International Atomic Energy Agency

Considerations for the Practical Application of the Safety Requirements for Nuclear Power Plant Design

Joint ICTP-IAEA Essential Knowledge Workshop on Deterministic Safety Analysis and Engineering Aspects Important to Safety

Trieste, 12-23 October 2015

J. Yllera

IAEA, Division of Nuclear Installation Safety

Background Information

- **The new Safety Requirements for the Design of NPPs, SSR - 2/1 introduced some new concepts and terminology, for which there is not always a common understanding in different Member States.**

- **A harmonized understanding is important (also for the IAEA Secretariat) prior to the revision of several safety standards and not only for NPPs .**

- **Therefore, the initiated the development of a TECDOC aimed at facilitating the understanding and provide more explicit information on selected topics introduced in SSR-2/1 and its new revision**

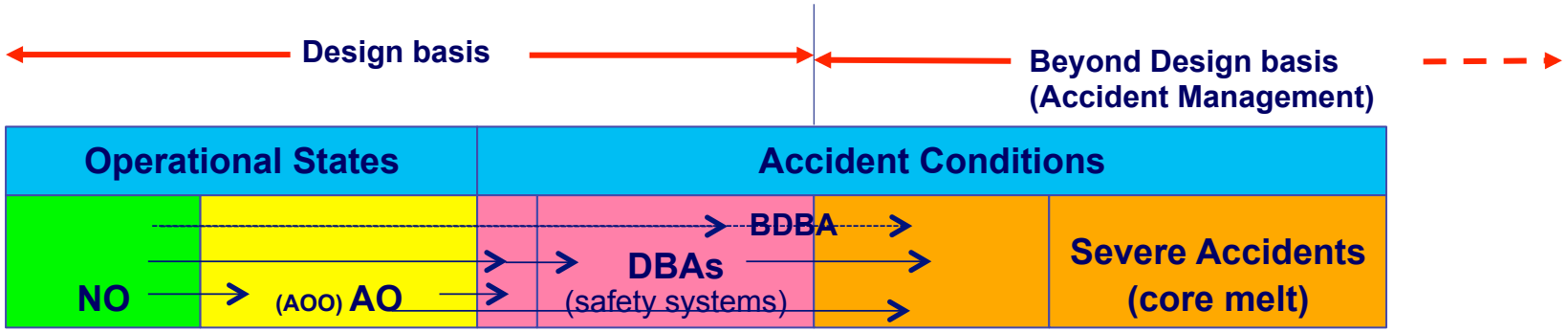
TECDOC Objectives / Scope

- **The TECDOC is aimed at facilitating the understanding and provide more explicit information on selected topics introduced in SSR-2/1 and its new revision.**
  - **Plant States considered in the design (for reactor and SFP),**
  - **Design Extension Conditions without and with fuel damage.**
  - **Design basis of plant equipment**
  - **Defence in Depth (DiD) strategy for new plants.**
  - **Independence of the levels of DiD and prevention of common cause failures.**
  - **Reliability of the heat transfer to the ultimate heat sink**
  - **Design margins and prevention of cliff-edge effects**
  - **Concept of "practical elimination" of early or large releases**
  - **Design for external hazards**
  - **Use of mobile sources of electric power and coolant**

