidents, design extension conditions, beyond design basis accidents for both nuclear reactor and spent fuel pools. Basic rules for identification of the plant states and relevant systems to cope with these states are indicated.
- Implications of the (reinforced) concept of independence of the safety provisions at different levels of defence in depth: guidance is provided on applicability and feasibility of implementation of the requirement for the independence specifically for plant systems at different levels of defence in depth, including also supporting systems (power supply, I&C, etc). The methods for justification of adequacy of provisions at different levels of defence are also addressed.
- Prevention of common cause failures: SSR 2/1 includes a requirement for the design of equipment to take due account of the potential for common cause failures of items important to safety, including to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability. Guidance is provided on the application of such concepts as defensive methods for different root causes of common cause failures.
- Interpretation of the concept of practical elimination: the concept has been investigated and, in addition to a qualitative definition of the term which exists in the IAEA Safety Standards, a more practical and possibly quantitative definition is proposed, considering both components and systems located in the containment as well as outside the containment.
- Design for external hazards: the implications of the new requirements of SSR-2/1 on the design for external hazards have been investigated also to address events possibly initiated by extreme external hazards and to provide guidance for design and safety assessment of equipment for different levels of defence. Considerations on equipment “ultimately necessary’ to prevent early or large release have also been included.
- Design measures for facilitating the use of mobile sources of electric power and coolant: the document describes the issue and indicates limitations in using mobile sources (both of the design as well as operational nature) and identifies additional preconditions for facilitating use of mobile sources, such as adequately robust preassembled connecting points. The need for adequate testing of the systems, availability of procedures and training of personnel is also emphasized.

- Considerations on the ultimate heat sink: the document describes the issue and provides guidance on the understanding of the ultimate heat sink, the relevant challenges to reliable heat transfer including a need of diversity, comprehensiveness of the systems and components to be covered.

STRUCTURE

Section 2 provides a description of the plant states that have to be considered in the design of a new nuclear power plant including an extensive list of examples and guidance for the safety assessment. Section 3 clarifies the concepts of design basis for the plant, design basis for a single structure, system and component, and the concept of beyond design basis. Sections 4, 5 and 6 deeply investigate the concept of defence in depth and its evolution from the original concept proposed by INSAG to the latest interpretation proposed by SSR-2/1 with particular attention the concept of independence of different levels of defence.

Sections 7 to 11 provide information on specific aspects in SSR-2/1 (some of them introduced or changed after the incorporation of the lessons learned from Fukushima) such as: reliability of the ultimate heat sink, prevention of common cause failures, design margins and cliff-edge effects, interpretation of the concept of practical elimination, design for external hazards and use of mobile sources of electric power and coolant. Appendix 1 and Appendix 2 address the acceptance criteria for different plant states and an expanded discussion on dependent failures respectively.

2. PLANT STATES CONSIDERED IN THE DESIGN OF NPPS

STATES CONSIDERED FOR THE DESIGN OF THE REACTOR

Compliance with the fundamental safety objective [2] in the design of a nuclear power plant should be demonstrated for the broad spectrum of plant states including: normal operation, anticipated operational occurrences and accident conditions.

<table>
<tr><th colspan="5">Plant states considered in the design</th></tr>
<tr><td colspan="2">Operational states</td><td colspan="3">Accident conditions</td></tr>
<tr><td rowspan="2">Normal operation (NO)</td><td rowspan="2">Anticipated operational occurrences (AOO)</td><td rowspan="2">Design basis accidents (DBA)</td><td colspan="2">Design extension conditions (DEC)</td></tr>
<tr><td>without fuel damage</td><td>with core melt</td></tr>
</table>

Figure 1. Plant States

In accordance with Requirement 14 of SSR-2/1 the necessary capability, reliability and functionality for items important to safety for individual plant states shall be also specified in their design bases. In accordance with Requirement 13 of SSR-2/1 the subdivision/grouping of the plant states into categories shall be primarily based on their frequency of occurrence at the nuclear power plant.

All sources of radioactive material in the plant, in addition to the reactor core, should be taken into account in the definition of the plant states. These include irradiated fuel

in transit, irradiated fuel in storage and radioactive waste in the waste building. In addition to equipment failures and human errors special attention should be paid to internal and external hazards which could have the potential to adversely affect more than one barrier at once or to cause simultaneous failures of redundant equipment of safety systems.

The table below shows indicative values of the frequency of occurrence of individual scenarios associated with postulated initiating events. These values are consistent with the generally established acceptable value for core damage frequency for new plants to be below 10^{-5}/y [3].

Plant state	Indicative frequency of occurrence
Anticipated operational occurrences	$> 10^{-2}$ events per year
Design basis accidents	$10^{-2} – 10^{-6}$ events per year
Design extension conditions without significant fuel degradation	$10^{-4} – 10^{-6}$ events per year
Design extension conditions with core melt	$< 10^{-6}$ events per year

Table 1. Frequency of occurrence of different plant states

Although boundaries between plant states are shown as specific numbers they should be considered as qualitative indicators rather than rigid borders. In particular there may be some groups of plant states which are traditionally considered as design basis accidents (e.g. large break LOCAs) although they may have lower frequencies. Frequency of occurrence in spite of its prime importance should not be used as the only basis for categorization of plant states.

The descriptions below refer mainly to water cooled reactors. For other kinds of reactors, specific considerations should be made case by case.

Normal operation (NO)

The safety analysis for normal operation should address all the plant conditions under which systems and equipment are being operated as expected, with no internal or external challenges. This includes all the phases of operation for which the plant was designed to operate in the course of normal operations and maintenance over the life of the plant, both at power and shut down.

The normal operation of a nuclear power plant typically includes the following conditions:
—Initial approach to reactor criticality;
—Normal reactor startup from shutdown through criticality to power;
—Power operation including both full and low power;
—Changes in the reactor power level including house load operation and load follow modes if employed;
—Reactor shutdown from power operation;
- Shutdown in a hot standby mode;
- Shutdown in a cold shutdown mode;

- Shutdown in a refuelling mode or equivalent maintenance mode that opens major closures in the reactor coolant pressure boundary or containment;
- Shutdown in other modes or plant configurations with unique temperature, pressure or coolant inventory conditions;
- Handling and storage of fresh and irradiated fuel.

Anticipated Operational Occurrences[1] (AOOs)

Anticipated operational occurrences are events more complex than the manoeuvres carried out during normal operation that exceed the capability of the control system and that have the potential to challenge the safety of the reactor. These occurrences might be expected to occur at least once during the lifetime of the plant. Generally they have a frequency of occurrence greater than 10^{-2} per reactor-year.

Typical examples of PIEs leading to anticipated operational occurrences could include those given below. This list is broadly indicative. The actual list will depend on the type of reactor and the actual design of the plant systems:

- *Loss of off-site power*
- *Increase in reactor heat removal:* inadvertent opening of steam relief valves; secondary pressure control malfunctions leading to an increase in steam flow rate; feedwater system malfunctions leading to an increase in the heat removal rate.
- *Decrease in reactor heat removal:* trip of one main feedwater pump; reduction in the steam flow rate for various reasons (control malfunctions, main steam valve closure, turbine trip, loss of external load, loss of condenser vacuum).
- *Decrease in reactor coolant system flow rate:* trip of one main coolant pump; inadvertent isolation of one main coolant system loop (if applicable).
- *Reactivity and power distribution anomalies:* inadvertent control rod withdrawal; boron dilution due to a malfunction in the volume control system (for a PWR); wrong positioning of a fuel assembly.
- *Increase in reactor coolant inventory:* malfunctions of the chemical and volume control system.
- *Decrease in reactor coolant inventory:* very small loss of coolant accident (LOCA) due to the failure of an instrument line.
- *Release of radioactive material from a subsystem or component:* minor leakage from a radioactive waste system.

Design Basis Accidents[2] (DBAs)

Typical examples of PIEs leading to DBAs could include those given below. This list is broadly indicative and the actual list will depend on the type of reactor and actual design:

---

1 ***anticipated operational occurrence.*** An operational *process* deviating from *normal operation* which is expected to occur at least once during the *operating lifetime* of a *facility* but which, in view of appropriate *design* provisions, does not cause any significant damage to *items important to safety* or lead to *accident conditions*.

2 ***design basis accident.*** *Accident conditions* against which a *facility* is designed according to established *design* criteria, and for which the damage to the *fuel* and the release of *radioactive material* are kept within *authorized limits*.

- *Increase in reactor heat removal:* steam line breaks.
- *Decrease in reactor heat removal:* feedwater line breaks.
- *Decrease in reactor coolant system flow rate*: trip of all main coolant pumps; main coolant pump seizure or shaft break.
- *Reactivity and power distribution anomalies:* uncontrolled control rod withdrawal; control rod ejection; boron dilution due to the startup of an inactive loop (for a PWR).
- *Increase in reactor coolant inventory:* inadvertent operation of emergency core cooling.
- *Decrease in reactor coolant inventory:* a spectrum of possible LOCAs; inadvertent opening of the primary system relief valves; leaks of primary coolant into the secondary system.
- *Release of radioactive material from a subsystem or component:* overheating of or damage to used fuel in transit or storage; break in a gaseous or liquid waste treatment system.

Design Extension Conditions (DECs)

Design extension conditions have been introduced in the requirements for the design of nuclear power plants for the purpose to further improve safety by enhancing the plant's capability to withstand accidents that are more severe than design basis accidents.

According to the IAEA definition design extension conditions are:

Postulated 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 conditions in events without significant fuel degradation and conditions with core melting.

The term "Design Extension Condition" (DEC) was first formally introduced in the European Utility Requirements (EUR) [4] to define some selected sequences due to multiple failures with the intent to improve the safety of the plant extending the design basis. The IAEA has adopted the term "design extension condition" for the first time in SSR-2/1.

Design extension conditions are those conditions induced by sequences caused by multiple failures which have a frequency of occurrence that cannot be neglected and in some cases comparable with the frequency of some DBAs. In general, three types of multiple failures can be considered according to the systems in which they are postulated to take place:

- initiating events that could lead to situation beyond the capability of safety systems that are designed for a single initiating event. Typical example is the multiple tube rupture in a steam generator of PWRs.

- multiple failures (e.g. common cause failures in redundant trains) that prevent the safety systems from performing their intended function to control the PIE. A

typical example is LOCA without actuation of the high pressure safety injection. The failures of supporting systems are implicitly included among the causes of failure of safety systems.

- multiple failures that cause the loss of a safety system while this system is used to fulfil the fundamental safety functions in normal operation. This applies to those designs that use, for example, the same system for the heat removal in accident conditions and during shutdown.

The concept of DEC is not completely new since some multiple failures of safety systems have been considered in the design and safety assessment of existing nuclear power plants or their importance were recognized and requirements were issued to backfit the existing designs. This is the case of the Station Blackout (SBO) and Anticipated Transients without Scram (ATWS). These conditions were beyond the traditional Design Basis Accidents because they involve the total failure of the safety system designed to cope with the respective abnormal event (emergency power supply for loss of off-site power or safety shutdown system for a PIE requiring the actuation of the RPS). The design of safety systems complies with the single failure criterion (two or more redundant trains), and their total functional failure requires for this reason more than one failure in the system. Therefore, the DECs not resulting directly from initiating events, imply necessarily the occurrence of multiple failures.

There are some interpretations that tend to include in the DECs some conditions originated by external hazards that exceed the design basis. Particularly, after the Fukushima accident, some national regulations require NPPs plant to demonstrate capabilities to withstand external events exceeding the original design basis without causing significant releases. This has no relation with the concept of DEC. It should be understood that in the approach of the IAEA Safety Standards (SSR 2/1), a DEC is a plant state (see Figure 1) that can be reached by a postulated sequence of events due to multiple failures of safety systems, but hazards are not considered as plant states. Thus for example, earthquakes exceeding the values specified in the design basis and aircraft crashes are external events with their associated loads and potential safety consequences but not postulated plant states. For this reason they are not included in the current definition of Design Extension Conditions, although similar requirements for analysis and for the acceptance criteria for them could be used as for DECs.

The consideration of a broader spectrum of accident conditions is the main difference in the design of existing and new plants. Design extension conditions can not completely bound any situation which is more severe than design basis accidents. However all plant states, which are more severe than design basis accidents and have a frequency of occurrence which cannot be ignored, have to be considered. Situations that could lead to a significant radiological release (early or large release) have to be considered and provisions have to be taken to make their likelihood so low that means for their mitigation may not be part of the design.

A deviation from normal operation can escalate into design extension conditions only very unlikely either due to extraordinary severity of the event itself or more typically due to multiple failures caused either by equipment malfunction or human error.

The most plausible reason for the failure of safety functions (such as reactivity control and core cooling) is the occurrence of dependent failures that may cause the failure of redundant trains simultaneously. Common cause failures (CCFs) are a predominant group that should be given high attention and provisions should be implemented in the design either to eliminate them to the extent possible or to cope with their consequences.

The use of PSA during the plant design process is a good practice for identification of those event sequences which eventually lead to design extension conditions. Systematic dependencies analysis between SSCs important to safety is a good practice to conclude whether CCFs have been adequately considered.

In the EUR [4] the DEC are defined as below:

A specific set of accident sequences that goes beyond Design Basis Conditions (DBC), to be selected on deterministic and probabilistic basis and including;

- *Complex sequences*
- *Severe accidents*

Appropriate design rules and criteria are set for DEC, in general different from those for DBC.

Both complex sequences and severe accidents result from multiple failures of safety systems. Complex sequences could lead to some core damage without resulting in core melt. Severe accidents refer to sequences leading to core melt.

A concept similar to the DEC introduced by the EUR was also adopted by WENRA [5], although the term design Extension Conditions is not explicitly used. WENRA also proposes to consider some selected multiple failures sequences in the design making a clear distinction between sequences with core melt and without core melt. Multiple failure events are treated as part of the 3rd level of defence in depth (level 3b), but with a clear distinction from level 3a that is related to the traditional Design Basis Accidents.
The figure below shows, a simplified comparison of some of the existing terminologies including examples of DECs.

WENRA	EUR	IAEA
	Design extension Conditions	**Design extension Conditions**
Postulated Multiple failure events	**Complex sequences**	**DEC without core damage**
Small LOCA + Low head safety injection	Main steam line break + consequential SGTR	So far examples are not available in the Safety Standards. They will be included in the revised Safety Guides for NPP Design and Safety Assessment. Proposals are made in this document
Station Blackout	Station Blackout	
ATWS	ATWS	
Loss of the RHR in normal, operation	Containment Bypass (multiple SGTRs)	
Loss of cooling of the spent fuel pool		
Postulated core melt accidents	**Severe accidents**	**Severe accidents**

Currently, following the publication of SSR-2/1 the term Design Extension Conditions is widely used and very often referred to even by Member States that do not explicitly use this term in their regulations.

In the current IAEA approach it is required that Design Extension Conditions include events without and with core melt.

The control of DECs is expected to be achieved by features implemented in the design and not only by accident management measures that are using equipment designed for other purposes. This means that a DEC is such if its consideration in the design leads to the need of additional equipment or to a reclassification of lower class equipment designed for other purposes to mitigate the DEC.

SSR-2/1 requires that the set of DECs to be considered in the design are derived on the basis of engineering judgement and deterministic and probabilistic assessment. Although the operating experience is not explicitly mentioned it is understood that this also will contribute to the derivation of DECs.

