IAEA 60 Years
Atoms for Peace and Development

Joint IAEA-ICTP Essential Knowledge Workshop on Nuclear Power Plant Design Safety

ICTP/Trieste, 9 – 20 October 2017

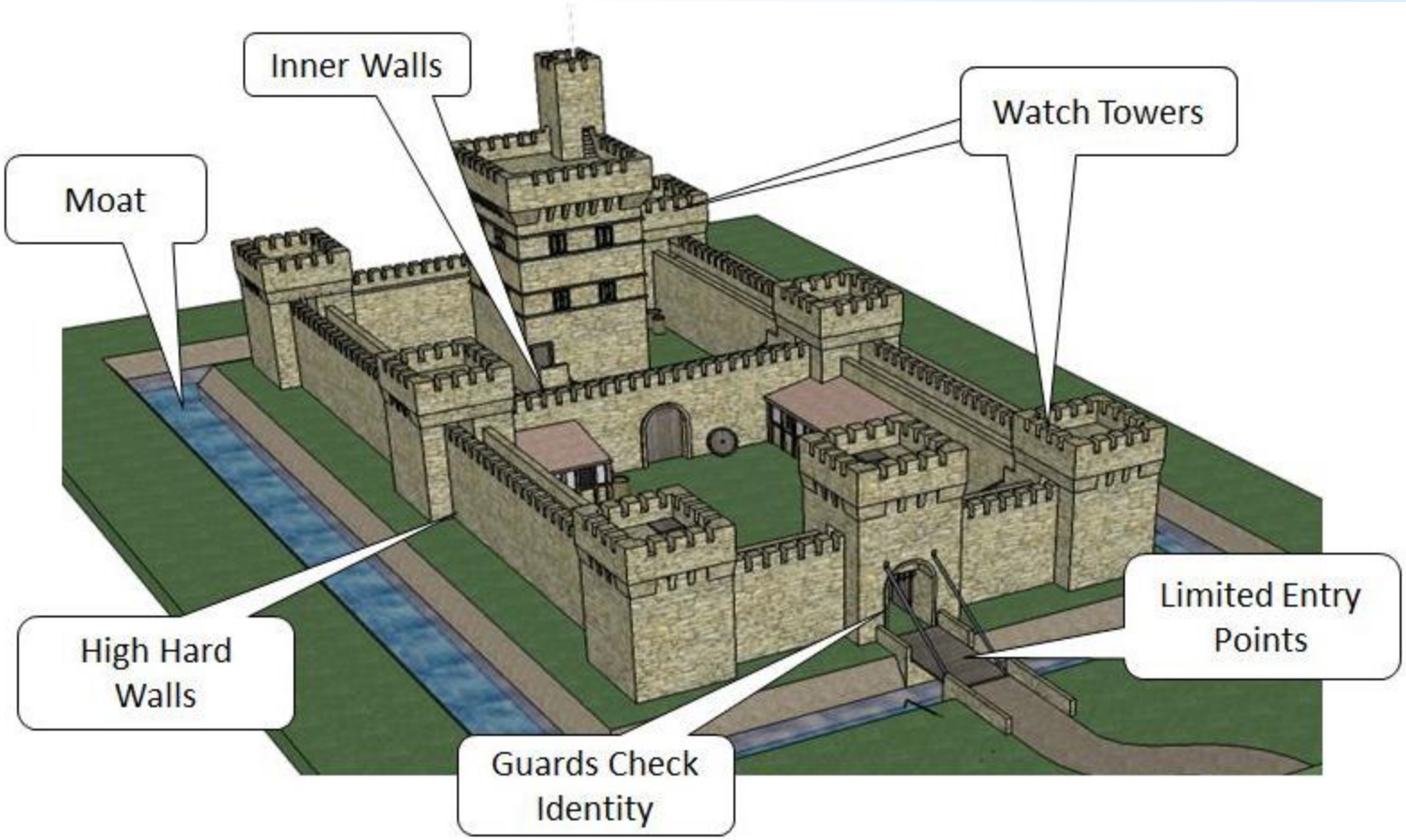
Assessment of Defence in Depth

Javier YLLERA
Safety Assessment Section
Division of Nuclear Installation Safety

Outline

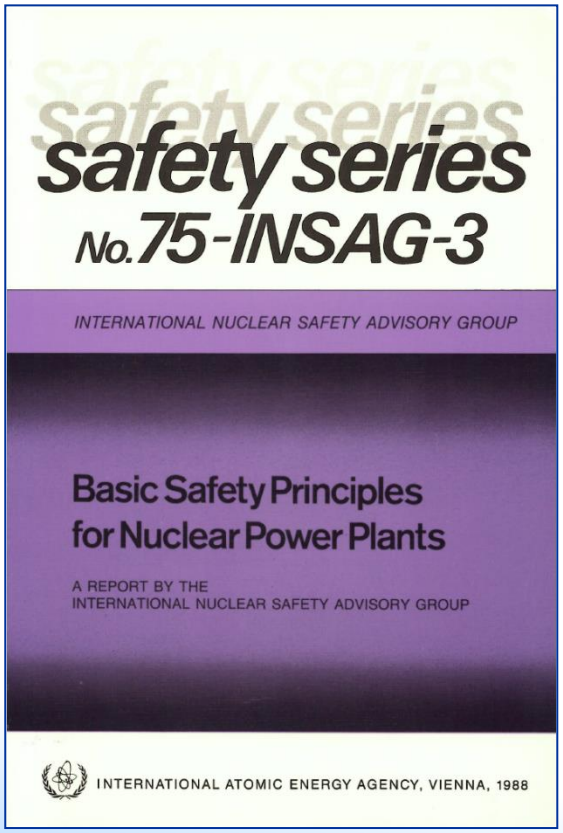
- Survey of the relevant IAEA publications on defence in depth
- Activities, current and future challenges
- Implementation and Assessment of DiD

Old and simple concept



INSAG-3 published in 1988

- The concept of defence in depth was used in nuclear safety for long time. The term was better defined following the Chernobyl accident but the five levels were first described in INSAG-3, published in 1988.