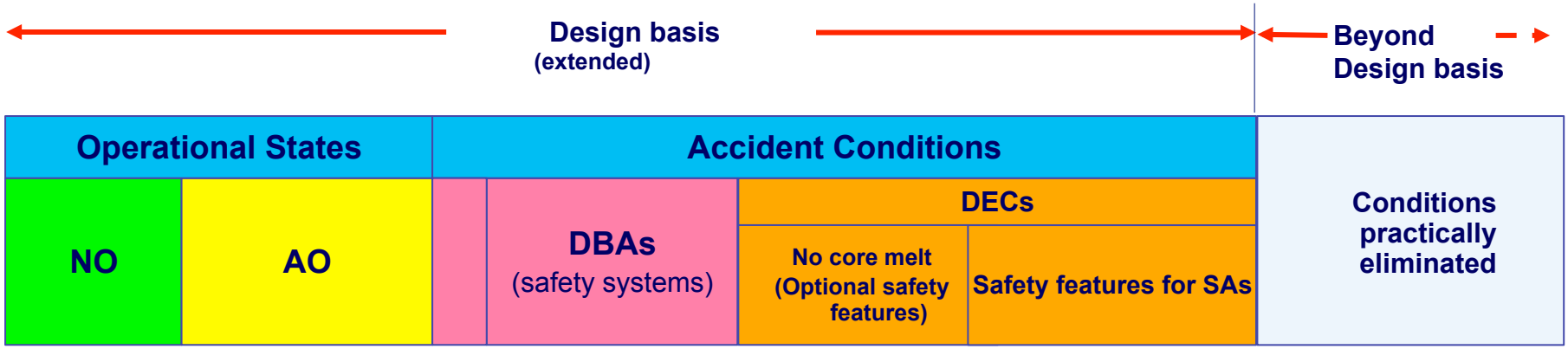
- **The importance of some of these issues has been confirmed by the lessons learned from the Fukushima accident.**

Plant Sates & Design Basis

Earlier Concept



SSR-2/1, 2012



Design Basis ≠ Design Basis Accidents

Beyond Design Basis ≠ Beyond Design Basis Accidents

- **Anticipated operational occurrence (AOO). From NO to AO**

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.

- **Design basis accident (DBA)**

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.

- **Design Extension Conditions (DECs). IAEA Definition:**

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.

Design Extension Conditions (DECs)

- **Term introduced in the EUR** to define **some** accident sequences selected on deterministic &probabilistic basis that go beyond Design Basis Conditions (DBC), including complex sequences and severe accidents with the intent to improve the safety of the plant extending the design basis.

- **Concept was basically adopted by IAEA in SSR 2/1.** DECs are a set of conditions induced by accidents more severe than DBA or involving additional multiple failures of safety systems that the plant has to withstand without unacceptable radiological consequences.

- **A similar concept was also adopted by WENRA,** although the term DEC was initially 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 it.

- **The concept of DEC is not completely new.** Some important multiple system failures (SBO, ATWS) had been addressed already in some designs or in plant backfitting.

Design Extension Conditions (DECs)

WENRA	EUR	IAEA
Multiple failures	Complex sequences	Design Extension Conditions
- Small LOCA + Low head safety injection	- Main steam line break + consequential SGTR	So far examples are not available in Safety Standards. They will be included in the revised Safety Guides for Design and Safety Assessment
- Station Blackout	- Station Blackout	
- ATWS	- ATWS	
- Loss of the RHR in normal operation	- Containment System Bypass (multiple SGTRs)	
- Loss of cooling of the spent fuel pool		
Postulated core melt accidents	Severe accidents	

- The control of DECs is expected to be achieved by specific features implemented in the design and not only by accident management measures using existing equipment designed for other purposes.

Design Extension Conditions (DECs)

- SSR-2/1 requires that the set of DECs are derived on the basis of engineering judgement and DSA and PSA. (OE is not explicitly mentioned but it will be considered).
- DECs are technology dependent, and recommended DECs (except for SBO) are not available in any IAEA SSs. Preliminary list of DECs without core melt as a reference:
  - ATWS,
  - SBO,
  - Total loss of feed water
  - LOCA together with the complete loss of one ECCS
  - uncontrolled level drop during mid-loop operation (PWR) or during refuelling
  - loss of the component cooling water or 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 SGTR
  - AOO or DBA combined with the failure of the reactor protection system and the actuation of safety systems
- For severe accidents (DECs with core melt), containments systems and other features are necessary to maintaining the integrity of containment as the main ultimate objective. However, the cooling and stabilization of the molten fuel needs to be achieved to ensure the containment integrity in the long term.