Although DECs are to some extent technology dependent, and recommended DECs (except for SBO) are not available in any IAEA safety standards, the list below is provided as a preliminary reference of DECs without core melt:

- anticipated transient without scram (ATWS)[3]
- station black out (SBO)
- total loss of feed water
- LOCA together with the complete loss of one emergency core cooling system (either the high pressure or the low pressure emergency core cooling system)
- uncontrolled level drop during mid-loop operation (PWR) or during refuelling
- loss of the component cooling water system or of the essential service water system
- loss of core cooling in the residual heat removal mode
- loss of fuel pool cooling
- loss of ultimate heat sink function
- uncontrolled boron dilution (PWR)
- multiple steam generator tube ruptures (PWR, PHWR)
- main steam line break and induced steam generator tube ruptures
- loss of required safety systems in the long term after a postulated initiating event
- AOO or DBA combined with the failure of the reactor protection system and the actuation of safety systems

Specific attention has to be paid to support systems (i.e. ventilation, cooling, electrical supply) when identifying credible multiple failures, as these systems may have the potential of causing immediate or delayed consequential multiple failures in both operational and safety systems.

[3] Anticipated transient is here synonymous of anticipated operational occurrence. The possibility of a scram failure following a design basis accident is not considered.

Which system failures need to be considered as DEC and consequently be backed up by alternative safety features becomes a matter of system reliability. Therefore, PSA can be a useful tool in the definition of DECs

For severe accidents (DECs with core melt), maintaining the integrity of containment is the main ultimate objective and also in this case the demonstration may be performed using penalizing assumptions on the key parameters. However, the cooling and stabilization of the molten fuel needs to be achieved to ensure the containment integrity in the long term.

ASSESSMENT OF ADEQUACY OF THE DESIGN FOR DIFFERENT PLANT STATES

The objective of the assessment of the adequacy of the design is to demonstrate that all safety requirements for all plant states are met. This includes, in particular, the demonstration that sufficient margins exist between the actual values of parameters relevant for the integrity of barriers and the threshold values of these parameters at which the barriers would fail.

The assessment of the adequacy of the design should demonstrate, with an adequate degree of confidence, that the radiological consequences for all the plant states considered in the design will remain within the established acceptance criteria and will be ALARA.

Acceptance criteria for maintaining the integrity of barriers and radiological acceptance criteria for each plant state are provided in Appendix 1.

The assessment should take account of the uncertainties in the modelling. SSR-2/1 requires that the deterministic analysis for design of AOOs and DBAs should be conservative while the analysis of design extension conditions may be addressed using a best estimate approach. In addition, a realistic analysis is needed for capturing the actual physical plant response for the development of the accident management programme.

High quality and adequately validated software tools, in particular computer codes are a necessary precondition for robust safety demonstration. Nevertheless, there are always uncertainties associated with the use of computer codes. There are different ways to address those uncertainties so that sufficient margins to acceptance criteria are ensured.

The uncertainties can be dealt with in two different ways:

a) the uncertainties are implicitly compensated (without quantification) by selection of conservative models, inputs and assumptions as well as conservative consideration of operator actions
b) the uncertainties in models as well as in other input data are quantified.

While in the first case, the results are expressed in terms of a set of calculated conservative values of parameters, in the second case, the results are expressed in terms of uncertainty ranges for the calculated parameters.

Both the approaches described above are well developed for anticipated operational occurrences and design basis accidents, but much less experience is available for the analysis of design extension conditions.

For design extension conditions with core melt (severe accidents) it is not always possible to determine in advance which assumptions are conservative. In addition, the same assumption can be conservative for the analysis of a particular phenomenon but non-conservative for the analysis of another phenomenon.

To ensure adequate robustness in the design, whenever it is possible, reasonably conservative assumptions may be made to account for the uncertainties on the physical processes being modelled. This can be done adopting sufficiently large margins (significantly larger than in case of design basis accidents) for the results in terms of predicted timing and severity of challenges to safety barriers.

It is advisable to demonstrate the adequacy of the design by crediting only systems dedicated to severe accident mitigation. This is particular important when the systems are needed for the practical elimination of early or large releases.

Regarding the operator response in design extension conditions, and its consideration for best estimate analysis, it seems appropriate to make the same assumptions (e.g. time necessary for operator action) as in case of design basis accidents.

To prove the implementation of an effective defence in depth and the independence between individual levels of defence, it is in general appropriate to perform comprehensive analysis of bounding cases demonstrating compliance with acceptance criteria for each plant state considering design provisions corresponding to the given level of defence only. However, it is acceptable to perform the analysis of design extension conditions without core melt by crediting systems belonging to level 3, if they are not affected by the combination of failures considered in each sequence. Regarding the analysis of design extension conditions with core melt, it is recommended to credit only features dedicated to these conditions (See Section 6).

3. DESIGN BASIS OF PLANT EQUIPMENT VERSUS BEYOND DESIGN BASIS

It is rather common to make reference to “Design Basis of the plant” or simply to “Design Basis” to indicate that specific conditions and specific rules have been considered in the design of the plant. This terminology is not very precise and, in some cases, it can be misleading. Each single structure, system or component to be correctly designed needs its own design basis and the design basis can be different for different structures, systems or components. Thus it is advisable to refer to the design basis of a structure, system or component.

The paragraph below (that reflects what is detailed in Req. 13-28 of SSR-2/1) summarizes the concept of design basis for a structure, system or component.

The Design Basis of a structure, system or component is the set of information that identifies conditions, needs and requirements necessary for the design including*:*

•*the functions to be performed by a structure, system or component of a facility*
•*the conditions generated by operational states and accident conditions that the structure, system or component has to withstand*
•*the conditions generated by internal and external hazards that the structure, system or component has to withstand*
•*the acceptance criteria for the necessary capability, reliability, availability and functionality*
•*specific assumptions and design rules.*

The design basis of a structure, systems or component is completed and supplemented by Specification Sheets and by detailed design calculations.

The text above could be used to integrate the current definition of Design Basis in the IAEA Safety Glossary[4] that refers explicitly to a facility.

Saying, for example, that a specific accident is included in the design basis of the plant (e.g. it is a design basis accident) means in practice that the conditions generated by this accident are included in the design basis of a set of structures, systems and components that have the function to deal with and control that accident.

Mostly because of historical reasons, there is sometimes confusion between the terms "Design Basis Accidents" and "Design Basis", and consequently between "Beyond Design Basis Accidents" and "Beyond Design Basis".

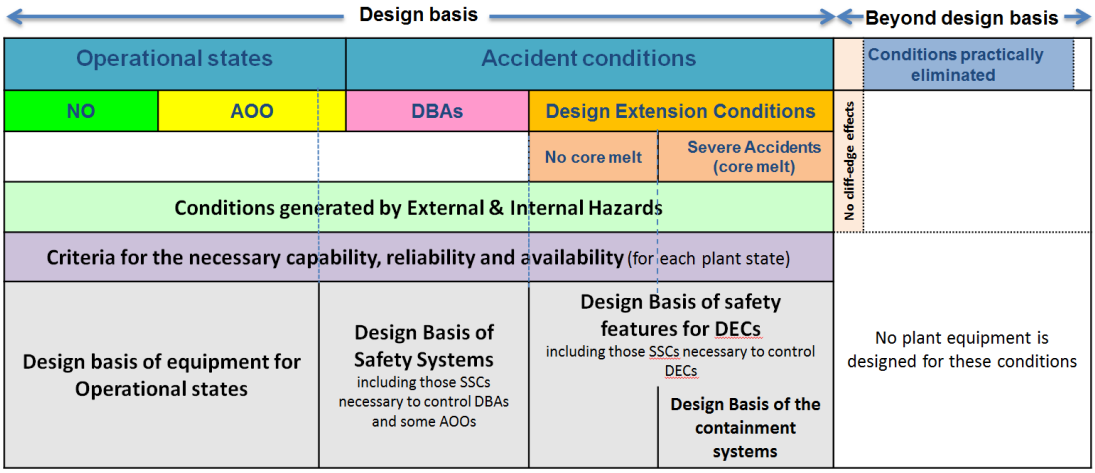
"Design Basis Accidents" is the set of postulated accident conditions that the plant has to withstand meeting the criteria and following the rules specified in SSR-2/1. Design basis accidents are used, together with other factors, to define the Design Basis for safety systems and other items important to safety that are necessary to control the conditions generated by the DBAs. The meaning of Design Basis is much wider than the meaning of Design Basis Accidents and includes all factors of the definition above.

The figure below represents in a simplified graphical form the different components that contribute to the definition of the design basis of the main sets of equipment important to safety.

The Operational states (Normal Operation and Anticipated Operational Conditions) mainly provide input to the design basis of the process equipment for normal operation and for control system, limiting systems and the reactor trip system.

The Accident conditions (DBAs and DECs) provide input to the design basis of Safety systems (control of DBAs) and Safety features for DECs (control of DECs).

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



According to SSR-2/1, conditions leading to early or large releases shall be practically eliminated (See Section 9) and consequently they are not required to be considered for the design of plant equipment, however, SSR-2/1 (paragraphs 4.11 and 5.21) requires that conditions moderately exceeding those postulated in the Accident conditions shall not result in cliff-edge effects (see Section 8).

The figure also shows that the conditions generated by External and Internal hazards and criteria for capability, reliability and availability, provide input to the design basis of the plant equipment. Although the figure does not differentiate these conditions and criteria for the different classes of equipment, it should be considered that the conditions and criteria depend on the safety classification of the specific plant equipment. For example, SSR-2/1 requires the application of the single failure criteria for the design of Safety systems and not for the design of Safety features for DECs.

4. DEFENCE IN DEPTH STRATEGY FOR NEW NPPS

Following the Chernobyl accident the Defence in Depth concept was defined and recognized as a fundamental and overarching principle of nuclear safety for preventing accidents and mitigating their consequences.

Although the implementation of the defence in depth concept has been required for long time, the Fukushima Daii-chi accident and the resultant complementary safety assessments (termed “stress tests” in the EU and other countries) conducted in different Member States have revealed weaknesses in its implementation in some plants. Therefore how to interpret the requirements embedded in the concept of defence in depth is an important element in ensuring its correct and full implementation.

The Table below is taken from INSAG-10 [7] and represents the first description of the concept of defence in depth formalized in five levels of defence. This scheme has

been incorporated in several Safety Standards of the IAEA and has also been followed, with some elaboration, for the preparation of SSR-2/1.

Levels of defence	**Objective**	**Essential means**
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

The defence in depth concept should not be understood as merely limited to the request for the implementation of a number of consecutive barriers and protection levels, but should be understood as any requirement necessary to achieve the quality and reliability expected for the barriers and for systems ensuring their integrity.

Some aspects such as vulnerabilities for common cause failures, appropriate independence between the different levels, robustness and avoidance of cliff edge effects, are key issues to reinforce the overall effectiveness of the implementation of the defence in depth. The sections below address specific aspects of the defence in depth concept and in particular those topics including terminology that are often misinterpreted.

PREVENTION AND MITIGATION

Prevention and mitigation are terms widely used in nuclear safety ad they are mostly referred to accidents (prevention of accidents and mitigation of the consequences of accidents). With references to defence in depth, the essential means of each level prevent the need for activation of the essential means of the following level and, at the same time, they mitigate the consequences of the failure of the previous ones. Level 1, being the first level, has a predominant preventive function and Level 5, being the last, has only a mitigative function.

Mitigation is interpreted as controlling or stopping the evolution of an event sequence so that the consequences on the plant and the environment are kept under control and hopefully below acceptable limits. At any stage of a given event sequence,

theoretically evolving from an initiating event to very severe conditions, prevention refers to what has not happened yet and mitigation to what has already happened. Considering for example the level 2 of defence in depth, the essential means are active to control or mitigating the consequences of an AOO while, at the same time, preventing the escalation of the AOO into an accident. Similar considerations can be made (*mutatis mutandis)* for Level 3 and Level 4.

COMPARISON OF THE IAEA AND WENRA APPROACHES TO DEFENCE IN DEPTH

IAEA approach

The concept of Defence in Depth as used in the IAEA Safety Standards in mainly based on INSAG-10 and SSR-2/1 and it is integrated with additional information for its practical implementation.

Below is a description of the purpose of each level of defence and the means to accomplish it. This description is taken directly from Section 2 of SSR-2/1. Some additional considerations have been added at the end of the description of each level.

(1) The purpose of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety. This leads to requirements that the plant be soundly and conservatively sited, designed, constructed, maintained and operated in accordance with quality management and appropriate and proven engineering practices. To meet these objectives, careful attention is paid to the selection of appropriate design codes and materials, and to the quality control of the manufacture of components and construction of the plant, as well as to its commissioning. Design options that reduce the potential for internal hazards contribute to the prevention of accidents at this level of defence. Attention is also paid to the processes and procedures involved in design, manufacture, construction and in-service inspection, maintenance and testing, to the ease of access for these activities, and to the way the plant is operated and to how operating experience is utilized. This process is supported by a detailed analysis that determines the requirements for operation and maintenance of the plant and the requirements for quality management for operational and maintenance practices.

The essential means required to meet the objective of the Level 1 of defence are, as indicated in the table above, a conservative design and high quality in construction and operation. More generally this level includes all provisions implemented to avoid challenging the subsequent levels by preventing equipment failure, system malfunctioning and human errors.

The need of an effective control system is not explicitly mentioned in the description above. The control system has the functions to maintain the values of the process parameters inside the normal operation range and to prevent abnormal operations. Although the control system is necessary to operate the plant and it should be included in Level 1 of defence in depth, INSAG-10 includes this system in Level 2. It should also be noticed that malfunctioning of the control system are among the main causes of AOOs, therefore this system and the systems designed to control AOOs should not be included in the same level of defence.

The reliability of the equipment of level 1 of defence in depth is expected to be such that frequency of occurrence of an AOO is less than 1/reactor/year and the frequency of occurrence of accident caused by equipment failure less than 10-2 /reactor•year. Accident not considered for the design of the plant should have a likelihood very low.

(2) *The purpose of the second level of defence is to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions. This is in recognition of the fact that postulated initiating events are likely to occur over the operating lifetime of a nuclear power plant, despite the care taken to prevent them. This s second level of defence necessitates the provision of specific systems and features in the design, the confirmation of their effectiveness through safety analysis, and the establishment of operating procedures to prevent such initiating events, or else to minimize their consequences, and to return the plant to a safe state.*

The intervention of the limitation or protection system may be necessary for the shutdown of the reactor power to control some postulated abnormal conditions (e.g. Anticipated Operational Occurrences). Modern designs avail on a limitation system that reacts upon some perturbations of the normal operation regime that cannot be handled by the control systems, preventing or delaying a reactor trip by quickly reducing the power of the reactor and providing signals to key plant systems and components to stabilize the plant. For some reactor designs, the protection system is a safety system that also has relevant functions in Level 3 for the actuaction of safety systems. Also a typical anticipated operational occurrence like the loss of off-site power requires either the house-load operation or the intervention of the onsite emergency power that has also relevant functions in level 3. This shows specific cases of difficulty to implement independence between Level 2 and Level 3 of defence in depth (see para 4.13a of SSR-2/1 reported below).

Equipment of level 2 of defence in depth is aimed at reducing the number of challenges to the DiD level 3. Their reliability is expected to be such that level 3 of defence in depth is not necessary to intervene with a frequency higher than 10^{-2}/reactor•year.

(3) *For the third level of defence, it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences or postulated initiating events might not be controlled at a preceding level and that an accident could develop. In the design of the plant, such accidents are postulated to occur. This leads to the requirement that inherent and/or engineered safety features, safety systems and procedures be provided that are capable of preventing damage to the reactor core or significant off-site releases and returning the plant to a safe state.*

In the current formulation of defence in depth Level 3 involves only with the postulated set of Design Basis Accidents. The essential means of achieving the objective of Level 3 are the Safety Systems and the accident procedures for DBAs. The safety systems are designed with a set of conservative, prescriptive rules and criteria (e.g. application of the single failure criterion) which provide high confidence in their success to meet the relevant acceptance criteria and safety limits.

The reliability of equipment of level 3 of defence in depth is expected to be such that the probability of failure per demand of level 3 is, at least, in the range of 10^{-3} - 10^{-4}).