Defence in depth

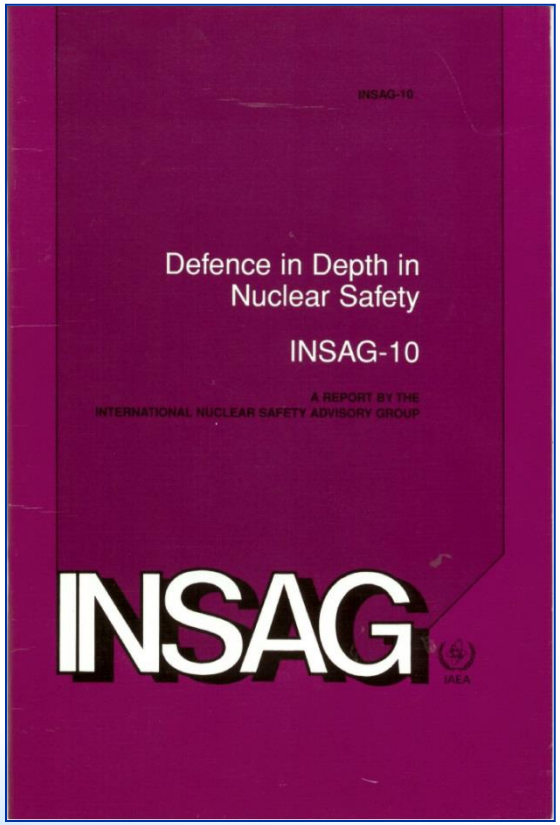
46. *Principle: To compensate for potential human and mechanical failures, a defence in depth concept is implemented, centred on several levels of protection including successive barriers preventing the release of radioactive material to the environment. The concept includes protection of the barriers by averting damage to the plant and to the barriers themselves. It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective.*

(…)

Defence in depth helps to establish that the three basic safety functions (controlling the power, cooling the fuel and confining the radioactive material) are preserved, and that radioactive materials do not reach people or the environment.

INSAG-10 published in 1996

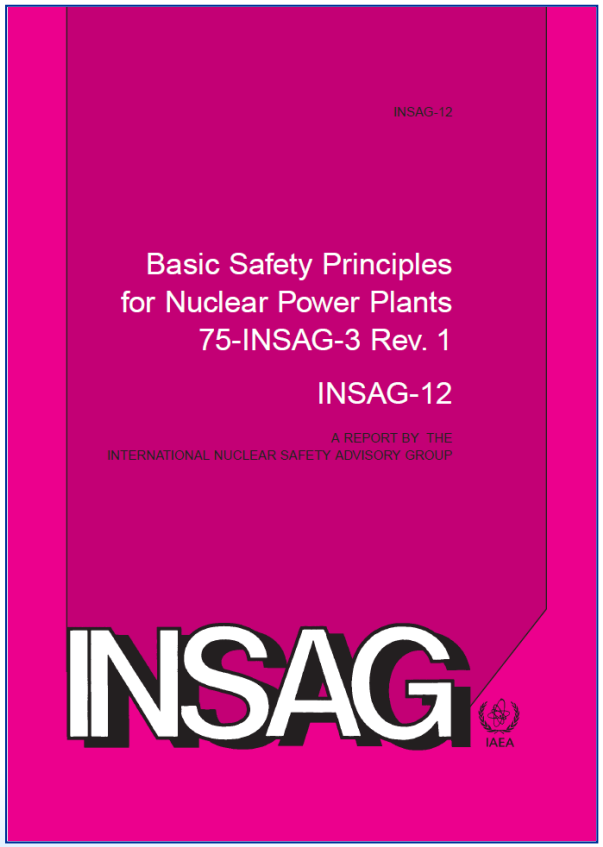
INSAG-10 presented a very detailed description of the concept of defence in depth including a table with the objective and the essential means of each level of defence.



Levels of defence in depth	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

INSAG-12 (INSAG-3 Rev.1) published in 1999

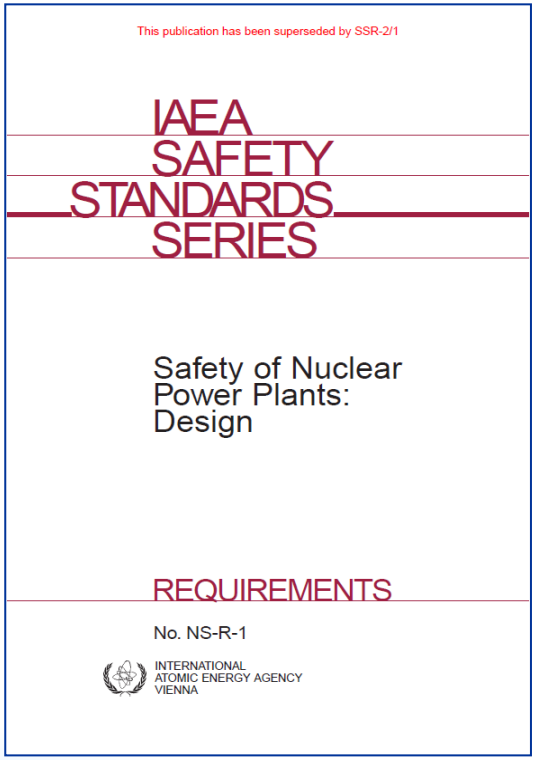
INSAG-12 elaborates the table of INSAG-10 introducing a link between plant states and levels of defence in depth.