Design Basis of plant equipment versus Beyond Design Basis

"Design Basis of the plant" is a common, not very precise and, in some cases, misleading term. It refers to 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 (features)

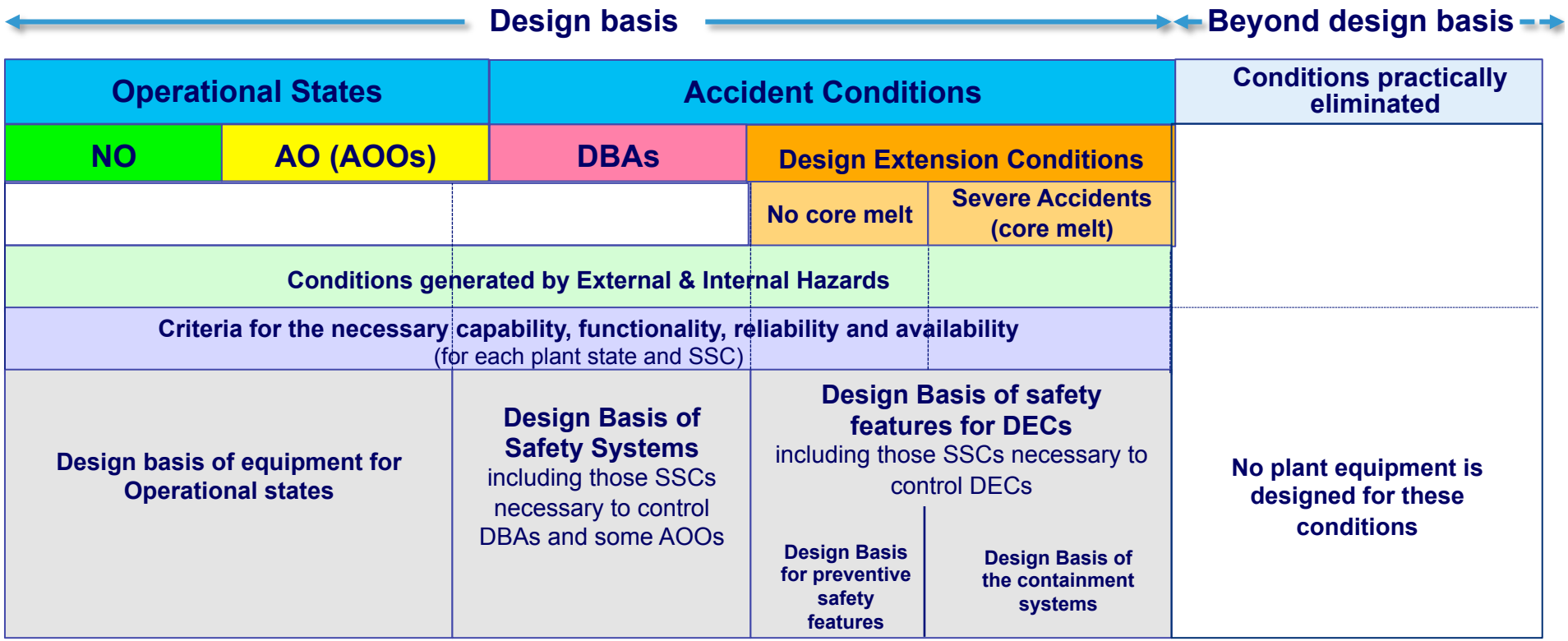
Saying, that a specific accident is included in the design basis of the plant (e.g. it is a design basis accident) means in reality that the conditions generated by this accident are included in the design basis of a set of structures, systems and components (SSCs) that have the function to deal with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

However, each single plant SSC to be correctly designed needs its own design basis and the design basis can be different from others.