(4) *The purpose of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth. This is achieved by preventing the progression of the accident and mitigating the consequences of a severe accident. The safety objective in the case of a severe accident is that only protective measures that are limited in terms of times and areas of application would be necessary and that off-site contamination would be avoided. Sequences that lead to large or early radioactive releases[5] are required to be 'practically eliminated'.*

In the current formulation Level 4 deals with the control of all postulated multiple failures with and without core melt. The essential means of achieving the objective of Level 4 include safety features for DECs and accident management procedures and guidelines.

DECs can be generated by multiple failures of safety systems either in normal operation (e.g. loss of RHR during shutdown) or following an AOO or a DBA. In the IAEA approach Level 4 includes DEC with and without core melt. The failure of level 2 can lead directly to DECs without core melt while the failure of level 3 can also lead to DECs with core melt. The two major objectives of Level 4 are: (a) to prevent DECs without core melt from progressing to core melt situations and (b) to mitigate the consequences of DECs with core melt.
In this sense the Level 4 of defence in depth can be considered as formed by two sub levels indicated in this publication as 4a and 4b.
Level 4a is mainly aimed at ensuring that, whatever the complex sequence based on internal events considered in the design, the risk that successive failure of the levels of DiD may lead to a core melt (Level 4b) is consistent with the targets defined in Table 1. Therefore Level 4a is further enhancing the prevention of core melt implemented by the other levels of DiD.

It is important to notice that since the failure of safety systems following an AOO can lead directly to a DEC, it is possible that the Level 3 of defence in depth is bypassed (e.g. ATWS, SBO).

Unlike the safety systems for DBAs the safety features for DECs are not required to be designed to meet the single failure criterion.

Equipment belonging to DiD level 4b are implemented to limit the radiological releases in case of core melt and are aimed at maintaining the containment functions.

Accident management should be understood as encompassing both hardware and procedures necessary to maintain the radiological release as low as possible in any accident. In particular SSR-2/1 requires (Req. 67) the implementation of a Technical Support Centre (TSC) to provide technical support to the operation staff during accident conditions. Given its function, the TSC is an important feature for the Level 4 of the defence in depth.

[5] 'Large radioactive release': a release for which off-site protective measures limited in terms of times and areas of application are insufficient to protect people and the environment. 'Early radioactive release': release for which off-site protective measures are necessary but are unlikely to be fully effective in due time.

The use of non-permanent equipment (see Section 11) is also a measure to reinforce the fourth level of defence and for dealing with conditions beyond the DECs.

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

According to the IAEA Safety Standard GSR Part 7 [8], the on-site emergency response facilities (which are separated from the control room and the supplementary control room) include the technical support centre, the operational support centre (OSC) and the emergency centre (EC). While the TSC is considered as an essential mean of Level 4 of defence in depth, the operational support centre and the emergency centre are essential means of Level 5 of defence in depth.

4.13 a The levels of defence in depth shall be independent as far as practicable to avoid a failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting of fuel) shall be as far as is practicable independent of safety systems.

The issue of the independence of the different levels of defence in depth is addressed in detail in Section 6 of this publication.

The table below, which is based on the original table of INSAG-10, presents the current approach as described in SSR-2/1 and includes the considerations made above. The main difference with the original table of INSAG-10 is represented by the introduction of the Design Extension Conditions (DECs). This fact, without impairing the general approach, has requested a slight elaboration of the fourth level of defence in depth and minor changes in the wording of Level 3. The column of the essential means has been split in two to better indicate essential means related to design and those related to operation.

Level of defence	**Objective**	**Essential design means**	**Essential operational means**
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction of normal operation systems, including monitoring and control systems	Operational rules and normal operating procedures
Level 2	Control of abnormal operation and detection of failures	Limiting and protection systems and other surveillance features	Abnormal operating procedures/emergency operating procedures
Level 3	Control of design basis accidents (postulated single initiating events)	Engineered safety features (safety systems)	Emergency operating procedures
Level 4	Control of design extension conditions (postulated multiple failures events) including prevention of accident progression and mitigation of the	Safety features for design extension conditions. Technical Support Centre	Complementary emergency operating procedures/ severe accident management

	consequences of severe accidents		guidelines
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	On-site and off-site emergency response facilities	On-site and off-site emergency plans

WENRA approach

The WENRA approach to defence in depth for new nuclear power plants, that was developed by the Reactor Harmonization Working Group (RHWG), is largely based on the IAEA approach and in particular on INSAG-10 [7] and SSR-2/1. Reference [5] provides a very good description of the WENRA approach including historical background and development.

RHGWG states: *"For new reactor designs, there is a clear expectation to address in the original design what was often "beyond design" for the previous generation of reactors, such as multiple failure events and core melt accidents, called Design Extension Conditions in IAEA SSR-2/1. This is a major evolution in the range of situations considered in the initial design to prevent accidents, control them and mitigate their consequences, and in the corresponding design features of the plant. It implies that the meaning of "beyond design basis accident" is not the same for existing reactors and for new reactors. Several scenarios that are considered beyond design basis for most existing reactors are now included from the beginning in the design for new reactors (postulated multiple failure events and core melt accidents)".*

The approach to defence in depth has been slightly refined to include in the design of new plants the consideration of accident sequences that are considered as "beyond design" for existing plants, such as multiple failure events and core melt accidents. This new approach is presented in the table below.

Levels of defence in depth	Objective	Essential means	Radiological consequences	Associated plant condition categories
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation, control of main plant parameters inside defined limits	No off-site radiological impact (bounded by regulatory operating limits for discharge)	Normal operation
Level 2	Control of abnormal operation and failures	Control and limiting systems and other surveillance features		Anticipated operational occurrences
Level 3 (1) 3.a	Control of accident to limit radiological releases and prevent escalation to core melt conditions (2)	Reactor protection system, safety systems, accident procedures	No off-site radiological impact or only minor radiological impact (4)	Postulated single initiating events
3.b		Additional safety features(3), accident procedures		Postulated multiple failure events
Level 4	Control of accidents with core melt to limit off-site releases	Complementary safety features(3) to mitigate core melt, Management of accidents with core melt (severe accidents)	Off-site radiological impact may imply limited protective measures in area and time	Postulated core melt accidents (short and long term)
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	Off-site emergency response Intervention levels	Off site radiological impact necessitating protective measures(5)	-

The refinements of level 3 and 4, according to the RHWG, are justified by the following considerations:

1) The phenomena involved in accidents with core/fuel melt (severe accidents) differ radically from those which do not involve a core melt. Therefore core melt accidents should be treated on a specific level of Defence-in-Depth.
2) For new reactors, design features that aim at preventing a core melt condition and that are credited in the safety demonstration should not belong to the same level of defence as the design features that aim at controlling a core melt accident that was not prevented.
3) The single initiating events and multiple failure events are two complementary approaches that share the same objective: controlling accidents to prevent their escalation to core melt conditions.

For the reasons described above it has been proposed to treat the multiple failure events as part of the 3rd level of DiD, but with a clear distinction between means and conditions (sub-levels 3.a and 3.b).

For level 3.b, analysis methods and boundary conditions, design and safety assessment rules may be developed according to a graded approach, also based on

probabilistic insights. Best estimate methodology and less stringent rules than for level 3.a may be applied if appropriately justified.

In item 1 above, the expression "core/fuel melt" seems to address the melting of the fuel in the core and the fuel in the spent fuel pool, while the last sentence of the same item refers only to "core melt". However, the core melt condition is postulated and dealt with by the essential means of the Level 4 of the defence in depth. The melting of the irradiated fuel outside of the containment cannot be postulated (if the spent fuel pool is outside the containment) and for this reason it should be practically eliminated. In this case the essential means of the fourth level of defence in depth are only aimed at preventing the fuel melting.

Practical implications of each approach

The two approaches are very similar and, at this level of generality, their implementation does not seem to have any substantial impact on the actual design provided that sub levels 4a and 4b are considered in IAEA approach, with adequate independence requirements.

The differences between the IAEA and WENRA approaches for new designs are mainly formal and concern the way the multiple failures considered in the design are allocated in the levels of defence in depth.

The IAEA in SSR-2/1 has chosen to group all the multiple failure sequences (with and without core melt) in a single category termed Design Extension Conditions and assuming that the control and mitigation of these conditions is performed by the fourth level of defence in depth. This implies that the essential means (Safety features for DECs) of Level 4 cover a broad set of equipment designed to cope with rather different situations including SBO, ATWS and those generated by core melt phenomena and possibly other multiple failure events selected to be included in DECs.
Additionally, since in SSR-2/1, the single failure criterion is required to be applied to each safety group, the application of this criterion is not required in a prescriptive manner for the safety features for DEC because they are not considered as part of the safety group[6]. It holds, however, the requirement that the reliability of any equipment important to safety shall be commensurate to its significance to safety.

The WENRA approach expects a sufficient degree of redundancy of active components of systems designed to cope with multiple failure events to reach an adequate level of reliability. In case of accidents with core melt WENRA expects redundancy for active parts to ensure the integrity of the containment.

In the WENRA approach the multiple failure sequences without core melt are included in Level 3b and for these conditions is required that the radiological consequences meet the same qualitative criteria requested for the Design Basis Accidents. This may appear as a more conservative approach than the IAEA

6 **Safety group:** The assembly of equipment designated to perform all actions required for a particular *postulated initiating event* to ensure that the *limits* specified in the *design basis* for *anticipated operational occurrences* and *design basis accidents* are not exceeded.

approach. However, since the current radiological acceptance criteria in WENRA and IAEA are still qualitative, it is expected that their quantitative definition and practical implementation will result in almost complete convergence of the two approaches on the requirements for the design of the features for multiple failure events, taking into account that it makes sense to expect lower radiological releases for accidents without core melt than for accidents with core melt. The criteria proposed in Appendix 1to this TECDOC for Level 4 of defence in depth already comply with this expectation.

5. DEFENCE IN DEPTH FOR THE IRRADIATED FUEL STORAGE

The considerations below are an attempt to show how the defence in depth approach can be applied to the design of the storage systems for irradiated fuel where the fuel is contained in a pool of water (spent fuel pool). In some existing LWR designs the irradiated fuel pool is hosted in a building located outside the containment.

The storage systems need to fulfil at all times, for the irradiated fuel, the three fundamental safety functions:

- maintaining subcriticality of the fuel;
- removal of decay heat from irradiated fuel;
- confinement of radioactive substances.

In addition they need to shield the radiation of the fuel elements to meet the limits for occupational radiation doses. To this aim a sufficient level of water over the top of the fuel elements is maintained, thus providing also passive mean to cool the fuel for a long period of time.

Although the irradiated fuel pool is to large extent independent from the reactor, the same design methodology based on a deterministic approach supplemented by probabilistic evaluations and applying a graded approach, can be used for the design and safety verification of the irradiated fuel pool systems. This implies that operational states (NO, AOO) and accident conditions (DBAs and DECs) need to be identified to establish the design bases for the equipment of the irradiated fuel storage. Design provisions and measures have to be implemented to eliminate possibilities for high radiation doses and early or large radiological release. The safety features (essential means) for each level of defence in depth should also be specified.

Normal operation

In all conditions considered for the design, including normal operation, the subcriticality is ensured by the physical layout (geometry of the positioning of the fuel elements) complemented, in some cases, by neutron absorbers (in solid bars or solved in water). The removal of heat from the fuel is ensured by the submersion under water that is cooled by a dedicated cooling system. The confinement of radioactive gases released from the fuel is ensured by the building isolation and the ventilation system that keeps the pressure in the building slightly below the atmospheric pressure.
Typical measures of the first level of defence in depth (high quality, conservative design, maintenance, cooling and purification systems, etc.) ensure the satisfactory operation and the prevention of failures and abnormal conditions.

Anticipated Operational Occurrences

Credible failures of equipment or systems, and abnormal operations, both within and outside the storage facility, have to be postulated in order to put in place adequate protective measures to ensure that the consequences will not exceed established criteria. Examples of anticipated operational occurrences are:
- loss of off-site power (LOOP)
- malfunction of decay heat removal system[7];
- leaking of water of the pool
- malfunctioning of the ventilation system.

Design Basis Accidents

The concept of design basis accidents can be applied to the design of systems for the spent fuel storage but some considerations are necessary. In most of the current designs there are not standby systems (safety systems) to deal with accident situations (third level of defence in depth). There are, however, systems that run during normal operations such as the heat removal system and the ventilation systems that also have the capability to deal with some postulated abnormal conditions. These systems are classified according to their more demanding safety functions.

The heat removal system is generally designed, as the plant safety systems, applying the concept of redundancy to satisfy the single failure criterion and is emergency supplied by the on-site AC power system. Currently an additional dedicated system to deal with the loss of the main cooling is not required. This is justified by the long time necessary to uncover the top of the fuel in case of loss of cooling because of the large thermal inertia of the water in the pool. In this sense, the essential means of the third level of defence in depth are the procedures to recover fuel cooling and to keep the fuel always submerged in water. The design basis of spent fuel cooling system does not include any design basis accident because this system is not designed to mitigate any specific accident caused by the failure(s) of other systems. However, given the importance of its function, the spent fuel cooling system is designed with redundant trains to meet the single failure criterion.

The ventilation system has the capability to remove and retain the radioactivity released from the fuel assuming that some rods can be damaged, for example, by dropping a fuel element during the fuel handling. The ventilation system has also the capability to remove the steam produced in case of prolonged loss of cooling. The dropped of a fuel element and the loss of cooling can be considered as design basis accidents for the ventilation system.

Design Extension Conditions

A multiple failure sequence considered as DEC is the station blackout. Since the electric power to the storage systems is provided by the same sources which provide power to other systems of the NPP, the SBO at the NPP also affects the storage

7 The total loss of decay heat removal is a DEC because can only result from multiple failures in the cooling system, SBO or loss of the cooling chain CCWS and ESWS

systems but the time allowed for the recovery of the power is much longer. The safety features to deal with the SBO at the NPP are imposed by the reactor and there are not additional dedicated safety features required by the storage system. In case of SBO the essential means of the fourth level of defence for the reactor provide protection also to the storage system as long as the electric distribution system allows for appropriate connections.

For a number of current NPPs, the loss of the reactor emergency cooling chain also affects the cooling of the spent fuel pool. In this case the event should be considered as a DEC also for the spent fuel pool cooling.

There are some designs that include an additional independent cooling system to deal with the complete loss of the main cooling system. In this case the event is considered as a DEC (multiple failures of the main cooling system) and the additional cooling system is considered as a feature of the fourth level of defence in depth.

For designs where the irradiated fuel is stored outside the containment, all conditions that could potentially lead to fuel melt have to be practically eliminated (there are no DECs with fuel melt to be considered) and for this reason these designs do not include safety features for the mitigation of fuel melting accidents. It is the objective of the safety analysis to demonstrate that the provisions implemented are sufficiently effective to exclude the need for means for the mitigation of fuel melt events.

Req. 6.68 of SSR-2/1 does not make difference between spent fuel pools outside or inside the containment and requires the prevention of fuel uncover, so as to practically eliminate the possibility of early or large releases.

6. INDEPENDENCE OF LEVELS OF DEFENCE IN DEPTH

Paragraph 3.31 of the IAEA Safety Fundamentals [2] states:

"The primary means of preventing and mitigating the consequences of accidents is 'defence in depth'. Defence in depth 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 people or to the environment. ..."

The paragraph above stresses two main aspects of defence in depth: the multiplicity of level of protection and the independence of these levels. These two aspects have been investigated at the IAEA and translated into safety requirements in SSR-2/1 taking also into consideration the lessons learnt from Fukushima Daiichi accident. The correct implementation of the requirements implies that the multiplicity of the levels of defence should not be a justification to weaken the efficiency of some levels relying on the efficacy of others. In a sound and balanced design each level of defence should be characterized by a reliability commensurate to its safety significance.