Strategy	Accident prevention			Accident mitigation	
Operational state of the plant	Normal operation	Anticipated operational occurrences	Design basis and complex operating states	Severe accidents beyond the design basis	Post-severe accident situation
Level of defence in depth	Level 1	Level 2	Level 3	Level 4	Level 5
Objective	Prevention of abnormal operation and failure	Control of abnormal operation and detection of failures	Control of accidents below the severity level postulated in the design basis	Control of severe plant conditions, including prevention of accident progression, and mitigation of the consequences of severe accidents, including confinement protection	Mitigation of radiological consequences of significant releases of radioactive materials
Essential features	Conservative design and quality in construction and operation	Control, limiting and protection systems and other surveillance features	Engineered safety features and accident procedures	Complementary measures and accident management, including confinement prodection	Off-site emergency response
Control	Normal operating activities		Control of accidents in design basis	Accident management	
Procedures	Normal operating procedures		Emergency operating procedures	Ultimate part of emergency operating procedures	
Response	Normal operating systems		Engineered safety features	Special design features	Off-site emergency preparations
Condition of barriers	Area of specified acceptable fuel design limit		Fuel failure; Severe fuel damage; Fuel melt	Uncontrolled fuel melt	Loss of confinement
Colour code	NORMAL		POSTULATED ACCIDENTS		EMERGENCY

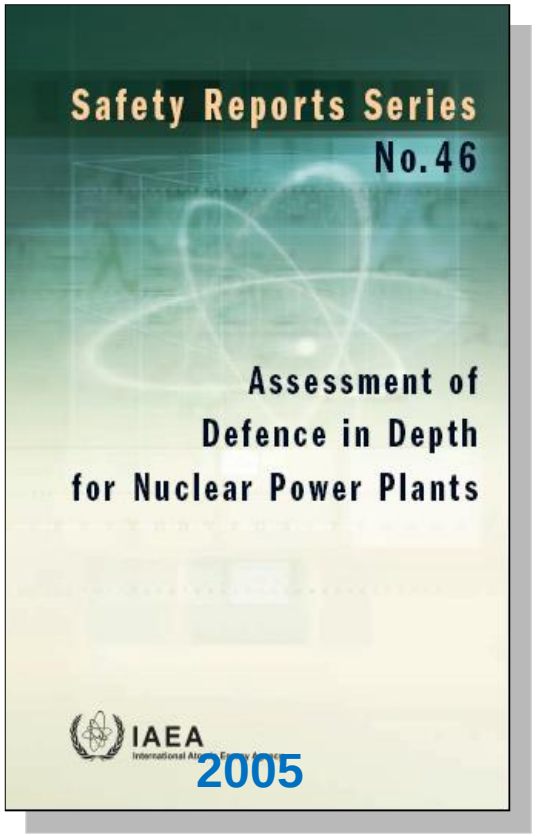
NS-R-1 published in 2000

NS-R-1 adopted the concepts and the terminology of INSAG-10.
Recognizes that defence in depth is a main pillar for generating safety requirements for design of NPPs
Includes several requirements that explicitly address defence in depth



Levels of defence in depth	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

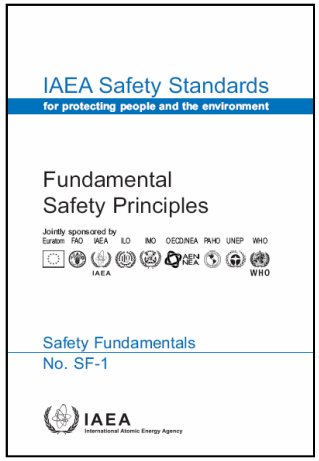
Safety Reports Series No. 46



- In 2005, IAEA published a report in Safety Report Series (No. 46) 'Assessment of Defence in Depth for Nuclear Power Plants'

  It describes a screening method for assessing the defence in depth capabilities of an existing plant, including both its design features and the operational measures taken to ensure safety

SF-1 published in 2006



Principle 8: Prevention of accidents

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

3.31. The primary means of preventing and mitigating the consequences of accidents is 'defence in depth'. (…) When properly implemented, defence in depth **ensures that no single** technical, human or organizational failure could lead to harmful effects, and that the combinations of failures that could give rise to significant harmful effects are of very low probability. **The independent effectiveness of the different levels of defence is a necessary element of defence in depth.**

3.32. Defence in depth is provided by an appropriate combination of:

— An effective management system with a strong management commitment to safety and a strong safety culture.

— Adequate site selection and the incorporation of good design and engineering features providing safety margins, diversity and redundancy, mainly by the use of:
  - Design, technology and materials of high quality and reliability;
  - Control, limiting and protection systems and surveillance features;
  - An appropriate combination of inherent and engineered safety features.

— Comprehensive operational procedures and practices as well as accident management procedures.

Fundamental Safety Principles

Safety Objective:

Protect people and the environment from effects of radiation

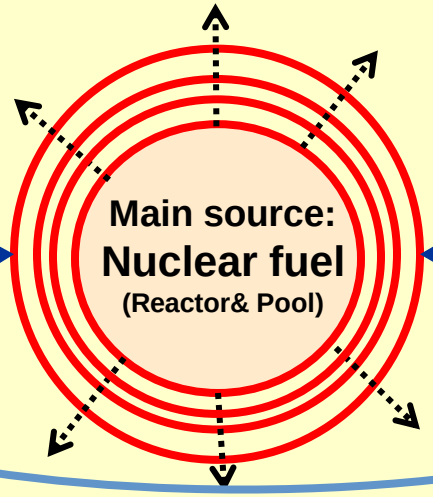
- **10 Safety principles:**

No. 8: Prevention and mitigation of accidents

Defence in depth

Based on a number of consecutive levels of protection

including physical barriers.