Design Basis (SSR 2/1) : Set of information which identifies for each SSC conditions, needs and requirements necessary for its design :

- the functions to be performed by the SSC of a facility
- the operational states, accident conditions in which it is required
- conditions generated by internal and external hazards that the structure, system and component has to withstand
- the acceptance criteria for the necessary capability, reliability, availability and functionality

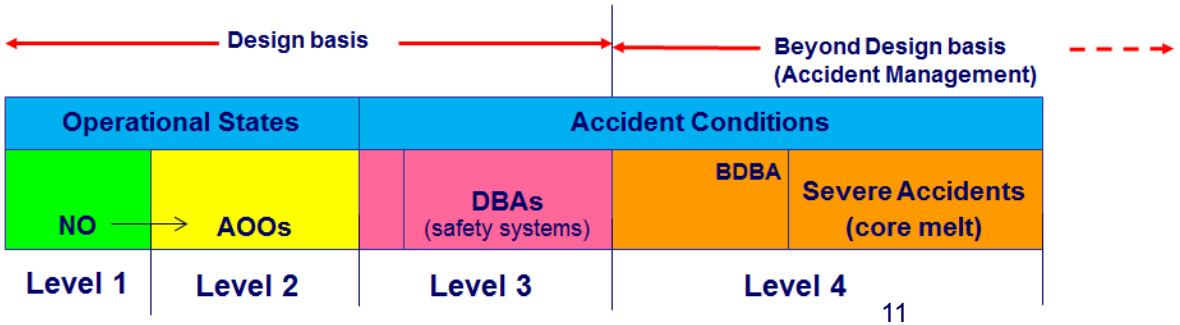
Plant Sates & Design Basis (SSR 2/1)



DiD approach form INSAG-10

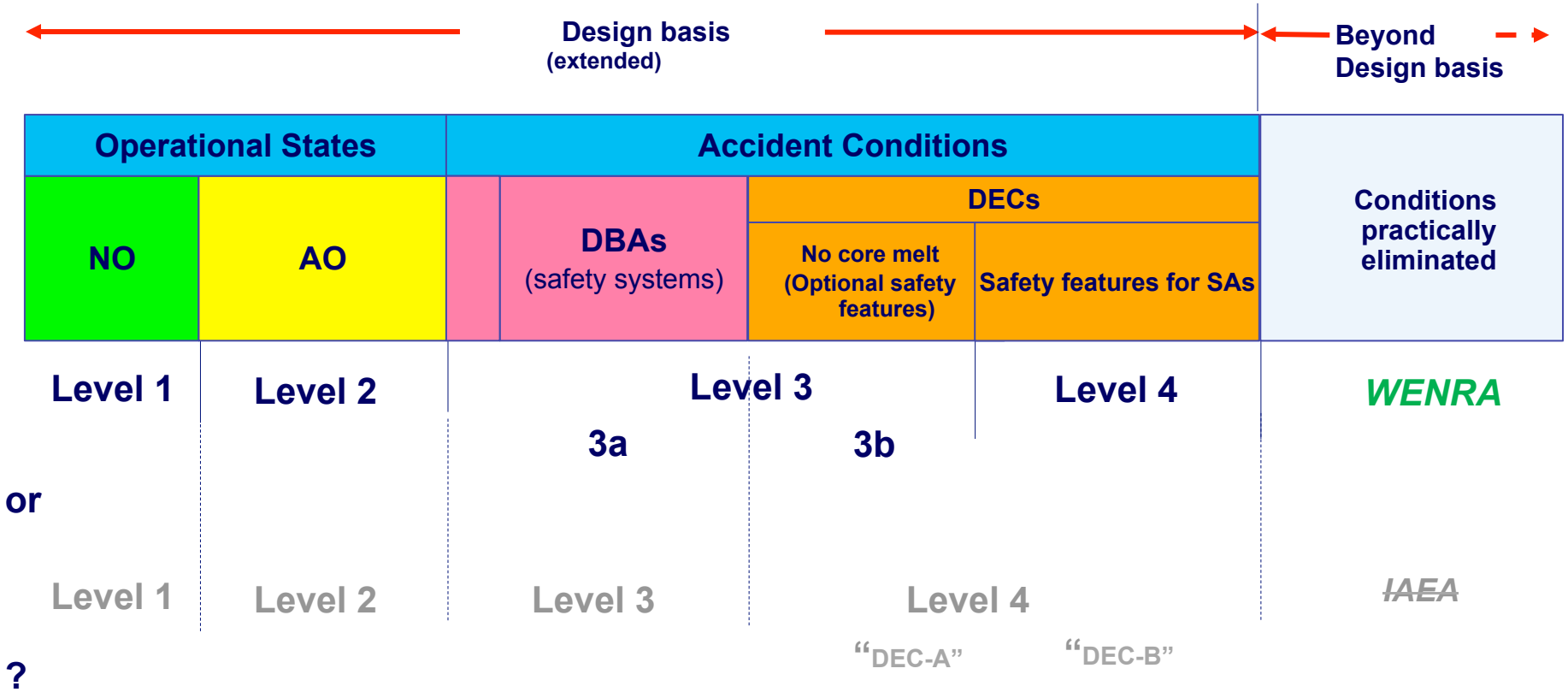
- INSAG formalized the DiD approach in 5 levels.
- Scheme incorporated in several IAEA SSs
- It is the basis for SSR- 2/1, but the terminology and specific aspects had to be changed to account i.a. for the extension of the design basis and facilitating its implementation.