Regarding the independence, it should be recognized that the full independence of the levels of defence in depth cannot be reached, due to several constraints, such as the common exposure to external hazards, the unavoidable sharing of some SSCs, e.g. the containment or the control room and ultimately the operating crew. Therefore since

the independence of the levels of DiD is a goal that cannot be achieved, it would be more appropriate to speak about reducing the degree of dependence between the levels of defence in depth, but the term independence of DiD levels is commonly spread in the international community, including documents of INSAG, IAEA, WENRA, NEA and others. Therefore, the interpretation ad use the term "independence of the levels of DiD" needs be understood as the "degree of independence", which should be the highest possible.

Multiple consecutive levels of protection achieve the objective of defence in depth if, following the failure of one level of defence, the subsequent level would not also fail for the same cause (full dependency). For this reason, SSCs serving different levels remains one of the key issues to ensure the overall efficiency of the defence in depth concept. To which extent the independence of different levels of defence is practically achievable and acceptable still needs to be clarified.

Requirement 7 of SSR-2/1 on application of defence in depth states: "(…). The levels of defence in depth shall be independent as far as is practicable."

Following the review of SSR-2/1 to incorporate the lessons learned from the accident of Fukushima in 2011, the following requirement has been added:

4.13a: "*The levels of defence in depth shall be independent as far as practicable to avoid a failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting of fuel) shall be as far as is practicable independent of safety systems*".

Factors that affect the independence of levels of defence

In preventing the occurrence of postulated initiating event and mitigating their consequences (should they occur) at different levels of the defence in depth, it is very important that safety provisions at the different levels are highly reliable.

In order to ensure very low frequencies of accident sequences resulting in severe accidents or external releases, it is necessary to ensure that the reliability of the levels of defence is not diminished by factors that compromise the independence of the levels of defence in depth. These factors, that should be avoided by design and complemented by adequate operational practices, are:

- The sharing of systems or parts of them for executing functions belonging to more than one level of defence in depth. Examples of this type of dependencies are the use emergency core cooling pumps for primary coolant make up or the use of common support systems or part of them for normal operation and PIEs. Examples can be found in power supply and component cooling water systems. It might be however not be always feasible to have different systems for different levels, such as different reactor scram systems for different levels.
- The exposure of SSCs to failures of a common origin other that the sharing of support systems. This includes the failure of redundant components due to internal or external hazards and other common cause failures.

PREVENTION OF COMMON CAUSE FAILURES

Requirement 24 of SSR-2/1 states that "*The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability*".

Common cause failures are relevant when they affect redundant equipment. Common cause failures affecting no redundant equipment are not specially significant, since it can be expected that their probability is lower than the probabilities of independent failures. For this reason the analysis of common cause failures is focused on redundant equipment, i.e. on equipment that need to fail for a given accident sequence to progress at some point.

In the first instance common cause failures can be considered between different redundancies of a system. Safety systems are designed in redundant manner as required by the application of the single failure criterion (SSR-2/1, Requirement 25). This is the most usual field of analysis of susceptibility to common cause failures. Common cause failures can be considered at the system level, subsystem level, or smaller system parts, e.g. isolation of a specific pipe section or the acquisition of some plant parameter by the instrumentation.

On the other hand common cause failures affecting components of different systems involved in an accident sequence should not be neglected. The common cause failures affecting equipment of different systems in an accident sequence jeopardize the independence of the levels of defence in depth.

There is not a unique understanding and use of the term "common cause" worldwide. Appendix 2 addresses the more general concept of dependent failures, from which common cause failures are a subset. Nowadays, the term common cause failure is not used to designate for instance the failure of several components in a system due to the failure of a support system, e.g. power supply. This would be considered a functional dependency. Appendix 2 provides some insights on the types of dependent failures, including common cause failures. It addresses also the root causes of common cause failures, the coupling mechanisms and defensive measures that are adequate for each of them.

Redundant equipment within a system are more exposed to commonalities in design, operational and maintenance practices. Other factors, such as hazards can affect several plant systems. Diversity has been broadly applied to the reactor protection system to ensure a very reliable generation of protection signals.

Safety systems have in general relied upon redundancy, functional independency, robust design and physical separation to ensure high reliability. Diversity has been usually a measure applied to reduce the likelihood of common cause failures between different levels of defence in depth, for instance turbine driven pumps (or isolation condenser) for AOOs in BWR designs and motor driven pumps in safety system, or a turbine driven pump in the auxiliary feedwater systems of PWRs with the view of potential SBO scenarios.

Functional independence between different levels of defence in depth is an aspect that cannot be taken for granted. It has been a frequent practice to share systems between different levels of defence.

In SSR-2/1 and its new revision for taking into account lessons learned from the Fukushima accident, the emphasis is being placed on reinforcing the independence between different levels of defence in depth and in particular between level 4 and the previous levels. Fully dedicated systems, i.e. functional independency, diversity, for instance on instrumentation, power supply or heat sink, as well as stronger safety margins and protection against external hazards, are among the measures to prevent common cause failure for stretching through different levels of defence in depth.

DESIGN FOR EFFECTIVE INDEPENDENCE OF LEVELS OF DEFENCE IN DEPTH

SSR-2/1 stresses the importance of the independence of different levels of defence in depth and requires that the independence is implemented as far as practicable.
As mentioned before, it is recognized that a full independence is not achievable because too many structures, systems and components have to serve more than one level of defence. A typical example is the containment that has relevant safety functions in different levels of defence and cannot reasonably be duplicated or triplicated. However, independence is essential where concurrent failures of two levels would lead to early or large releases with harmful effects to people or to the environment.

In general, to which extent the degree of independence of the levels of defence in depth should be achieved is still an open issue that requires a relevant effort to identify practical measures for a satisfactory implementation.

Some recommendations for the correct implementation of the Requirement 7: Application of Defence in Depth, of SSR-2/1, are given below.

General recommendations

- The successive means required for mitigating a given PIE should be identified;
- Two sets of consequential independent safety features are expected to be available to prevent the core melt for any PIE.
- Safety features specifically designed to mitigate the consequences of core melt accidents should be independent from those designed to prevent such accidents;
- Safety features for DEC, designed to back up SSCs implementing safety functions, should be independent from SSCs postulated as failed in the accident sequence;
- Independence between SSCs or safety features should be pursued through the identification of all dependencies and the elimination of the most significant ones.
- The safety analysis should demonstrate that the safety features intended to respond first are not jeopardized by the initiating event;

A detailed description of dependent failures and means for reducing their likelihood is included in Appendix 2.

Specific recommendations

- Vulnerabilities which could result in the total failure of the safety systems should be identified and, if any, combinations with PIE should be considered or postulated to assess if they could escalate to a core melt accident. Usually, for each combination analysed, if the consequences exceed those acceptable for Design Extension Conditions, separate, independent and diverse safety features (e.g. AC alternate power supply in case of the total loss of the standby diesel generators, or a separate and diverse decay heat removal chain, etc.) unlikely to fail for the same common cause are provided to strengthen the defence in depth and to prevent core melt.

- At least one design extension condition with core melt should be postulated and dedicated safety features should be implemented to mitigate the consequences. As a core melt accident would result from multiple failures of the safety systems (failure to mitigate design basis accidents), the equipment dedicated to mitigate the consequences of core melt accidents are expected to be separated and independent as far as reasonably practicable from the equipment designed for mitigating design basis accidents. Thus it is necessary to implement an effective independence between levels 3 and 4, and within level 4, between SSCs necessary to prevent progression to core melt (level 4a) and SSCs necessary to mitigate the consequences of a core melt accident (level 4b).

- Level 3 should be independent from levels 1 and 2 as far as reasonably practicable. To avoid challenging excessively level 4, the ability of the safety systems to perform their function should not be jeopardized by a postulated single initiating event, or by failures of systems designed for normal operation (level 1) and Anticipated Operational Occurrences (level 2). This includes also shared support systems between these levels. Multiple failures in these systems resulting to the total loss of a safety system can only be controlled by the independent safety features implemented in level 4 for the list of DECs considered in the design. Safety features in level 4 are however not required to meet the single failure criterion. All measures need to be taken to ensure the highest level of independence between safety features in levels 3 and 4.

- Level 2 should be independent from level 1 as far as reasonably practicable. Generally, Anticipated Operational Occurrences are controlled by non-safety systems and ultimately by the reactor trip system. So the reactor trip system shall be separated from operational systems, and its ability to perform its functions should not be jeopardized by a postulated single initiating event or by single equipment failure of systems designed for normal operation (level 1). Multiple failures resulting in the total loss of the reactor trip system are controlled by the diverse safety features implemented in level 4 (e.g. with DAS I&C system). Limitations systems (level 2) usually share components

with the control systems (level 1). A full independence of these systems might lead to excessive complexity that is not justified by the benefits to safety.

Independence of levels of defence in depth in relation to I&C systems

I&C systems have a relevant role for performing safety functions in all levels of defence in depth. The correspondence between the different functions and the level of defence in depth together with some recommendations to enhance independence of different levels are summarized below:

- Level 1. Belong to this level the functions necessary to operate the plant during normal operating modes and to maintain the main plant variables within the specified range.

- Level 2. Belong to this level the functions to prevent Anticipated Operational Occurrences from escalating into accident conditions. This level also includes the reactor trip function and the limitation functions. The limitation system is designed to control AOOs without activating the reactor trip as much as possible.
  Limitations functions (Level 2) should be separated from the operational I&C (Level 1) to the extent feasible. Separation may not be implemented where it would lead to increase significantly the number of data transfer between these two I&C systems (e.g. between I&C controls and limitations where the controlled equipment is the same).

- Level 3. Belong to this level the functions designed to automatically control Design Basis Accidents without exceeding acceptance criteria and functions designed to operate reliably the reactor to safe shutdown conditions after following a DBA.
  Initiation of reactor trips and safety systems should be processed in a separated and independent I&C system from the I&C systems used for operational states and the I&C systems used for Level 4.Provisions should be taken to ensure that failures of systems classified in a lower safety class will not prevent the reactor protection system from performing its intended functions.

- Level 4. Belong to this level the functions designed to prevent design extension conditions from escalating to core melt (back up functions necessary to prevent combinations of PIE with CCF in the I&C systems escalating to a core melt accident) and specific functions designed to mitigate the consequences of a core melt accident also belong to level 4.
  I&C system dedicated to the mitigation and monitoring of a core melt accident should be separated and independent from any other I&C systems. The independence of level 4b and level 3 requires the independence of their respective DC power sources

To reduce the volume of data to exchange and communications within I&C systems, in existing designs, some I&C functions may be performed by a single I&C system. That may be the case for some control and limitation functions, or with the Reactor Protection System which often processes both the reactor trips and the actuation of the

safety systems. In that case the physical separation is not implemented but the functions should be decoupled.

In I&C systems independence is intended to prevent the propagation of failures between redundant channels or from system to system and is achieved by implementing functional independence, communication independence and avoiding interconnections. If independence is not implemented, the data transfer shall be secured and the shared signals decoupled (e.g. Data transfer between the redundant channels of the Reactor Protection System are necessary for the voting logic). Physical separation is intended to prevent the effects of electromagnetic fields and common cause failures due to internal hazards.

Considerations on sensors

The efficacy of all four levels depends upon sensor response but this does not imply that all sensors must be independent or diverse. Nevertheless the independence between redundant trains of a safety system, and between systems assigned to different levels of defence in depth, should not be jeopardized by the sensors (e.g. redundant trains within a safety system should not share instrumentation).

The following considerations and recommendations apply:

- Generating back up protection signals should rely on independent and diverse sensors to not impair independence and diversity between the Reactor Protection System and the Diverse Actuation System (DAS) [8].

- Monitoring the key variables for the management of DBAs and DECs without core melt should also be possible using sensors different from those used to initiate the operation of the safety systems and DEC safety features respectively. To the extent possible sensors used for the protection and for the monitoring should not fail because of a common cause.

- Monitoring the key variables for the management of core melt accidents should be to the extent possible performed by dedicated sensors, and in particular it should not be dependent on the DC source used for DBA management. Sharing sensors with other DiD levels may be acceptable provided the sensors are qualified for the environmental conditions prevailing in case of a severe accident and an adequate number of redundant sensors are implemented with effective separation and independence. In this case the shared sensors should provide input to different I&C systems only through appropriate buffering and isolation devices. The I&C backup system (DAS) should be separated, independent and diverse from the Reactor Protection System.

- Sharing sensors between level 1, 2 and 3 may be acceptable provided an adequate number of redundant sensors are implemented with effective separation and independence. In this case the shared sensors should provide input to different I&C systems only through appropriate buffering and isolation devices.

[8] Annex III of the Safety Guide DS-431 "Design of Instrumentation and Control Systems for Nuclear Power Plants" addresses the topic and the current practices of Member States in detail.

- For the automatic actuation of safety systems or for the monitoring of plant parameters in accident conditions, it is a good practice to rely on different physical parameters to reduce the consequences of failure of sensors due to common causes.

Considerations on the use of diverse actuation system (DAS)

The demonstration that I&C systems using software or hardware description language (HDL) are error free is very difficult and often disputable. Therefore, for new plants it is common practice to postulate common cause failure in I&C systems that are using the same technology. The functions of the I&C systems necessary to cope with a failure of the Reactor Protection System are performed by an additional independent and diverse I&C system (DAS).

The design of the DAS is based on the analysis of the consequences of postulated CCFs that could prevent the initiation of mitigation actions. The analysis should consider the likelihood of the combinations of the CCF with PIEs, but usually, the complete failure of the software used for processing the protection signals is considered as the bounding case. In that case, only signals processed by different software can be credited in the analysis. If the consequences exceed the acceptance criteria established to prevent significant core damage, a backup signal that is not subjected to the same CCF, should be generated. Back up signals should also be such to prevent the initiating event from escalating to a core melt accident. In the estimate of the consequences, the plant response may be modelled with less conservatism than for DBA analyses.

7. RELIABILITY OF THE HEAT TRANSFER TO THE ULTIMATE HEAT SINK

The possible “loss of the ultimate heat sink” has been typically described as one of the important issues of the Fukushima accident that would require considerations for safety enhancement.

The IAEA safety glossary defines the UHS as: “A medium into which the transferred *residual heat* can always be accepted, even if all other means of removing the heat have been lost or are insufficient (This medium is normally a body of water or the atmosphere)”. Requirement 53 “Heat transfer to an ultimate het sink” of SSR-2/1 requires that the capability to transfer heat to an ultimate heat sink shall be ensured for all plant states. Requirement 70 “Heat transport systems” also addresses the need for removing the heat form systems and components that are required in operational states and accident conditions. Therefore, in this context the heat to be removed has to be understood as the decay heat in both the reactor core and the spent fuel, and the heat to be removed from a number of components important to safety in order to maintain their operability.

Although mechanisms have been identified for the loss of the UHS in a strict sense, including for instance the clogging of the plant water intake filters, in a broad sense,

the loss of the UHS is understood not only as the loss of the UHS itself but also as the failure of the SSCs that transfer the heat to the sink.

Depending on the particular plant design, such SSCs for transferring heat to the UHS typically include a chain of cooling systems generally named as cooling water and service water systems. For the removal of heat from items important to safety a common denomination is essential service water system (ESWS) for an open cooling circuit transferring the heat to the UHS and component cooling water system (CCWS) for an intermediate closed loop system, which transfers heat from the majority of the items important to safety to the ESWS in order to reduce the probability of radiological releases to the environment. Some designs however, don't avail on the CCWS as intermediate closed loop. This is for instance the case of many operating BWRs. Some plant designs have different heat transfer systems for items important to safety than for the rest. If this is not the case, Requirement 70 of SSR 2/1 also requires that the isolation of the cooling circuits serving items that are not essential for safety has to be ensured.