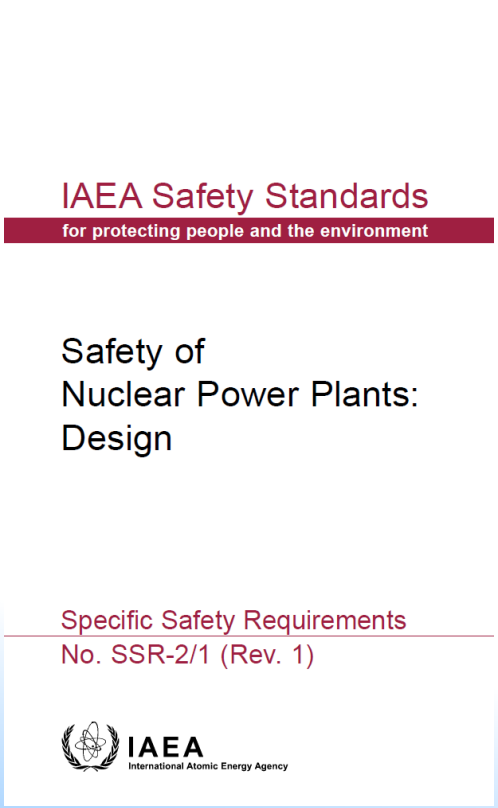
Fundamental Safety Functions

- Control of reactivity
- Removal of heat from the fuel
- Confinement of radioactive material and shielding

The current implementation of DiD at nuclear power plants comprises **5 levels** of protection and it is based on 4 physical barriers (fuel matrix, fuel cladding, reactor coolant boundary and containment building)

Defence in Depth
SSR-2/1, published in 2012/Revised 2016

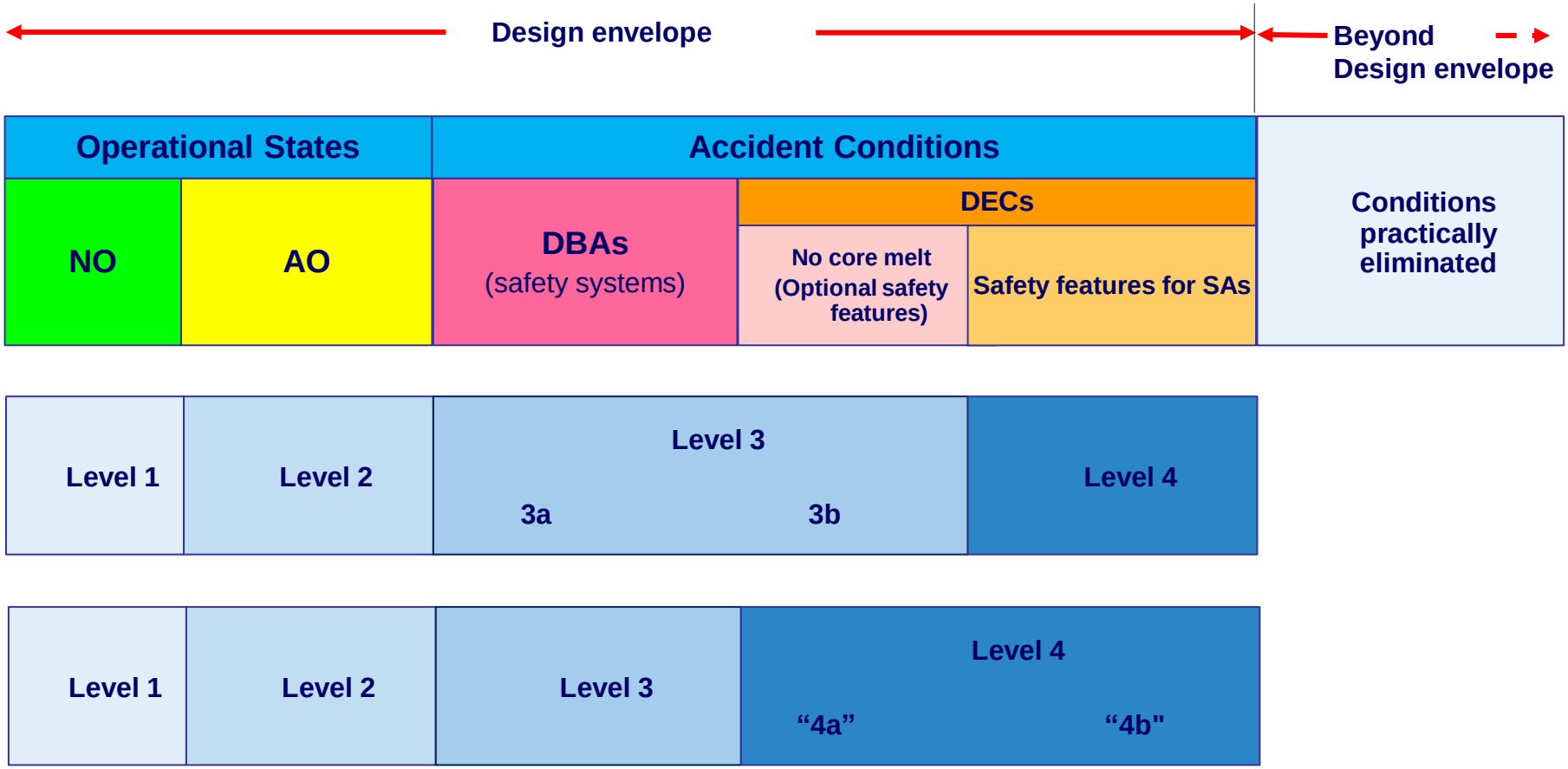
SSR-2/1 maintained the structure and the approach to defence in depth of NS-R-1
SSR-2/1 introduced the concept of Design Extension Conditions (DECs) without differentiating between DECs without and with core melting
SSR-2/1 did not make explicit associations between plant states and levels of defence in depth in any requirement