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



Application of DiD approach form INSAG-10 to SSR 2/1

- INSAG-10 is still the basis for SSR- 2/1, but the terminology and specific aspects had to be changed to account i.a. for the extension of the design basis and facilitating its implementation.



New TECDOC: DiD approach of SSR 2/1. Elaboration on the original table form INSAG-10

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 3a	Control of design basis accidents (postulated single initiating events)	Engineered safety features (safety systems)	Emergency operating procedures
3b	Control of design extension conditions (postulated additional failures) to prevent core melt	Additional safety features	Emergency operating procedures
Level 4	Control of design extension conditions (postulated multiple failures events) to mitigate the consequences of severe accidents	Safety features for design extension conditions. Technical Support Centre	Complementary emergency operating procedures/ severe accident management 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

DiD for the Spent Fuel Pool

- SFP may be inside or outside the containment (in an adjacent building or area). The 3 Main Safety Functions must be always fulfilled.
- Use of the DiD approach (with a graded approach) leads to the interpretation of Plant Stages and DiD levels
  - **Normal Operation (level 1)**. Similar measures as with the reactor. High quality, conservative design, maintenance, cooling and purification systems, etc. to ensure the satisfactory operation and the prevention of failures and abnormal conditions.
  - **AOOs (level 2):** 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. Examples: loss of off-site power (LOOP), malfunction of decay heat removal system (including breaks), leaking of water of the pool, malfunctioning of the ventilation system, etc. Antisyphoning provisions are mandatory to avoid fuel uncovery
  - **Accidents, DBAs (3a):** Most designs don't have stand by safety systems. The normal operating systems (pool cooling, ventilation, etc.) are designed as safety systems. The essential means for level 3a are procedures to recover the cooling given the long time available. If not possible, it as handled as DEC. The drop of a fuel element or the loss of cooling can be considered as design basis for the ventilation system.
  - **DEC without fuel damage (3b):** The SBO is a one scenario affecting the whole plant, but for the SFP the time available is very long. For the loss of cooling, DEC provisions can be an alternative cooling system or means to refill the pool (they are also useful for SBO).
  - **DEC with fuel damage (level 4):** Fuel uncovery needs to be practically eliminated. It means a large release if the SFP is outside the containment or very demanding measures if inside the containment (massive hydrogen generation, zircaloy fires, a "spent fuel catcher", etc.). Its pays-off to focus on prevention also, given the time available.