Components typically cooled by the CCWS in existing PWRs are: the RHR heat exchangers, the spent fuel pool water cooling system, containment systems (e.g. fan-coolers), electrical pump motors of safety systems, HVAC systems of safety important areas, as well as the thermal barriers of the main coolant pump seals and the non-regenerative heat exchanger of the let-down line of the chemical and volume control system (CVCS) of the Reactor coolant system. The ESWS in typical PWRs cools the heat exchangers of the CCWS and some additional components such as the Diesel Generators.

It is common in BWR designs, that cooling functions of items important to safety are accomplished directly by the ESWS without an intermediate cooling circuit in many instances. It has to be remarked however, that these are common examples in existing designs but that many plants can deviate in several aspects from the examples. The very often discussed use of air cooled Diesel Generators in some units of the Fukushima Daiichi plant is just one case. CCWS and ESWS are system denominations used in the following for systems accomplishing the functions just described, although other names are used for similar systems in specific reactor designs.

At power operation the main heat sink is the condenser and in shutdown conditions the heat can also be transfer to the atmosphere through steam relief or safety valves in the PWRs, but even in those situations the CCWS and the ESWS continue to be the mechanism to remove heat from SSCs important to safety.

The loss of CCWS or ESWS seems to be a more credible mechanism for the failure of heat transfer in shutdown conditions to the UHS, rather than the loss of UHS itself. Due to the direct contact of the intake structure of the ESWS in some designs with very large bodies of water, e.g. rivers or seas, some components and structures of the ESWS are more exposed than others to the impact of external hazards (e.g. tsunamis) as it was experienced in the Fukushima accident. The reinforced safety requirements for the heat transfer to the UHS calls for the provision of an alternative UHS or a

different access to it[9]. This means on one hand to ensure the as appropriate margins in the design of CCWS and ESWS, and in particular for the parts of the ESWS interfacing with the UHS, to ensure that external hazards that affect the plant through the UHS, e.g. tsunamis or external flooding, cannot render the ESWS unavailable.

Where tsunamis are a hazard to be considered, a temporary withdraw of sea waters before the arrival of tsunami waves is also a phenomenon to be considered in the design of the water intake for the ESW. In addition, pipe failures of a system like the ESWS in case of an earthquake, bear the potential for internal flooding of important plant areas. Other external hazards potentially affecting the UHS are tornados, liquefaction of the soil and sandstorms. When is not practical to reinforce this part of the ESWS, the alternative solution considered in SSR 2/1 would mean an additional branch of the ESWS that would allow a different and protected access to the UHS or the connection of the ESWS to a different UHS. In most cases, the alternate UHS would be a closed water repository and water-air cooling devices of sufficient cooling capacity and designed with appropriate seismic margins. Such a repository would be free from the impact of external hazards except from earthquakes. The installation of an alternative UHS access or an alternative UHS entails design provisions in the ESWS to operate safely using different access points or UHSs. It could be possible to limit the capacity of the alternative UHS to the functional demands of the PIEs that could be caused by the external hazards. Thus for example the alternate UHS could be designed for the heat transfer rates associated with an AOO caused by an external flooding but not necessarily with heat transfer rates required after a design basis accident.

Due to all these reasons, the design bases of SSCs accomplishing the heat transfer to the UHS need to be designed with sufficient margins against postulated external hazards and with high levels of reliability. Reliability can be ensured by a number of safety provisions, including high quality, redundancy, diversity, physical separation, etc. as appropriate. It is important to notice that also the reliability of the ECCS and other safety systems that depend on the heat transfer to the UHS will be always limited by the reliability of the heat transfer systems.

From the typical list of equipment serviced by CCWS or ESWS, it is evident that the loss of one of these systems would very likely lead to a PIE and render inoperable SSCs that would be necessary to respond to the initiating event at levels 2 and eventually 3 of DiD. Thus for instance the failure of CCWS, forces a reactor shutdown as result of the failure of the CVCS (malfunction of the non-recuperative heat exchanger in the discharge line) and loss of cooling of the MCP thermal barriers. In spite of the resistance of the of the MCP seal and the long thermal inertia in plant SSCSs, the loss of HVAC for rooms and sensitive I&C or electrical equipment together with the loss of spent fuel cooling and the unavailability of ECCS equipment could eventually result in design extension conditions. The failure of the ESWS could result in similar consequences. Therefore, such common designs of ESWS and CCWS in NPP in operation result in a strong functional dependence between systems

[9] 6.19b: The heat transfer function shall be fulfilled for levels of natural hazards more severe than those selected for the design basis. This may require the use of a different ultimate heat sink or different access to the ultimate heat sink.

required at various levels of defence in depth. For the newest generations of LWRs, it can be expected that the functional dependences introduced by heat transfer systems to the UHS are not so strong. However, the failures of CCWS or ESWS (or systems fulfilling the same functions) are flagged out for their failures to be taken into account as DEC scenarios considered in the design.

The designer should analyse the impact of the functional dependencies introduced by these cooling systems to decide on the need of specific safety features for DEC or to justify that the plant is safe enough to ensure that systems equivalent to CCWS or ESWS are enough to transfer the heat from the fuel and the containment SSCs even in case of severe accidents.

Should the analysis conclude that this scenario is relevant, the safety features to back up these safety systems that would be included in the design would need to be necessarily independent from the systems to remove residual heat used at the 3rd level of defence. This may include the need for an alternate UHS or connecting point as being currently required in SSR2/1. Also, in the light of the foreseeable impact of external hazards on plant through the cooling function, the design should consider the requirement of high safety margins at least for some components of the heat removal systems, to ensure that the safety function can be maintained even in case of extreme external hazards.

8. DESIGN MARGINS AND CLIFF-EDGE EFFECTS

In SSR-2/1, the need to include margins in the design is addressed in the following requirements:

Requirement 7, item 4.11: (b) *The design shall be conservative, and the construction shall be of high quality, so as to provide assurance that failures and deviations from normal operation are minimized, that accidents are prevented as far as is practicable and that a small deviation in a plant parameter does not lead to a cliff edge effect.*

Requirement 17, item 5.21a: *The design of the plant shall provide for an adequate margin to protect items ultimately necessary to prevent large or early radioactive releases in the event of levels of natural hazards exceeding those to be considered for design taking into account the site hazard evaluation.*

SSR-2/1 also requires that the existence and adequacy of the different margins is proved in the safety assessment of the plant:

Requirement 42, item 5.73: *The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and that adequate margins are available to avoid cliff edge effects and large or early radioactive releases.*

In this section the concepts “cliff-edge effect” and “design margin” are elaborated to provide a sound interpretation of the requirements above. Both terms are closely linked, as sufficient margins will contribute to the robustness of the design and prevent cliff-edge effects.

DESIGN MARGINS[10]

In the IAEA-TECDOC-1332 [9], the safety margin is defined as:

The difference or ratio in physical units between the limiting value of an assigned parameter the surpassing of which leads to the failure of a system or component, and the actual value of that parameter in the plant.

In this TECDOC safety margin is used according to this definition and the terms “margins”, “safety margins” and ”design margins” are used as synonyms.

As the concept of “design margin” is frequently used in the IAEA Safety Standards, this TECDOC provides a basis for a common understanding of the meaning of the term and the purpose of using the concept of margin for the design of new NPPs as a measure to prevent the occurrence of cliff-edge effects.

Historically margins were first requested to demonstrate that the regulatory dose limits were met with a high level of confidence. This implied the use of conservative models, penalizing rules and plant parameters to make sure that the objective was met despite uncertainties in the modelling of the plant response and in the performances of the equipment. In particular, the demonstration of design margins was requested by the Regulatory Body for the analyses of the Design Basis Accidents.

The request to fulfil a number of engineering decoupling criteria (or acceptance criteria) primarily to ensure the integrity of the confinement barriers for different plant states (e.g. low limit for DNBR, upper limit for the cladding temperature, or upper pressure limit for the containment, etc.), also implicitly provided additional margins.

This approach was recognized by the Regulatory Bodies as a good practice to fulfil the concept of “conservative design” for safety systems. Later, design margins were explicitly requested to demonstrate the absence of cliff edge effects (see below).

Adopting margins in the design of a NPP is now a common practice to improve the robustness of the design and providing an effective mean to deal with uncertainties. However, the extension of the design basis with the introduction of DECs has introduced new elements that need to be addressed.

The Fukushima Daiichi accident has reinforced the importance of the effects of external events and, because of the uncertainties associated with their determination,

[10] Detailed discussions on margins for existing reactors are available in documents from IAEA [9] or OECD/NEA [10].

also the importance of adequate design margins to cope even with events of magnitude exceeding the design basis[11].

Design margins for design basis accidents

The Design Basis Accidents are used as boundary conditions to establish the design bases of the safety systems following a conservative approach.

DBA conditions are calculated taking into account the less favourable initial conditions and equipment performances, and taking into account the single failure affecting the most the global performance of the safety system.

With regard to the design of structures and components, margins result from both the methodology followed to define the loading conditions and compliance with the stress limits defined by the design/manufacturing codes. The methodology to define loading conditions is similar to that used for calculating DBA conditions. Meeting the stress limits established by proven codes is generally a proof for justifying the structural integrity in the different plant states. This proof is generally supplemented by some tests to justify the operability of equipment.

Uncertainties are also determined by applying a conservative approach. The possibility of cliff-edge effects need to be investigated and necessary margins have to be added to increase the capability of the SSCs. In addition, a design margin could be added by the designer to cope with possible changes during the lifetime of the NPP (e.g. ageing).

Thus, the *expected capability* of the safety systems and other items important to safety that are necessary to control design basis accidents consists of:

- conservatively *calculated capability* to cope with design basis accidents;
- an allowance for uncertainties in calculations and phenomena determined conservatively;
- an allowance for possible cliff-edge effects near the conditions generated by the design basis accidents;
- an optional design reserve.

Consequently, the margin can be understood as the difference between the calculated and the expected capability.

It has to be mentioned, that the *achievable capability* is usually even higher than the *expected capability*, because additional margins are practically introduced by the design and manufacturing process. For example, the wall thicknesses of chosen raw materials are slightly higher than the calculated necessary thickness. However, this kind of margin is not credited in the safety demonstration.

Design margins for design extension conditions

[11] Section 10 provides an interpretation of the SSR-2/1 requirements for the design for external hazards.

Margins of equipment for DECs are expected to be smaller than those existing for DBA conditions.

According to SSR-2/1 Requirement 20, the analyses of the design extension conditions may be performed using more realistic assumptions. Furthermore, meeting the single failure criterion is not required.

It is proposed, that in the design of SSCs for DECs, the loads have to be defined in a similar way as for DBA, but using a best estimate approach for determining the accident scenario and the environmental conditions. Values of acceptable behaviour limits justifying the integrity or operability of SSCs may be less conservative than those used for DBAs.

With regard to the design margins, there is a substantial difference between design extension conditions without core melt and design extension condition with core melt. Although SSR-2/1 does not make any difference between the two some consideration are relevant. For DECs without core melt the uncertainties are similar to those for DBAs, while for_DECs with core melt, the uncertainties are larger than those for DBAs. In both cases margins can be based on the best estimate approach.

CLIFF-EDGE EFFECTS

The term cliff-edge-effect was intensively stressed after the accident at the Fukushima Daiichi NPP. However, no common unique understanding of the term is available. This TECDOC provides a definition of the term for an adequate interpretation of the requirements of SSR-2/1.

The definition of cliff-edge effect in the IAEA Glossary is:

In a nuclear power plant, an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another (not need to change the plant status but the status of SSCs)following a small deviation in a plant? parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.

WENRA [5] has proposed a similar, more synthetic definition:

A cliff edge effect happens where a small change in a parameter leads to a disproportionate increase in consequences.

Hence, cliff edge effects imply consequences of high relevance following a small deviation in a "parameter" [12].The worst case would have a large release as the consequence. Other cliff edge effects would be the failure of a barrier or the occurrence of a severe accident. A physical barrier could fail if the safety functions protecting the barrier fail as a result of the change in the input parameter.

[12] The term plant parameter in the IAEA or the WENRA definitions of cliff edge effect, need to be interpreted in abroad sense, as any plant physical variable, design aspect, equipment condition, magnitude of a hazard, etc. that can influence equipment or plant performance.

Typical examples could be:

- The failure of the containment because of hydrogen detonation
- Earthquake causing a LOCA (typical)
- External hazards (flooding) failing safety systems

The goal of the safety assessment is to prove that there are adequate margins to avoid cliff edge effects. For this purpose, it is not always necessary to determine the magnitude of the deviation of the value of the parameter that could eventually lead to a cliff-edge effect.

9. THE CONCEPT OF PRACTICAL ELIMINATION

INTERPRETATION OF THE CONCEPT

The term "practically eliminated was originally introduced in the IAEA Safety Guide NS-G-1.10 which deals with the design of containment systems and it was published in 2004. It is defined as: "*the 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 degree of confidence to be extremely unlikely to arise"*.

The *"certain conditions"* to be addressed include hypothetical accident sequences that could lead to large radioactive releases due to early containment failure than cannot be mitigated with implementation of reasonable technical means.

The analysis of the definition points at two options for demonstration of different nature, the first of a deterministic nature, the physical impossibility, and the second involving probabilistic judgement, to be more specific, that the probability is very low (extremely unlikely), and the degree of confidence of the probability estimate is very high. The degree of confidence can be characterised by a confidence interval or other statistical measure of uncertainty. A probabilistic demonstration in these terms is however not always possible given the large uncertainty bounding very rare events. Other non-mathematical interpretations of likelihood and confidence would be on the other hand subjective.

Paragraph 2.11 of SSR-2/1 states that "The design for safety of a nuclear power plant applies the safety principle that practical measures must be taken to mitigate the consequences for human life and health and the environment of nuclear or radiation incidents (Ref. [2], Principle 9). Plant event sequences that could result in high radiation doses or radioactive releases must be practically eliminated and plant event sequences with a significant frequency of occurrence must have no or only minor potential radiological consequences. An essential objective is that the necessity for off-site intervention measures to mitigate radiological consequences be limited or even eliminated in technical terms, although such measures might still be required by the responsible authorities."

The term is also used in the supporting paragraphs to the following specific requirements:

- Requirement 5: Radiation protection (para 4.3*): "The design shall be such as to ensure that plant states that could lead to high radiation doses or large radioactive releases are practically eliminated.*

  and

- Requirement 20: Design extension conditions

  - (para 5.27) : "… *The plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained, with the result that early or large radioactive releases would be practically eliminated."*

  - (para 5.31): "*The design shall be such that the possibility of conditions arising that could lead to early or large radioactive releases is practically eliminated*."

It is therefore necessary to practically eliminate early and large releases and to this aim, the plant conditions that would ultimately originate them, are those that need to be practically eliminated by design.

The concept of practical elimination should not be misinterpreted or misused. It should be considered as part of a general approach to safety and, its appropriate application, as an enhancement of the defence in depth. Practical elimination describes how, in practice, the design of a nuclear power plant deals with rare phenomena or sequences with the potential to cause unacceptable consequences. These phenomena or sequences are in fact rare because of all the safety provisions made in the previous levels of defence in depth

As a first step for the implementation of design provisions for the practical elimination of undesired conditions it is necessary to identify what are these conditions and then for each of them specify the design provisions. It will be the decision of the safety authorities to assess if the measures implemented are satisfactory for the purpose. The decision will be based on engineering judgment, deterministic and probabilistic considerations.

The accident sequences that have a potential to lead to large releases involve both severe damage of the reactor core or spent nuclear fuel and the loss of the containment integrity or containment by-pass. Large releases could also be caused by severe damage of spent fuel that is in storage or in transfer outside the reactor containment.