- The introduction of DECs implies some modifications to the table of Defence in Depth correlating plant states and levels of defence;
- Level 4 is reinforced by requirements for the essential means necessary to mitigate the consequences of severe accidents:
  - SSCs for DECs shall be independent to the extent practicable of those used in more frequent accidents, (SSR-2/1 Req. 5.29 (a);
  - SSCs are capable of performing their intended functions under environmental conditions prevailing during DECs (SSR-2/1 Req. 5.29 (b)

Plant Sates & DiD

SSR-2/1



TECDOC -1791: DiD approach of SSR 2/1. Elaboration on the original table form INSAG-10

Level of defence Approach 1	Objective	Essential design means	Essential operational means	Level of defence Approach 2
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 1
Level 2	Control of abnormal operation and detection of failures	Limitation and protection systems and other surveillance features	Abnormal operating procedures/emergency operating procedures	Level 2
3a	Control of design basis accidents (postulated single initiating events)	Engineered safety features (safety systems)	Emergency operating procedures	Level 3
Level 3 3b	Control of design extension conditions to prevent core melting	Safety features for design extension conditions without core melting	Emergency operating procedures	4a
Level 4	Control of design extension conditions to mitigate the consequences of severe accidents	Safety features for design extension conditions with core melting. Technical Support Centre	Complementary emergency operating procedures/ severe accident management guidelines	Level 4 4b
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	Level 5

Principal Technical Requirements

- **Requirement 7: Application of defence in depth**

  The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable.

  – The design shall take due account of the fact that the existence of multiple levels of defence is not a basis for continued operation in the absence of one level of defence. All levels of defence in depth shall be kept available at all times and any relaxations shall be justified for specific modes of operation.
  – The design:
    a) Shall provide for multiple physical barriers to the release of radioactive material to the environment;
    b) 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;

Principal Technical Requirements

- **Requirement 7: Application of defence in depth ….**
  - c) Shall provide for the control of plant behaviour by means of inherent and engineered features, such that failures and deviations from normal operation requiring actuation of safety systems are minimized or excluded by design, to the extent possible;
  - d) Shall provide for supplementing the control of the plant by means of automatic actuation of safety systems, such that failures and deviations from normal operation that exceed the capability of control systems can be controlled with a high level of confidence, and the need for operator actions in the early phase of these failures or deviations from normal operation is minimized; Shall provide for systems, structures and components and procedures to control the course of and, as far as practicable, to limit the consequences of failures and deviations from normal operation that exceed the capability of safety systems;
  - e) Shall provide multiple means for ensuring that each of the fundamental safety functions is performed, thereby ensuring the effectiveness of the barriers and mitigating the consequences of any failure or deviation from normal operation.

Principal Technical Requirements

- **Requirement 7: Application of defence in depth …**
  - To ensure that the concept of defence in depth is maintained, the design shall prevent, as far as is practicable:
    a) Challenges to the integrity of physical barriers;
    b) Failure of one or more barriers;
    c) Failure of a barrier as a consequence of the failure of another barrier;
    d) The possibility of harmful consequences of errors in operation and maintenance.
  - The design shall be such as to ensure, as far as is practicable, that the first, or at most the second, level of defence is capable of preventing an escalation to accident conditions for all failures or deviations from normal operation that are likely to occur over the operating lifetime of the nuclear power plant.
  - The levels of defence in depth shall be independent as far as practicable to avoid the 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 as far as is practicable be independent of safety systems.

Independence of DiD Levels
Prevention of common cause failures

- **SSR 2/1: Common Cause Failures**

  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.

IAEA International Conference on Topical Issues in Nuclear Installation Safety:

Defence in Depth — Advances and Challenges for Nuclear Installation Safety held in Vienna, 21-24 October 2013

President's Conclusions and Recommendations

Among the president's conclusions there was a confirmation of importance and value of DiD for both existing and new plants. In the conclusions a number of ideas were presented with the objective of further strengthening DiD, such us:

- Strengthening of DiD in accordance with the most recent safety objectives reflected in new IAEA Safety Standards (in particular attention paid to level 4 of defence and to independence of levels) and its maintenance by periodic safety reviews over the entire life of the plants
- Further development of guidance documents and tools for assessment of required new features of defence in depth
- Special attention to be paid to potential effects of extreme external hazards jeopardizing simultaneously several levels of defence
- Providing additional guidance on effects of hazards and combination of hazards, of human factor and reliability of I&C systems on defence in depth
- Taking into account operational experience feedback and results of research and development in implementation of defence in depth

Current and future challenges

- **Adequate robustness of SSCs of different levels of defence in depth**
- **Independence of levels of defence in depth**
- **Protection of SSCs of different levels of defence in depth against external events**
- **Safety classification and qualification of SSCs of different levels of defence in depth**

Revision of Safety Guide on Format and Content of SAR.

Defence in depth

- *3.3.12. This section should describe the approach adopted to incorporate the defence in depth concept into the design of the plant. It should be demonstrated that the defence in depth concept has been considered in all stages of the lifetime of the nuclear power plant, for all plant states and for all safety related activities in accordance with SSR-2/1 (Rev.1), paras 2.12 to 2.18 [3]. It should also be demonstrated that measures are taken for adequate robustness and independence of levels. Particular emphasis should be placed in describing how independence of safety systems and safety features for design extension conditions with core melting is approached.*
- *3.3.13. It should be demonstrated that there are physical barriers to the release of radioactivity and systems to protect integrity of the barriers and measures are taken to ensure robustness of provisions at each level of defence in depth.*
- *3.3.14. Where appropriate, any envisaged operator actions to mitigate the consequences of events and to assist in the performance of important safety functions essential for defence in depth should be described.*
- *3.3.15. Where appropriate, any envisaged support needed outside the plant site should be described.*

Assessment of DiD Implementation (proposed new SG)