Independence of DiD Levels
Prevention of common cause failures

*Paragraph 3.31 of the **IAEA Safety Fundamentals** 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. …"

SSR 2/1:

Requirement 24 indicates 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.

***New** 4.13a: "The SSC's at different 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".*

Independence of DiD Levels
Prevention of common cause failures

- DiD Levels are not and cannot be independent: Necessary sharing of SSCs (control room, containment, control rods), the operators and the impact of hazards, among other factors.
- "independence of the levels of DiD" needs be understood as the "**degree of independence**", which should be the highest possible.
- The TECDOC addresses the factors that affect the independence of levels of defence and measures to prevent common cause failures. Main factors are sharing SSCs between DiD levels and exposure to hazards
- The TECDOC provides general and specific recommendations for effective "independence" of levels of DiD
- The TECDOC addresses specifically:
  - Independence of DiD in relation to I&C systems.
  - The independence of power supply (AC&DC) between level 3a and 3b and in particular between level 3 and 4

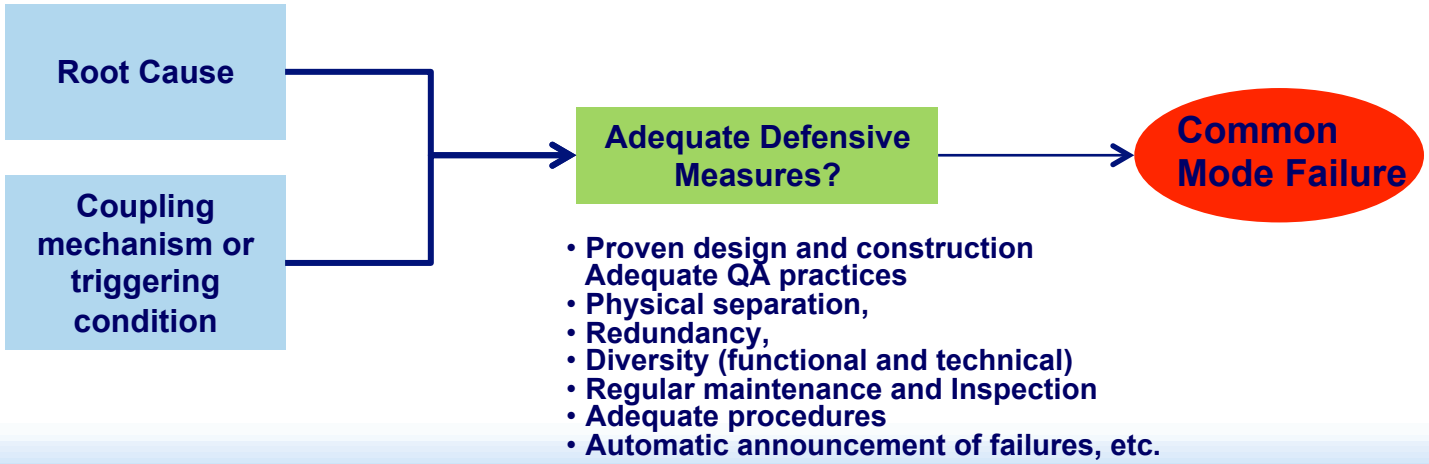
Independence of DiD Levels
Prevention of common cause failures

- The effectiveness of the levels of DiD can be jeopardized by sharing SSCs between DiD levels.
- In some cases the sharing leads to the bypass of a level, e.g. ATWS or SBO. (2 to 3b)
- Each level needs to achieve its own and necessary level of reliability. The multiplicity of the levels should not be a justification to weaken the efficiency of some levels for relying mainly on the efficacy of others
- Common cause failures (in a broad sense dependent failures) jeopardize the reliability within provisions at a given level of DiD if redundancy exists (application of single failure criterion) and the independence between levels of DiD
- Common cause failures need to be prevented or made very unlikely