The IAEA Safety Guide NS-G-1.10 provides a list of some conditions resulting from severe accident that strongly challenge the containment integrity and therefore should be practically eliminated.

The particular considerations of this kind addressed in the guide are:

- Severe accident conditions that could damage the containment in an early phase as a result of direct containment heating, steam explosion or hydrogen detonation;
- Severe accident conditions that could damage the containment in a late phase as a result of basemat melt-through or containment overpressurization;
- Severe accident conditions with an open containment — notably in shutdown states;

The conditions to be addressed for "practical elimination" could be classified within three types of hypothetical accident sequences. The first type could lead to prompt reactor core damage and consequent early containment failure. Such accidents could not be mitigated with implementation of reasonable technical means and they have to be "practically eliminated" from occurring. The second type comprises all conditions following a severe accident for which no effective technical solutions can be engineered to cope with the associated severe accident phenomena and therefore the confinement function would be lost. The third type consists of severe accidents in the absence of a leak tight containment.

The hypothetical accident conditions that require a specific demonstration of their "practical elimination" include at least following:

1. Events that could lead to prompt reactor core damage and consequent early containment failure
    a. Failure of a large component in the reactor coolant system
    b. Uncontrolled reactivity accidents
2. Severe accident conditions for which technical solutions for maintaining containment integrity cannot be ensured.
    a. Core meltdown in high pressure
    b. Steam explosion
    c. Hydrogen explosion
    d. Containment failure due to overpressure
    e. Containment boundary melt-through
3. Non confined severe fuel damage
    a. Severe accident with containment by pass.
    b. Significant fuel failure in a storage pool outside the containment

Some of these categories entail very severe challenges to the integrity of the physical barriers for radionuclide retention and require specific and very strong design and operation provisions for their practical elimination. The practical elimination can be considered as a design process followed by the necessary inspection and surveillance processes during manufacturing, construction, commissioning and operation. The demonstration of practical elimination is based on and assessment of such provisions, that would necessarily include engineering, deterministic and probabilistic judgement.

The technical measures to deal with each of these situations need to be provided and their effectiveness shall be analysed separately. None of the phenomena mentioned above should be overlooked just on the arguments on low likelihood but credible

research results and dedicated means to eliminate the identified risks shall support the safety claims.

In the following, each of the above hypothetical accident conditions is discussed.

Failure of a large component in the reactor coolant system

A sudden mechanical failure of a single large component in the reactor coolant system could initiate an event where reactor cooling would be lost in a short time and a pressure wave or a missile would damage the containment boundary. The defence in depth provisions would not be effective in such situation and an early large radioactive release would follow.. This is a very exceptional type of initiating event for which safety systems and safety features cannot be designed for their mitigation and therefore it should to be demonstrated that their likelihood would be certainly so low that they can be excluded, i.e. practically eliminated. It is therefore necessary to ensure and demonstrate that the likelihood of a catastrophic failure of any large vessel in the reactor coolant system is so low that it can be excluded, i.e. practically eliminated. This is essential at least for the reactor vessel, which break would eliminate the capability of holding and cooling the core but also the likelihood of pressurizer and steam generator shell failure should be shown to be extremely low, or alternatively it should be demonstrated that a failure of pressurizer or steam generator would not lead to unacceptable consequences to the containment.

The safety demonstration needs to be especially robust and the corresponding assessment suitably demanding, in order that an engineering judgment can be made for the following key requirements:

a. the most suitable composition of materials needs to be selected;
b. the metal component or structure should be as defect-free as possible;
c. the metal component or structure should be tolerant of defects;
d. the mechanisms of growth of defects are known
e. design provisions and suitable operation practice are in place to minimize thermal fatigue, stress corrosion, embrittlement, pressurized thermal shock, overpressurization of the primary circuit, etc.
f. an effective in service inspection and surveillance programme is in place during the manufacturing and the operation of the equipment to detect any defect or degradation mechanisms and to ensure that the equipment properties are preserved over the lifetime of the plant

In addition, evidence should be provided to demonstrate that the necessary level of integrity will be maintained for the most demanding situations.

Several sets of well-established technical standards, for instance the ASME Boiler and Pressure Vessel Code and equivalent codes used in other countries, are today available for ensuring reliability of large pressure vessels, and the demonstration of "practical elimination" of vessel failures can be based on rigorous application of those standards. The technical standards also provide instructions for verification of the state of pressure vessels during the plant lifetime.

The practical elimination of failures of large components is thus achieved by the essential means of the DiD Level 1 without relying on the subsequent levels of defence in depth.

The demonstration of low failure likelihood with a high confidence level could be supplemented by a probabilistic fracture mechanics assessment, which is today a widely recognized and commonly used technique. It is important to note, that probabilistic assessment in the demonstration of practical elimination, and specially in this case, is not restricted to the use of Boolean reliability models, e.g. fault trees or event trees, or failure rates derived from the statistical analysis of observed catastrophic failures. Probabilistic fracture mechanics includes assessments of material fracture toughness, weld residual stress, etc. which in turn consider deterministic analysis, engineering judgment and the measurements of monitored values as well.

Uncontrolled reactivity accidents

Reactivity accidents can be very energetic and have a potential to destroy the fuel and other barriers. The prevention of such accidents needs to be ensured at the DiD Level 1 by proper reactor design. The main protection is provided by negative reactivity coefficient with all possible combinations of the reactor power and coolant pressure and temperature, thus suppressing reactor power increase during any disturbances and eliminating the reactivity hazards with help of laws of nature (demonstration of practical elimination by impossibility of the conditions).

An uncontrolled reactivity excursion could also be caused by sudden insertion of a cold or un-borated water plug into a reactor core, although the reactivity addition would probably be smaller than what is needed for achieving prompt criticality. Nevertheless, all potential risks of sudden changes in the coolant properties must be identified and prevented by design provisions.
More complex situations could arise however if criticality can be reached during severe accidents. This has been a topic of concern in specific core melt-down scenarios in reactors where the control rod material has a lower melting point and eutectic formation temperature than the fuel rods. A potential hazardous scenario might occur if reactor vessel would be re-flooded with un-borated water in a situation when control rods have relocated downwards but the fuel rods are still in their original position. This is again an aspect to be analysed considering the design provisions and severe accident management features together, to reach a plausible conclusion that the condition has been practically eliminated.

Core meltdown in high pressure

Core meltdown in high pressure could cause a violent discharge of molten corium material into the containment atmosphere and this would result in direct containment heating by chemical reaction. High pressure core melt situations must therefore be eliminated by design provisions to depressurize the reactor coolant system when a meltdown is found unavoidable.

Any high pressure core meltdown scenario would evidently be initiated by a small coolant leak or boiling of the coolant and release of steam through a safety or relief

valve. In such situations it must be a design objective to transfer the high pressure core melt to a low pressure core melt sequence with a high reliability so that high pressure core melt situations can be practically eliminated. The depressurization must be such that very low pressure can be achieved before start of the meltdown process. On the other hand, dynamic loads from depressurization must not cause a threat to the essential containment structures.

Dedicated depressurization systems have been installed in existing plants and designed for new plants. At PWR plants they are based on simple and robust devices and straightforward operator actions that eliminate the risk of erroneous automatic depressurization but provide adequate time to act when need arises. At BWR plants the existing steam relief systems generally provide means for depressurization, with possibly some modifications in valve controls to ensure reliable valve opening and open valve position also in very low pressures.

Steam explosion

Steam explosion is a well-known phenomenon that has caused major damages in metal industries when molten metal has been brought to contact with water. The conditions of steam explosion triggering and the energy of explosion in various situations have been widely studied in reactor safety research programs. It has been concluded that risks of steam explosion cannot be fully eliminated in all core meltdown scenarios where molten corium may be dropped to water.

For eliminating steam explosions that could damage the containment barrier, the preferred method is to avoid dropping of molten core to water in any conceivable accident scenarios. Such approach is used in some PWR type reactors: existing small reactors where reliability of external cooling of the molten core has been proven and in some new reactors with a separate core catcher. In some existing and in some new designed BWR type reactors the molten core would in all severe accident scenarios drop to a pool below the reactor vessel and be solidified and cooled in the pool. In any such circumstances where corium drops to water, it must be proven with arguments based on the physical phenomena involved in the respective scenarios that risks from steam explosion to the containment integrity have been practically eliminated.

Hydrogen explosion

Hydrogen combustion is very energetic phenomenon, and an a fast combustion reaction (detonation) involving sufficient amount of hydrogen would cause a significant threat to the containment integrity. Dedicated means to eliminate hydrogen detonation are needed at all nuclear power plants, although different means are preferred at different plants.

In BWR containments that are all relatively small, the main protective mean is filling of the containment with inert nitrogen gas during power operation. In large PWR containments the current practice is to use passive catalytic recombiners or other devices that control the rate of the oxygen and hydrogen recombination.

It is also necessary to ensure and confirm with analysis and tests that circulation of gases and steam inside the containment provides proper conditions for hydrogen recombination and eliminate too high local hydrogen concentrations. Furthermore, the risk of hydrogen detonation increases if steam providing inertisation.

It is also necessary to ensure and confirm with analysis and tests that circulation of gases and steam inside the containment provides proper conditions for hydrogen recombination and eliminate high local hydrogen concentrations. Furthermore, the risk of hydrogen concentration increase under steam inerting conditions and subsequent steam condensation is eliminated.

An uncertainty that needs additional attention and further research relates to the highest conceivable rate and the total amount of hydrogen generation inside the containment. Some of the current core catchers can significantly reduce or even eliminate the ex-vessel hydrogen generation in the accident phase when the corium has dropped to the catcher, and this could bring major reduction also to the total amount of hydrogen generated inside the containment.

The design provisions for preventing hydrogen detonation need to be assessed in other to demonstrate the practical elimination of this phenomenon.

Containment failure due to overpressure

In a situation where core decay heat cannot be removed by heat transfer systems to outside of the containment and further to the ultimate heat sink, or in severe accident where the core is molten and is generating steam inside the containment, cooling of the containment atmosphere is a preferred mean for preventing its overpressure.

Several examples are found today from both existing plants and from new plant designs of robust dedicated containment cooling systems that are independent of other safety systems and are considered to practically eliminate the risk of containment rupture by overpressure.

An alternative to cooling is to eliminate the containment overpressure by venting. This is necessary especially in BWR type reactors where the size of the containment is small and pressure limitation may be needed both in the design basis accident as well as in accidents with core melt. The existing venting systems prevent overpressurization at the cost of some radioactive release involved in the ventilation, also in the event that the venting is filtered.

Containment venting avoids some peaks of pressure threatening the containment integrity, but the stabilization of the core and the cooling of the containment is still necessary in the longer term.

The safety demonstration should be based on the capability and reliability of the specific measures implemented in the design to cope with the severe accident phenomena. A PSA level 2 analysis can be used to demonstrate the a very low probability (practical elimination) of large releases.

Containment boundary melt-through

Containment boundary melt-through is a real threat to containment integrity unless means for cooling and solidifying the molten core are provided. Alternative means have been developed and verified in extensive severe reactor accident research programs conducted nationally and in international co-operation.

The means suggested today include

- keeping of the molten core inside the reactor vessel by cooling the vessel from outside,
- installing a dedicated system or device that would catch the molten corium as soon as it has penetrated the reactor vessel wall, and
- installing a pool below the reactor vessel and demonstrating that a catastrophic steam explosion is practically eliminated in any conceivable severe accident scenario.

In all of these approaches cooling of the corium is provided inside the containment by passive means that generate steam inside the containment and it is necessary to provide a separate dedicated system for heat removal from the containment, as discussed below.

Containment bypass

Containment bypass can occur in different ways, such through circuits connected to the RCS that exit the containment or defective steam generators tubes (PWRs). Accident sequences with non-isolated penetrations connecting the containment atmosphere to the outside as well as accident sequences during plant shutdown with containment open should be also considered as containment bypass scenarios. All these conditions have to be "practically eliminated" by design provisions such as adequate piping design pressure and isolation mechanisms.

It has to be taken into account that failures of lines exiting the containment and connected to the primary system, including steam generator ruptures are at the same time accident initiators, whereas other open penetrations just constitute a release path in accident conditions.

The safety demonstration for elimination of by-pass sequences should include a systematic review of all potential containment bypass sequences and cover all containment penetrations.

Requirement 56 in SSR 2/1 establishes the minimum isolation requirements for various kinds of containment penetrations. The requirement addresses aspects of leak-tightness and leak detection, redundancy and automatic actuations as appropriate. Specific provisions are given also for interfacing failures in the reactor coolant system. National regulations address in more detail what are the applicable provisions for containment isolations and prevention of containment bypass or interfacing LOCAs.

Based on the implementation of the design requirements or specific country regulations and the in-service inspection and surveillance practices, the analysis has to

assess the frequency of bypassing mechanisms. This analysis, although of probabilistic nature, it needs to combine aspects of engineering judgement and deterministic analysis in the probabilistic calculations, and always be based upon the redundancy and robustness of the design, the application of relevant design rules, e.g. fail safe actuation, as well as the pertinent inspection provisions and operational practices, similar to the previous cases. While the analysis of isolation of containment penetrations or steam generators is amenable to conventional fault tree and event tree analyses with due consideration of failures in power supplies, isolation signals and human actions, other analysis aspects may require the use of other probabilistic methods together with deterministic methods and engineering judgment to demonstrate the practical elimination of containment by pass.

This should lead on one hand to a defensible low frequency estimate of the by-pass mechanisms associated to each penetration based. On the other hand, the reliability of design provisions for the isolation of by-pass paths based upon conventional probabilistic analysis should complement the demonstration that the containment pass has been practically eliminated.

Significant fuel failure in storage pool

Facilities for spent fuel storage shall be designed to ensure that the potential for high radiation doses or radioactive releases to the environment are practically eliminated.
To this aim, it is necessary to ensure that spent fuel stored in a pool is always kept covered by an adequate layer of water. This requires inter alia

- a pool structure that is designed against all conceivable internal and external hazards that could damage its integrity
- avoiding siphoning of water out of the pool
- providing redundant lines for pool cooling that eliminate possibility of long lasting loss of cooling function, i.e. for time needed to boil-off the water
- reliable instrumentation for pool level monitoring.
- Appropriate reliable means to compensate any loses of water inventory.

Risks for mechanical fuel failures should be eliminated by

- lay-out design that ensures avoiding heavy lifts above the spent fuel stored in the pool
- structures of that together with potential pool covers eliminate the possibility of structures collapsing on the top of the fuel

In designs where the spent fuel pool is outside the containment, the uncovery of the fuel would lead to fuel damage and a large release could not be prevented. Means to evacuate the hydrogen would prevent explosions that could cause further destruction to the pool and prevent a later reflooding and cooling of the fuel.

In some designs, the spent fuel pool is located inside the containment. In this case, even though the spent fuel damage would not lead directly to a large release, the amount of hydrogen generated by a large number of fuel elements, the easy penetration of the pool liner by the corium without a fuel catcher, among other harsh effects would eventually lead to a large release. Therefore, it is also necessary to

ensure by design provisions that also in this case that the uncover of spent fuel elements has been practically eliminated.

SAFETY DEMONSTRATION

Physical impossibility

Where a claim is made that it is “physically impossible” for the conditions to arise that might lead to an accident condition that needs to be practically eliminated, it is necessary to examine the inherent safety characteristics of the system, or reactor type to demonstrate that the fundamental safety functions (Requirement 4) of reactivity control, heat removal and limitation of radiological effects will be achieved.

Extremely unlikely conditions

The safety demonstration has to analyse the response of the plant to multiple failure situations as well as internal and external hazards. The safety demonstration with respect to these situations and hazards needs to be made on the basis of adequate design provisions and margins against the magnitude of hazards supported by probabilistic assessments. In this regard, it needs to be noted that specific probabilistic safety assessment methods are applied for external hazards, such as earthquakes. Possible links between internal and external hazards and single initiating events have also to be considered. In the short term, the safety of the plant shall not be dependent on the availability of off-site services such as electricity supply and firefighting services. The design shall take into account site specific conditions to determine the delay after which off-site services need to be available.