- DiD implementation strategy for new NPPs (general part)
  - Objective of levels of DiD and plant states
  - Assessment of effectiveness and reliability of the design provisions:
    - Identification of safety functions and challenging mechanisms (e.g. PIEs, sequences, hazards and phenomena)
    - Identification of safety provisions for the applicable plant state
    - Deterministic assessment (demonstration of compliance with applicable requirements supported by the complete safety analysis)
    - Probabilistic assessment (assessment of reliability of the design provisions)
    - Integration of deterministic and probabilistic assessment
- Assessment of safety provisions for different plant states: Assessment of safety provisions for NO (all modes), AOOs, DBA, DEC without and with core melt
- Assessment of independence between safety provisions for different plant states
  - Functional independence between different plant states
  - Assessment of common cause failures and defensive mechanisms, including use of PSA for identification and assessment of dependencies

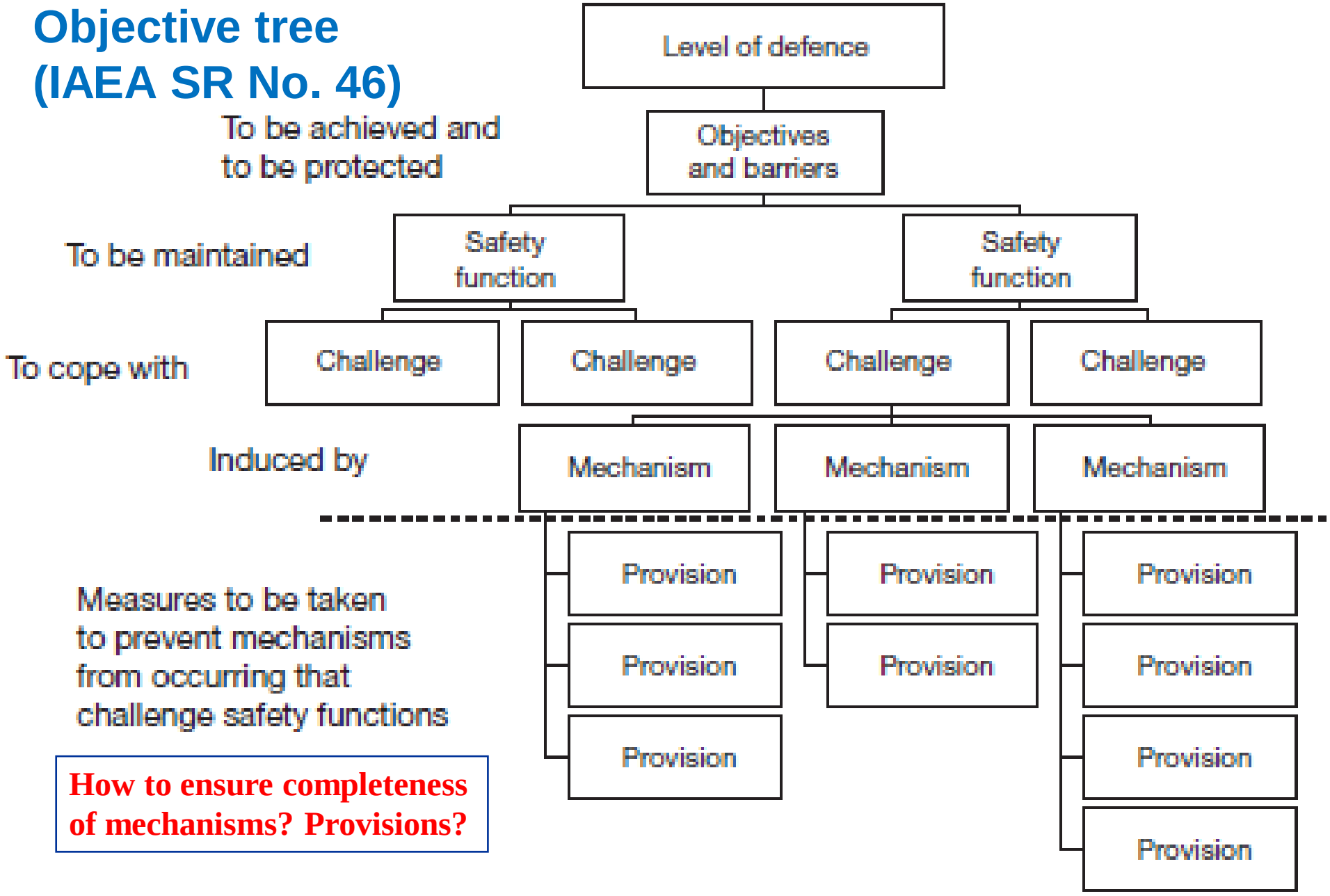
Application of Defence in Depth

- Defence in depth concept : a simple and logical concept
- Avoid harmful consequences by providing several levels of defense in series:

"Should one level fail the subsequent level will come into play"