Dependencies within or between DiD levels

- Functional Dependencies (Support systems) affecting redundant trains
- Common system interfaces
- Systems and components with multiple functions, e.g. for different DiD levels
- Failures/conditions induced by a PIE on plant SSCs.
- Operation errors

- Common cause failures (CCFs):
  - Failure/conditions caused by external hazards
  - 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
- **Measures to adequately prevent CCFs depend on the causes and coupling mechanisms**



Independence of DiD levels

- **General recommendations**:
  - The successive means required for a given PIE should be identified;
  - Two sets of consequential independent safety features are expected to prevent the core melt for any AOO.
  - Safety features specifically designed to mitigate the consequences of core melt accidents should be independent from those designed to prevent such accidents;
  - The ability of SSCs to perform their functions should not be affected by the initiating event and its consequences for which they are designed to respond;
  - Safety features, designed to back up SSCs implementing safety functions, should be independent from SSCs postulated as failed in the sequence;
  - Independence between SSCs or safety features should be achieved through the identification of all dependencies and the elimination of the most significant.
  - The safety analysis should demonstrate that the safety features intended to respond first are not jeopardized by the initiating event;

Independence of DiD levels

Specific recommendations:

- 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 3a and subsequent levels and within level 4, between SSCs necessary to prevent progression to core melt (level 3b) and SSCs necessary to mitigate the consequences of a core melt accident (level 4).
- Level 3a should be independent from levels 1 and 2 as far as reasonably practicable. To avoid challenging excessively level 3b or 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 AOOs (level 2).
- 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 3b.
- Specific Recommendations for I&C systems are also given

Design Margins – Avoidance of cliff edge effects

- When the design basis of an SSC is exceeded, failure is prevented by available margins. Margins are particularly important if exceeding them leads to a …

  cliff edge effect, i.e.. *an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another 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*. (IAEA)

  - The term was intensively stressed after the accident at the Fukushima accident. There are different interpretations.
  - WENRA definition: “A cliff edge effect happens where a small change in a parameter leads to a disproportionate increase in consequences”.

Design Margins – Avoidance of cliff edge effects

Cliff edge effects

- Cliff edge effect implies high consequences following a small deviation in a “parameter”
- The worst case would have a large release as the consequence.
- In general, other cliff edge effects would be the failure of a physical 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.
- Typical examples could be:
  - The failure of the containment, e.g. because of hydrogen detonation
  - Earthquake causing a LOCA
  - External hazards (e.g. flooding) failing some vital safety components or 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.

Design Margins – Avoidance of cliff edge effects

Design margins for DEC:

- Are expected to be smaller than those existing for DBA conditions. Req. 20 allows analyses for DEC to be best estimate and 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 stress behaviour limits justifying the integrity or operability of SSCs may be less conservative than those used for DBAs.
- Substantial differences between DEC without and with core melt are not made in SSR-2/1. For DECs without core melt the uncertainties are similar to those for DBAs. For DECs with core melt, the uncertainties are larger than those for DBAs.

- Revised SSR 2/1 requires larger margins for items ultimately necessary to prevent large or early radioactive releases and specifically against external hazards to avoid cliff edge effects.

Interpretation of the Concept of Practical Elimination

SSR 2/1: ***"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 term was already introduced in INSAG 12 (1990) and in the IAEA Safety Standards (NS-G-1.10 on Containment) in 2004.
- The "certain conditions" to be addressed referred to hypothetical accident sequences that could lead to early or large radioactive releases due to containment failure than can not be mitigated with implementation of reasonable technical means.
- 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

Interpretation of the Concept of Practical Elimination

- **1st step:** identify what are the conditions to be practically eliminated
- **2nd step:** identify design provisions for it
- **3rd step:** assessment of the provisions based on to DSA,PSA and engineering judgement