The "practical elimination" of accident situations which could lead to large or early releases can be mainly demonstrated by deterministic considerations supported by probabilistic considerations, taking into account the uncertainties due to the limited knowledge of some physical phenomena. Each type of sequence must be assessed separately.

It is important to note that although probabilistic targets can be set, "practical elimination" cannot alone be demonstrated by showing the compliance with a general probabilistic value, and the achievement of any probabilistic value should not be considered as a justification for not implementing reasonable design or operational measures.

For new designs which adopt the latest technological solutions for a strong implementation of defence in depth, it is expected that a probabilistic target of lower than 1×10^{-7} per reactor year should be achievable.

On the basis of the considerations made in this section it is proposed to adopt the following definition for the “conditions practical eliminated”:

The possibility of conditions occurring that could result in high radiation doses or early or large radioactive releases 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 degree of confidence to be extremely unlikely to arise because

of the rigorous prescriptive and deterministic measure adopted. It is expected that a frequency value of lower than 1x 10^{-7} per reactor year can be demonstrated for each of the conditions identified.

The frequency level of 10^{-7}/y in the definition above refers to events of internal origin in the plant. It is generally impractical (perhaps impossible) for some external hazards to adopt a very low frequency threshold (such as 10^{-7}/y) for the occurrence of a hazard of such severity that could cause extensive plant damages leading to a large or early release and therefore needing to be practically eliminated.

The assessment of external hazards requires a convolution analysis of the frequency of a hazard of a given magnitude, the plant (SSCs) resistance and the plant response for practically eliminating a large or early release. Due to the scarcity of experience, the frequencies that can be estimated for very rare but extreme external hazards entail very large uncertainties. It should be recognized that some external hazards at an "estimated" frequency range of 10^{-4}/y to 10^{-5}/y may have the potential to lead to unconsidered plant conditions immediately (i.e. as singletons) because they can disable multiple levels of DiD simultaneously. Some examples include volcanoes, tsunamis, fault displacement hazards and large airplane crashes. In cases where such hazards are possible it is important to attempt to practically eliminate the effects of them. This can be done through a high quality evaluation of the involved parameters and the provision of adequate design, beyond design basis and site protection measures. In cases where this is not feasible, the site should not be used for the operation of an NPP.

This shows the limitations of probabilistic methods to claim the demonstration of the practical elimination. For these reason, it is advisable to keep the "practical elimination" concept for external hazards separate from those associated with internal plant sequences.

10. DESIGN FOR EXTERNAL HAZARDS

In relation to external hazards, the Fundamental Safety Principles recognize the selection of an adequate site for the NPP as an important aspect of the Defence in Depth. External hazards have the potential to trigger initiating events, cause failures of equipment needed to mitigate them and also adversely affect directly or indirectly the barriers to the release of radioactive materials. The site selection and site characterization is not considered explicitly as a level of defence in depth, but is an essential input for the design of SSCs associated with all the levels, including infrastructure that may be required for emergency planning and response. In relation to external hazards the site selection aims at selecting a site that is less prone to natural and human induced external hazards both in terms of intensity and frequency of occurrence. This results in fewer and less severe challenges to the design of plant SSCs.

The design of NPPs includes due consideration of those external events that have been identified in the site evaluation process. All foreseeable external hazards need to be identified and their effects evaluated. The derivation of the design bases of SSCs

for external hazard is part of the Site Evaluation process and the requirements related to this are provided in NS-R-3 [13]. In particular, NS-R-3 requires that:

"2.7. The hazards associated with external events that are to be considered in the design of the nuclear installation shall be determined. For an external event (or a combination of events) the parameters and the values of those parameters that are used to characterize the hazards should be chosen so that they can be used easily in the design of the installation."

There are several alternatives for the derivation of the design basis of plant SSCs for external hazards depending on the hazard and the characteristics of the site region. These alternatives, considered in NS-R-3 and associated safety guides include deterministic, probabilistic or hybrid approaches.

In general, the term "plant design" includes also the plant grade and the plan layout, which are important in relation to external hazards. Site protection measures, on the other hand, include such features as sea walls, pressure barriers, dykes, etc. which are not part of the plant SSCs but need to be designed and constructed with due consideration that they will be performing safety functions.

As discussed in Section 2, Design Extension Conditions are a specific category of plant states. However external events exceeding the values specified in the design basis and their associated loads are not postulated plant states. For this reason they are not included in the current definition of a Design Extension Condition, which is a an accident condition used to introduce in the design of the NPP the consideration of postulated sequence of events typically caused by multiple safety systems failures. For external events that exceed the design basis, i.e. the magnitude for which the safety systems are designed to remain functional both during and after the external event, the the term "Beyond Design Basis External Event" (BDBEE) is proposed and used in this document.

Although design extension conditions can not completely bound any situation which is more severe than design basis accidents, in general the plant states identified as DECs for internal events in the design may be similar to potential conditions which may develop following a BDBEE.

Paragraph 5.21a of SSR-2/1 requires that "*The design of the plant shall provide for an adequate margin to protect items ultimately necessary to prevent large or early radioactive releases in the event of levels of natural hazards exceeding those to be considered for design taking into account the site hazard evaluation".*

SSR-2/1 imposes more demanding requirements for the protection against external natural hazards for equipment ultimately necessary to prevent early or large releases. The design of these items is expected to be particularly robust and to include margins to withstand loads and conditions generated by natural external hazards exceeding those derived from the site evaluation. This implies that cliff edge effects should not occur not only for small variations but also for significant variations of the loads and conditions. This has the purpose to ensure that if a severe accident were to occur due

to an external hazard (similar to the case of Fukushima Daiichi NPP13) there are appropriate assurances that sufficient mitigative means would be available.

The possibility that a subsequent level of defence in depth (e.g. Level 4) may be impaired before the previous one (e.g. Level 3), is contrary to the DiD logic. The above provision is needed because external hazards may challenge levels of DiD without regard to their order.

The implications of the requirement above have not yet formally addressed in any Safety Standard of the IAEA, but it is clear that there are some important issues to be addressed and resolved. In particular, it is necessary to compile the list of the equipment ultimately necessary to prevent early or large release and then to provide guidance on the external events to include in the design basis of these equipment and on the rules for their design and qualification, and for the assessment of the margins.

Equipment ultimately necessary to prevent early or large releases

SSCs ultimately necessary to prevent early or large release refer to equipment of the fourth level of defence in depth and in particular to some of the SSCs necessary to mitigate the consequences of accidents with core melt. A detailed list of these SSCs is design dependent, however, in general they include at least:

- Containment structure;
- Systems necessary to contain the molten core and to remove heat from the containment and transfer heat to the ultimate heat sink in severe accident conditions;
- Systems to prevent hydrogen detonations
- Alternative power supply (alternative to the Emergency Power Supply);
- Supporting systems to allow the functionality of the systems above;
- Control room[14].

For instance, if flooding is considered as the external hazard, this would mean that either all the structures hosting the above mentioned systems are located at an elevation higher enough above the beyond design basis flood, or adequate engineered safety features (such as water tight doors etc.) would be in place to protect these structures and ensure that mitigative actions can be maintained.

Design for natural external hazards exceeding the design bases

It is expected that the probability of occurrence of a natural hazard significantly more severe than that considered for the design of plant be very low (probability comparable to the probabilistic target for core damage). This gives confidence for the appropriate selection of the design basis hazards.

[13] Note that severe accidents, i.e. DECs, were not part of the design basis

[14] The control room is the only item for which SSR-2/1 explicitly requires margins for natural hazards more severe than those included in the design basis; SSR-2/1 6.40a : *The design of the control room shall provide an adequate margin against natural hazards more severe than those selected for the design basis.*

The prevention of early or large releases requires that that the SSCs ultimately necessary to prevent large releases be still operable in case of external events significantly exceeding those used for the design basis.

The following options are available to comply with the requirement 5.21a of SSR-2/1:

1. To adopt a higher value of the design basis event for the SSCs ultimately necessary to prevent early or large releases

2. To demonstrate, following a best estimate approach, that values of parameters for which cliff edge effects would occur are not reached because of adequate design margin. For this purpose, the demonstration should include the determination of the severity of the event and the probability at which the cliff edge effect would occur.

The approach to be followed will depend on the nature of the hazard and the function of the SSCs and has to be decided by the designer and the safety authority.

The probabilities of external hazards exceeding a well-established design basis are very low and generally associated with significant uncertainties. It is important to understand the behaviour of the plant SSCs to levels of the loading parameters associated with BDBEE. How much exceedance is needed to adequately understand this behaviour depends on the aleatory and epistemic uncertainties associated with these parameters, the potential evolution of these parameters through time (non-stationarity), which is especially valid for human induced events, and the tolerance of plant SSCs to increased levels of the external event under consideration.

Most experience related to this type of evaluation is on the subject of seismic safety. International practice considers an increase of about 50% above the design basis seismic levels for an adequate evaluation of the beyond design basis earthquake. This would mean that a plant should not get into a core damage situation when the seismic demand is increased to 1.5 times the seismic level 2, (SL2), the one imposing the most stringent safety requirements in the plant design. This evaluation requires the use of a different set of safety and behaviour limit criteria.

Conservative design margins should be associated with the design basis evaluation for all external hazards and environmental factors. This is because at the expected frequency levels of design basis external events, i.e. around 10^{-4} /year, does not allow estimates to be based solely on historical data.
Conservative design margins should be associated with the design basis evaluation for all external hazards and environmental factors such as air/water temperature, etc. This is because at the levels of 10^{-4}/y corresponding to external event design bases there is a lack of data and the values cannot be based on frequency considerations only. This forces the analyses to be model based and phenomenological, which introduces epistemic uncertainties into the process. Together with the aleatory uncertainties already present in the nature of the hazard, the design basis estimates start becoming driven by uncertainties. This requires ample margins to be considered in design. In addition, beyond design basis needs to be considered for the consideration of the cliff edge effects.

Some plant SSCs are designed for the extreme loads originated by accident conditions and external hazards. The eventual margin that is incorporated into the design can be determined from the sizing and the support of the SSC under consideration. As an example, if for the containment structure the governing loads are due to airplane impact, there may be a larger margin in the design for withstanding the loads resulting from an accident, e.g. a LOCA.

The acceptance criteria related to design basis external hazards should be compatible with the DBA criteria. The evaluation of the design basis external events and the associated design aspects should be conservative including significant safety margins.

Acceptance criteria related to BDBEEs should be compatible with the DEC criteria. Evaluation of the BDBEEs and the design features associated with the BDBEEs could be based on best-estimate considerations.

11. USE OF MOBILE SOURCES OF ELECTRIC POWER AND COOLANT

The revision of SSR-2/1 that was prepared to take into consideration the lessons learned from the accident of Fukushima includes three requirements on use of mobile equipment.

Req. 6.28b states: *For defence in depth, the design shall include features to enable the safe use of non-permanent equipment for restoring the capability to remove heat from the containment.*

Req. 6.45a states: *For defence in depth, the design shall include features to enable the safe use of non-permanent equipment to restore the necessary electrical power supply.*

Req. 6.68 states: *For defence in depth, the design shall include features to enable the safe use of non-permanent equipment to ensure sufficient water inventory for the long term cooling of spent fuel and for providing shielding against radiation.*

The design should be such that all conditions considered in the design are taken care by safety systems and safety features permanently installed at the plant. There should not be any need for additional equipment to comply with the acceptance criteria established for each plant state.

Non-permanent equipment may be added as complementary essential means of the fourth level of defence in depth.

According to the safety approach of the IAEA, the non-permanent equipment should be considered as necessary provisions to cope with conditions exceeding those considered for the design. For such situations, minimizing the radiological release and avoiding long term off-site contamination are the objectives which should be achieved.

Credit to the use of non-permanent equipment as an accident management measure (not for the safety demonstration of the design) may be given only if their installation

is possible in the time available before unacceptable consequences occur. The amended version of SSR-2/1 requires that the design shall include features for the safe use of non-permanent equipment for restoring the capability to remove heat from the containment (Req. 6.28a), for restoring the necessary electrical power supply (Req. 6.45a) and for ensuring sufficient water inventory for radiation shielding and long term cooling of spent fuel (Req. 6.68). If non-permanent equipment are planned to be used, it should be demonstrated that their installation is possible in the time available before unacceptable consequences occur. The demonstration should involve comprehensive commissioning tests that are used to verify the procedure for their connection and intended use. This is especially important for the safe connection of the electrical supply. The upkeep of practical skills for installation of non-permanent equipment should be ensured in emergency exercises simulating accident conditions

The ability to deliver the equipment on time should be demonstrated also for conditions involving significant degradation of offsite transportation infrastructures associated with extreme natural disasters.

Moreover flexibility to cope with different scenario brought by the use of non-permanent equipment without increase of complexity of the design should be also considered.
The coping time, installation time and flexibility are the key parameters to decide whether complementary equipment should be pre-installed at the site or stored in a remote storage.

There are already examples of non-permanent power sources (Req. 6.45a) and non-permanent equipment for cooling (Req. 6.28a, 6.68) being implemented on existing operating reactors.

12. REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No.SSR-2/1, IAEA, Vienna (2012).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, IAEA Safety Standards Series No.SF-1, IAEA, Vienna (2006)

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Basic Safety Principles for Nuclear Power Plants, INSAG-12, Vienna (1999)

[4] EUROPEAN UTILITY REQUIREMENTS FOR LWR NUCLEAR POWER PLANTS, Revision D, October 2012

[5] WESTERN EUROPEAN NUCLEAR REGULATOR'S ASSOCIATION, Safety of new NPP designs, WENRA Reactor Harmonization Working Group, (2013)

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4, IAEA Vienna (2008)

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Defence in depth in nuclear safety, INSAG-10, Vienna (1996)

[8] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION,INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (in preparation).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety margins of operating reactors, IAEA TECDOC 1332, Vienna (2003)

[10] Safety Margin Evaluation-SMAP Framework Assessment and Application", NEA/CSNI/R (2011)3, 30 Nov. 2011,

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-R-2, Vienna (****)

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. DS-431, In preparation

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. NS-R-3 (Rev. 1), IAEA, Vienna (in preparation).

13. ABBREVIATIONS

AC alternate current
AOO anticipated operational occurrence
ATWS anticipated transient without scram
BDBEE beyond design basis external event
CVCS chemical volume control system
CCWS components cooling water system
CCF common cause failure
CDF core damage frequency
CLI criteria for limited impact
DC direct current
DiD defence in depth
DAS diverse actuation system
DBA design basis accident
DEC design extension condition
DNBR departure from nucleate boiling ratio
EC emergency centre
ECCS emergency core cooling system
ESWS essential service water system
EUR European utility requirements
BWR boiling water reactor
HDL hardware description language
HVAC heating ventilation and air conditioning
I&C instrumentation and control
LOCA loss of coolant accident
LOOP loss of offsite power
LWR light water reactor
MCP main coolant pump
NO normal operation
OSC operation support centre
NPP nuclear power plant
PIE postulated initiating event
PWR pressurized water reactor
RHR residual heat removal system
RHWG reactor harmonization working group
RWST refuelling water storage tank
SBO station blackout
SSC structure, system and components
TSC technical support centre
UHS ultimate heat sink
WENRA Western European Nuclear Regulator Association

14. APPENDIX 1: ACCEPTANCE CRITERIA[15] FOR DIFFERENT PLANT STATES

The demonstration of adequacy of the design to cope with different plant states includes the demonstration of the compliance with the acceptance criteria, which are established, following a graded approach, for each plant state. The application of the graded approach leads to acceptance criteria more restrictive for events with higher probability of occurrence.