Independence is implicitly embarked in the concept

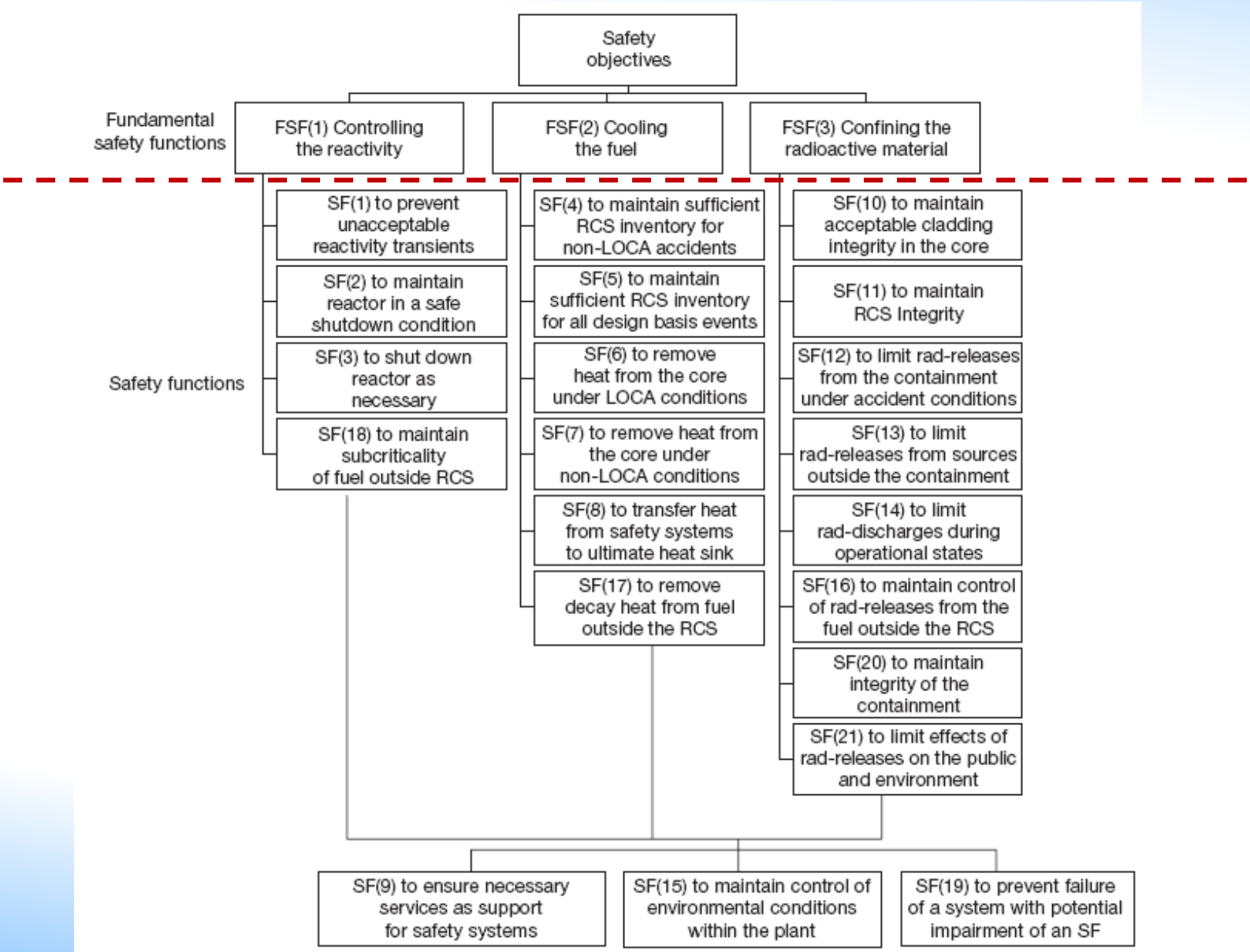
Objective tree (IAEA SR No. 46)



How to ensure completeness of mechanisms? Provisions?

FIG. 2. Structure for defence in depth provisions at each level of defence.

Fundamental and derived safety functions - Conditions for ensuring integrity of barriers



Objective ProvisionTrees

- Objective trees developed to provide a comprehensive list of the possible options for provisions (not necessarily all of them need to be implemented in parallel).
- For each safety principle and corresponding level(s) , challenges and mechanisms that affect corresponding safety functions were provided
- The provisions offered in the objective trees were mainly derived from the IAEA and INSAG safety principles, the IAEA Safety Standards and on the basis of an additional engineering judgment

SR-46 Methodology and update needs

- SR-46 is a systematic way for screening of comprehensiveness of defence in depth.
- The screening approach, which uses graphical way of objective trees, offers a tool for determining the strengths and weaknesses of defence in depth at a specific plant.
- The top down approach has been used for the development of objective trees, i.e. from stating the objectives and relevant safety functions for each level of defence, through the challenges to performance of these safety functions composed of various mechanisms affecting the performance, up to the provisions which may be implemented to prevent challenges to safety functions to take place.
- The approach did not include any quantification of the extent of defence in depth at a plant nor a prioritization of the provisions of defence.

SR-46 Methodology and update needs

- It was originally intended only for screening, i.e. for identification of both the strengths and weaknesses for which provision should be considered.
- There were no strict criteria on what is considered a sufficient level of implementation of individual provisions.
- The level of detail and completeness of evaluation are at the discretion of the user of the screening approach.
- Among the IAEA Conference president's conclusions, further development of the tools based on the methodology described in the Safety Report was recommended as a means for ensuring that defence in depth safety provisions are comprehensive enough.
- There is a need to align SR-46 with the new Safety requirements for Design (SSR 2/1) and Operation (SSR 2/1), for instance considering new plant states (DEC) and definition of the levels
- The approach does yield quantitative results within one level or measures of dependencies between levels. However, this is essential for the assessment of DiD