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. Very energetic phenomena in severe accident conditions for which technical solutions for maintaining containment integrity cannot be ensured.
   a. Core meltdown at high pressure (Direct Containment Heating)
   b. Steam explosion
   c. Hydrogen explosion
   d. Containment boundary melt-through
   e. Containment failure due to fast overpressurization
3. Non confined severe fuel damage
   a. Severe accident with containment by pass.
   b. Significant fuel failure in a storage pool

Interpretation of the Concept of Practical Elimination

- **Example: Reactor Pressure Vessel break**:
  - Exceptional case. The failure would invalidate the DiD (Failure of level 1 leads to level 5)
  - The safety demonstration needs be especially robust and demanding, in order that an engineering judgment can be made for the following key requirements:
    - the most suitable composition of materials needs to be selected;
    - the metal component or structure should be as defect-free as possible;
    - the metal component or structure should be tolerant of defects.;
    - the mechanisms of growth of defects are known
    - design provisions and suitable operation practices are in place to minimize thermal fatigue, stress corrosion, embrittlement, PTS, overpressurization, etc.
    - an effective in service inspection and surveillance programme is in place during the manufacturing and the operation

  The demonstration needs to ensure a very high level of reliability (structural integrity) based upon the fulfilment of the key requirements in design manufacturing and operation.

  Role of PSA limited

Interpretation of the Concept of Practical Elimination

- **Demonstration of Practical Elimination**
  - Wherever possible based on physical impossibility (e.g. insufficient hydrogen/oxygen concentration, intrinsic safety coefficients, etc.)
  - Justification need to rely on design features and operational means to prevent the conditions
  - Combined use DSA & PSA (not limited to Boolean models). The degree of confidence remains often an issue.
  - The arguments and methods for justification depend highly on the case.
  - It cannot alone be achieved by showing the compliance with a general probabilistic value. This should not be considered as a justification for not implementing reasonable design or operational measures

- **Proposal for definition (limited to events of internal origin):**

  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.

Design for External Hazards

Equipment ultimately necessary to prevent early or large releases

SSCs ultimately necessary to prevent early or large release refer to DiD level 4 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 it includes 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 .

Design for natural external hazards exceeding the design bases

Two 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 these SSCs
2. To demonstrate, following a BE approach, with high level of confidence that values of parameters for which cliff edge effects would occur are not reached because of adequate design margin.

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.

Interpretation of the Concept of Practical Elimination

- **Example: Hydrogen detonation**
  - Demonstration needs to rely con containment volume, inert atmosphere, adequate number and design of recombiners, etc.
- **Example: High pressure core melt conditions**
  - The demonstration requires design provisions, such as a diverse system and automatic system to depressurize the reactor coolant system
  - PSA useful to assess the reliability of the depressurization system
- **Example: Containment by-pass**
  - All sequences with core damage and containment by pass need to be eliminated
  - Paths need to be identified (SGTR, uninsulated penetrations, etc.)
  - PSA is useful in assessing reliability of isolation provisions (Req. 56)
- **Example: Containment boundary melt-through**
  - Provisions need to be made to ensure the stabilization of the core inside the vessel or outside the vessel (core catcher) to prevent that the corium reachs the containment wall.
  - Role of PSA case specific

- **General severe accident conditions (slow progressing phenomena):**
  - The containment and its systems, specifically designed for SAs, should be capable of contributing to the reduction of radioactive releases to a frequency and magnitude that only require outside actions limited in area and time (typical level 2 PSA assessment but for a plant designed for SAs).

Use of Non Permanent Equipment

- What is not permanent is not part of the design.
- After the Fukushima accident the revision of SSR 2/1 requires design provisions to enable the connection of some types of non permanent equipment in a smooth and safe manner (for situations exceeding the design basis).
- For new plants, the features for hooking up non permanent equipment should not be necessary for DBA and DEC.

Thank you for your attention !