Acceptance criteria (we ned to distinguish acceptance criteria in terms of level of redundancy, system design, behaviour limits for materials, etc. from acceptance criteria for radiological levels) are established in terms of acceptable radiological consequences and in terms of degree of integrity of barriers against releases of radioactive substances (fuel matrix, fuel cladding, reactor coolant pressure boundary or containment) – see the table below.

High level criteria are typically expressed in terms of discharges or releases of radioactive material to the environment, whole body effective doses, equivalent doses for selected body organs, and radioactivity or contamination levels of ground, water, corps and food items. Derived criteria are typically expressed in terms of surrogate variables determining integrity of barriers, such as pressures, temperatures, stresses, strains, etc.

Since the acceptability of radiological consequences is to large extent related to off-site emergency actions, it is reasonable to associate radiological safety objectives or acceptance criteria with intervention levels adopted for emergency actions.

Acceptance criteria for design should be significantly lower than the intervention levels adopted for emergency measures.

The target would be to minimize the need for emergency measures

SSR-2/1 in art. 5.25 and 5.31 provides the hint for a link between the design provisions and the emergency intervention levels so that the radiological acceptance criteria should be established consistently with reference levels.

Guidelines for intervention levels and action levels in emergency exposure situations are provided in Annex III of [5] as follows (with more specific information in the Standard). The generic optimized intervention level for sheltering is 10 mSv of avertable dose in a period of no more than 2 days.

- The generic optimized intervention value for temporary evacuation is 50 mSv of avertable dose in a period of no more than 1 week
- The generic optimized intervention value for iodine prophylaxis is 100 mGy of avertable committed absorbed dose to the thyroid due to radioiodine.
- The generic optimized intervention levels for initiating and terminating temporary relocation are 30 mSv in a month and 10 mSv in a month, respectively.

[15] These criteria should be understood as design targets rather than as regulatory acceptance criteria.

- Permanent resettlement should also be considered if the life time dose is projected to exceed 1 Sv.
- The doses to be compared with these intervention levels are the total doses from all routes of exposure that can be averted by taking the countermeasure but usually this will exclude routes involving food and water.

Level of defence	Objective	Associated plant state	Criteria for maintaining integrity of barriers	Criteria for limitation of radiological consequences
Level1	Prevention of abnormal operation and failures	Normal operation	No failure of any of the physical barriers except minor operational leakages	Negligible radiological impact beyond immediate vicinity of the plant. Acceptable effective dose limits are bounded by general radiation protection limit for the public (1 mSv /year[16] commensurate with typical doses due to natural background), typically of order of 0.1 mSv/year.
Level 2	Control of abnormal operation and detection of failures	Anticipated operational occurrence	No failure of any of the physical barriers except minor operational leakages	Negligible radiological impact beyond immediate vicinity of the plant. Acceptable effective dose limits are similar as for normal operation, limiting the impact per event and for the period of 1 year following the event (0.1 mSv/y)
Level 3	Control of design basis accidents (DBAs)	Design basis accident	No consequential damage of the reactor coolant system, maintaining containment integrity, limited damage of the fuel	No or only minor radiological impact beyond immediate vicinity of the plant, without the need for any off-site emergency actions. Acceptable effective dose limits are typically of order of few mSv.
Level 4a	Control of DECs without core melt (prevention of accident progression into severe accident)	Design extension conditions without core melt	No consequential damage of the reactor coolant system, maintaining containment integrity, limited damage of the fuel.	The same or similar radiological acceptance criteria as for the most unlikely design basis accidents
Level 4b	Control of DECs with core melt (mitigation of consequences of severe accidents)	Design extension conditions with core melt (severe accident)	Maintaining containment integrity both in an early as well as late phase, and practical elimination of fuel melt sequences when the containment is disabled or by-passed	Only emergency countermeasures that are of limited scope in terms of area and time are necessary[17]

[16] See Radiation protection and safety of radiation sources: international basic safety standards: general safety requirements. GSR Part 3, Section III-3, Interim edition. IAEA, Vienna, International Atomic Energy Agency, 2011.

[17] Ref. 4 provides more detailed guidance on interpretation of the limited scope of radiological consequences.

Level 5	Mitigation of radiological consequences of significant releases	Accidents with releases requiring implementation of emergency countermeasures	Containment integrity severely impacted, or containment disabled or bypassed	Off site radiological impact necessitating emergency countermeasures

15. APPENDIX 2: DEPENDENT FAILURES

In the context of the design and safety assessment of an NPP it is of particular relevance to minimize or eliminate the degree of dependency[18] between the occurrence of PIEs and the failure of the equipment or human actions designed to mitigate it, between failures of redundant system trains carrying mitigating functions and between failures of equipment associated with different levels of defence in depth, in particular between levels 3 and 4. Other dependent failures should be also taken into consideration if possible, but their safety significance is much lower for instance in the case that they relate to non-redundant equipment.
For reducing the likelihood of these types of dependent failures, it is important to understand the different types of dependencies and how are they treated in the plant safety assessment as well as the types of root causes and the defence measures that can be used in design and operation to prevent them. The analysis and classification of these types of dependencies is useful in addition to establish a coherent terminology regarding the different kind of dependent failures.

PSA is particularly useful tool to address dependent failures, starting from the fact that all basic events postulated in PSA models are considered as statistically independent. To be able to make this assumption, the level of detail of the models needs to be sufficient to model all kind of sources of dependency explicitly. These sources of dependency can be categorized in the following categories:

1) *Functional dependencies*

These are dependencies of a component on its support systems, e.g. power supply, cooling, instrumentation, etc. The component becomes functionally unavailable or eventually fails (e.g. due to overheating) because of a support system failure. Such dependencies cannot be eliminated as they are needed for the operation of the system. However, it is of importance for safety that redundant trains rely on different trains of support systems. This should be a requirement for safety systems. It is necessary to ensure that swing trains in cooling system used in some design to support different trains of front line systems, don't introduce dependencies of redundant trains on a common train of supply in a support system.
To this category belong also some subtle dependencies on non-connected support systems, typically the ventilation or air conditioning system if it is needed for the functionality of the equipment, at least in the long term.

---

[18] Two events of any kind, A and B, as for instance failures of a component or a system in a nuclear power plant, are statistically independent if and only if:
$Probability\ (A \cap B) = Probability\ (A) \cdot Probability\ (B)$

Otherwise the two events are dependent and
$Probability\ (A \cap B) = Probability\ (A) \cdot Probability\ (B|A) = Probability\ (B) \cdot Probability\ (A|B)$

If $Probability\ (A \cap B) = Probability\ (A)$
or $Probability\ (A \cap B) = Probability\ (B)$
then the two events are fully dependent.

For three or more events, the condition of independence condition needs to be met by any double, triple, … combination of the events under consideration.

2) Dependencies through system interfaces

In some designs some systems are connected to common lines of piping or tanks for delivering of flow or water supply, without constituting a functional dependency as discussed in the previous section. Similarities can exist in electrical systems regarding power buses. Thus the failure of a common line of piping or a valve, or the need to perform maintenance in the area of the interface may lead to a diversion of flow or render parts of different systems inoperable, normally of a single train. As example could be a common RWST to high and low pressure emergency core cooling and containment spray with all these systems sharing a common line for each train. In this example, none of this system is a support system of the other but a failure or maintenance in the interface area affects all of them. In some cases this kind of interface may exist with the same system

3) Dependencies between PIEs and mitigating systems

Provisions need to be taken in the design such as physical separation, protections against dynamic effects, anti-whip equipment qualification, electrical protections, etc. to prevent or minimize the effects of the initiation events on plant SSCs. Notwithstanding some initiating events by their own nature may impair or diminish the reliability of equipment that could be called upon for its mitigation. This is the case of the loss of offsite power, loss of some power buses inducing reactor scram or the loss of the main condenser. The design needs to be in such cases sufficiently robust to shut down the plant safely with the remaining equipment.

4) Multifunction of systems and components

Plant designs use some common systems or equipment for different functions that are often associated with different levels of defence in depth for the purpose of plant economy or design limitations. This is the case of the reactor scram system, for which is practically not feasible to have separate systems for levels 2 and 3 or the use of parts of the emergency core cooling systems in the CVCS or the RHR system.

5) Operation errors

These are dependencies in the performance of different plant equipment due to the actions of the operating crew. These actions are affected by both operational aspects, e.g. procedures, operator training, and design aspects, e.g. adequacy of instrumentation and man machine interface.

6) Common cause failures

Common cause failures are used to designate failures of two or more redundant[19] components of the same kind due to a number of different causes excluding those

[19] Common cause failures of non-redundant components are not especially relevant as they are expected to be much less frequent than independent failures causing the same effect.

indicated before, that can take place simultaneously or close enough in time[20] for the redundant components to fail to fulfil their required function following a PIE. The cause of common cause failures can be grouped as:

- Errors in design, manufacturing and construction
- Errors or inadequate practices during maintenance, surveillance or inspection
- Environmental or external factors resulting in conditions exceeding the margins of the design.
- Impact of internal or external hazards.

Behind most of these causes a human component can be identified. In fact, the real root causes of common cause failures might not be evident and need in depth investigations. Frequently proximate causes of the failure are identified in the short term. They can lead to actual common cause failures or incipient failures or degraded failure conditions, that if not timely identified may lead to common cause failures. Finally ageing could be considered as an unavoidable common cause root cause affecting a wide range of components in the long term, for which adequate measures must be put in place.

In NUREG/CR-5460[21] an elaborated analysis of how root causes of common cause failures linked by coupling mechanisms can lead to common cause failures if defensive mechanisms are not in place or are inefficient, is presented. A synthesis of this analysis is presented here for helping to understand the development of common cause failures and establishing the adequate design provisions in the design to ensure effective independence of the defence in depth levels an adequate reliability of the safety functions required at each level.

Wherever equal or similar components used in the design to provide redundancy, or more generally combination of failures of equal or similar components may allow the progression of a PIE, such kind of components should be considered for the analysis of susceptibility to common cause failures. However, this general criterion may lead to an arduous work if no additional criteria are taken into account to reduce the groups of components that could realistically be affected by common cause failures. Thus, is not practical to consider that a common cause failure could affect for instance check valves of the same size and manufacturer in the plant, although a design or manufacturing error could indeed affect to all of them.

The consideration of coupling mechanisms, such as e.g. belonging to the same system, accomplishing the same function, undergoing the same testing procedure or being in the same location play an important role on establishing the group of components that are more susceptible to a common cause. In addition, it is considered that common cause failures of active equipment would be predominant over common cause failures of passive systems. The latter are therefore analysed in less detail in general.

[20] Common cause failures can be latent or remain undetected until a given triggering condition takes place or the components are required to enter into function.

[21] U.S. Nuclear Regulatory Commission, *A Cause-Defense Approach to the Understanding and Analysis of Common-cause Failures,* NUREG/CR-5460, March 1990, SAND89-2368.

The causes of common cause failures can be originated in the preoperational phase of the plant. This includes a series of cause in the design specification, manufacturing, construction, installation and commissioning. They can also be related to the plant operation, e.g. how components are maintained or calibrated, or to environmental causes, e.g. corrosion, effect of heat, steam or water impingement.

In the context of this document, associated to the application of SSR 2/1, root causes as well as coupling mechanisms and defensive measures related to the plant design are the focus of importance. Therefore, for common cause failures rooted in the preoperational phase of the plant the applicable defensive mechanisms can be:

Diversity

Two principal kinds of diversity are normally defined: 1) Functional diversity or use of components based on different operating principles or variables measured and 2) Technical diversity or use of components of different manufacturing or physical characteristics. Diverse equipment provide also redundancy, i.e. they fulfil the single failure criterion. Diversity is a specific measure aimed at preventing common cause failures and other dependent failures although not efficient for every specific cause.

Regulations in some countries include requirements for diversity. Functional diversity is for instance required in the generation of signals of the reactor protection system. Functional diversity is stronger than technical diversity although not always feasible. In addition technical diversity goes against the goal of design standardization and entails additional maintenance and testing practices. Functional diversity implies in practice technical diversity.

Proven design and construction

The use of proven engineering practice is a pillar of the first level of defence in depth and equally applicable to systems involved in other levels.

Physical separation

Physical separation of redundant trains and components is efficient against common cause failures and other dependent failures originated by harsh environmental conditions and the effects of several hazards, as well as the direct impact of mechanical or electrical failures of one train on the redundant train.

Earthquakes, fires and floods among other hazards have the potential to fail or degrade the condition of many plant SSCs at once. Moreover some of these hazards can induce other hazards as it happened in the Fukushima accident. Physical separation, adequate plant layout and design robustness are at the core of the defensive measures to reduce the impact of natural hazards, in addition to adequate design margins and protective measures as well as good operational practices

Of particular importance is the adequate separation of cable routings of different electrical and instrumentation divisions. A full physical separation of trains might not be feasible in all plant areas. Physical separation can be accomplished either by full

separations of trains through qualified barriers, the installation of protections on one train's relevant equipment and the separation by sufficient distance. The first option gives in general the highest protection

Self-testing equipment and self-announcement of failures

By an immediate detection and indication of a failed condition in stand by components, it is possible to undertake fast corrective actions for increasing the availability of the component and the systems. This applies also to the early detection of common cause failures. This principle is applied extensively in the reactor protection system design.

Regular maintenance and inspection and testing

Adequate testing and inspection programmes reduce the probability of failures, allow an the early detection of inspection failures and if a proper analysis of failures or findings in component conditions is carried out, including subsequent testing or inspections of redundant components if deemed necessary, it contributes to the early detection of common cause failures. In addition the implementation of a staggered testing or maintenance policy versus a sequential one reduces the likelihood of human related common cause failures.

Redundancy

Redundancy can also be efficient against several root causes of common cause failures, since they don't normally lead to simultaneous failures, particularly if the components don't have the same operation regime, e.g. it usual to have one pump running and one pump in standby in cooling systems during plant operation. Hence, the occurrence of a common cause failure in one component can be still be compensated by the functioning of the redundant components. If adequate instrumentation to detect failures is available and an analysis of the causes of failures is performed, degradations in the redundant component can be identified before an actual common cause failure occurs in it.

Diversity, in particular functional diversity is of value against errors during design, manufacturing and construction. Technical diversity is less efficient as it may not prevent potential error in the formulation of the component design basis and specifications.

Proven design and constructions as well as adequate quality control processes, including design review, inspection and testing from manufacturing to commissioning are also two important defensive mechanisms to prevent common cause failures originated in the pre-operational phase of the plant.

With regard to environmental related causes of common cause failures, such factors can be originated within the system, e.g. due to the physicochemical properties of the system fluids or to external environmental effects. Environmental effects could be fast or slow acting. For slow acting effects, appropriate policy and practice for surveillance and maintenance may be efficient. For fast developing environmental effects physical separation is the most efficient defensive mechanism.

Equipment diversity may also help is as much as diverse equipment may be differently susceptible to slow acting internal or external environmental common cause stressors.

16. CONTRIBUTORS TO DRAFTING AND REVIEW

D.J. Burger, Ontario Power Generation, Canada

E.J.F. Courtin, Areva NP, France

M. Gasparini, Consultant, Italy

L. Gilbert, Bruce Power, Canada

A. Gürpinar, Consultant, Turkey

J. Laaksonen, Rosatom Overseas, Russian Federation

J. Misak, Nuclear Research Institute Rez, Czech Republic

K.U. Nuenighoff. Gesellschaft für Anlagen und Reaktorsicherheit, Germany

B. Poulat, International Atomic Energy Agency

J. Yllera, International Atomic Energy Agency

Consultant meeting, Vienna 10-14 March 2014

Consultant meeting, Vienna 30 June – 2 July 2014