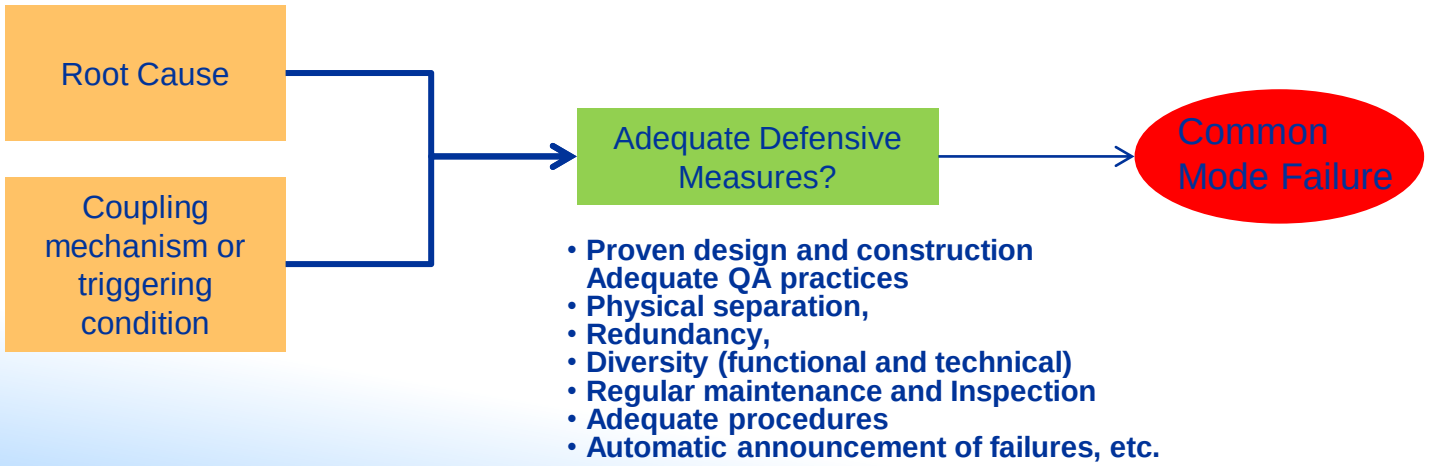
Independence of DiD Levels
Prevention of common cause failures (CCFs)

- CCFs (in a broad sense dependent failures) are defined as the failure of two or more structures, systems or components due to a related root cause.
- The effectiveness of the levels of DiD is reduced by sharing SSCs between DiD levels.
- In some cases the sharing leads to the bypass of a level, e.g. ATWS or SBO.
- Each level needs to achieve its own and necessary level of reliability.
- CCFs jeopardize the reliability within provisions at a given level of DiD if redundancy exists and the independence between levels of DiD. Diversity is effective against some root causes of common cause failures
- High reliability requires that vulnerabilities for CCF should be eliminated to a reasonable extent.

Existing 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**



Common Cause Failures (CCFs)

A CCF is an unpredictable latent fault which may be revealed when an initiating event triggers the actuation of the equipment affected causing the fault of two or more redundancies of a system. Periodic testing, continuous monitoring, and other measures may allow an early detection of CCFs.

Although common cause failures are considered to be beyond the deterministic design rules of the safety systems architecture, a diversity and defense in depth analysis proving that vulnerabilities to CCF have been adequately addressed is expected.

Independence of DiD levels

- **General recommendations**:
  - The successive means required for a given PIE should be identified;
  - 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
Prevention of common cause failures

- Independence between levels of defence does not replace independence between redundancies implemented within one level, and both of them should be considered for the evaluation of the overall effectiveness of the defence in depth concept.

- Strengthening one level or the architecture cannot be an excuse to the decrease the reliability of the individual levels.

- Ideal design where each SSC would be allocated to a single level is unrealistic and could lead to useless complexity

- How far independence between levels should be implemented is not totally clear and might explain weaknesses in its application.

Common Cause Failure (CCF)

The need to provide a diverse system or equipment can be identified by either or both probabilistic and deterministic approaches and it depends both on the estimate of the consequences and the estimated frequency of occurrence of the initiating event.

Nevertheless where the risk is high a deterministic approach is preferred.

Consequently, a CCF may be postulated between all the redundancies of systems designed to control AOOs and the most frequent DBA, if diversity between them cannot be justified, with the goal to prevent the initiating event from escalating to a core melt accident.

If a need for a back up is identified, then diverse means should be provided.

Note: Two components might be considered as diversified enough if the elimination of the likely common failure modes identified can be justified

Common Cause Failure (CCF)

Independence between SSCs should be pursued through the identification of dependencies and their elimination to the greatest practicable extent.

CCF may be initiated by:

- propagation of the effects of an external or internal hazard,
- propagation of a failure,
- unpredictable latent fault in design, manufacturing, etc.

High reliability requires that vulnerabilities for CCF should be eliminated to a reasonable extent.

- segregation and independence is effective to prevent propagation,
- Diversity is more appropriate to eliminate latent faults.

1-Vulnerabilities which could result in failure of the safety systems should be identified

2-Combinations with PIE should be considered or postulated to assess if they could escalate to a core melt accident

3-Usually, where consequences exceed those accepted for DBAs a change in the layout or, the implementation of safety features unlikely to be subjected to the same common cause failure, is needed.

Common Cause Failure (CCF)

- For modern I&C systems, in particular systems whose functionality depends upon software, and irrespective of all preventive measures, demonstration that I&C system is proven to be error free is very difficult and may always be disputed.
- Therefore, combination of credible PIE with CCF in the I&C should be postulated .
- Verification that the overall I&C design adequately addresses the potential for common cause failure (CCF) is expected.

*

CCF vulnerabilities may be addressed by eliminating the vulnerability, or justifying acceptance of the vulnerability:

- Vulnerabilities for combination of credible PIE with CCF in I&C leading to (significant) core damage should be removed,
- Realistic hypotheses may be used to assess the consequences and to demonstrate the efficiency of the diverse provision when implemented.

Diversity is a way to reduce CCF vulnerability resulting from design, manufacturing or maintenance error, and to include conservatism to compensate for the difficulty of demonstrating the specified level of reliability.

E.g: Diverse Actuation System (DAS), which provides a diverse sub-set of backup protection system functions is more and more often implemented where the Reactor Protection System uses digital technology.

Diverse means should be selected not to be subjected to the same CCF and should be of appropriate reliability to rule out of the design a simultaneous failure of the RPS and its back up.

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, etc.). **There is no level 4 of DiD for the SFP**

IAEA 60 Years
Atoms for Peace and Development

Thank you!