ÚJV Řež, a. s.

Defence in depth: assessment of comprehensiveness and further strengthening of the concept

Jozef Misak

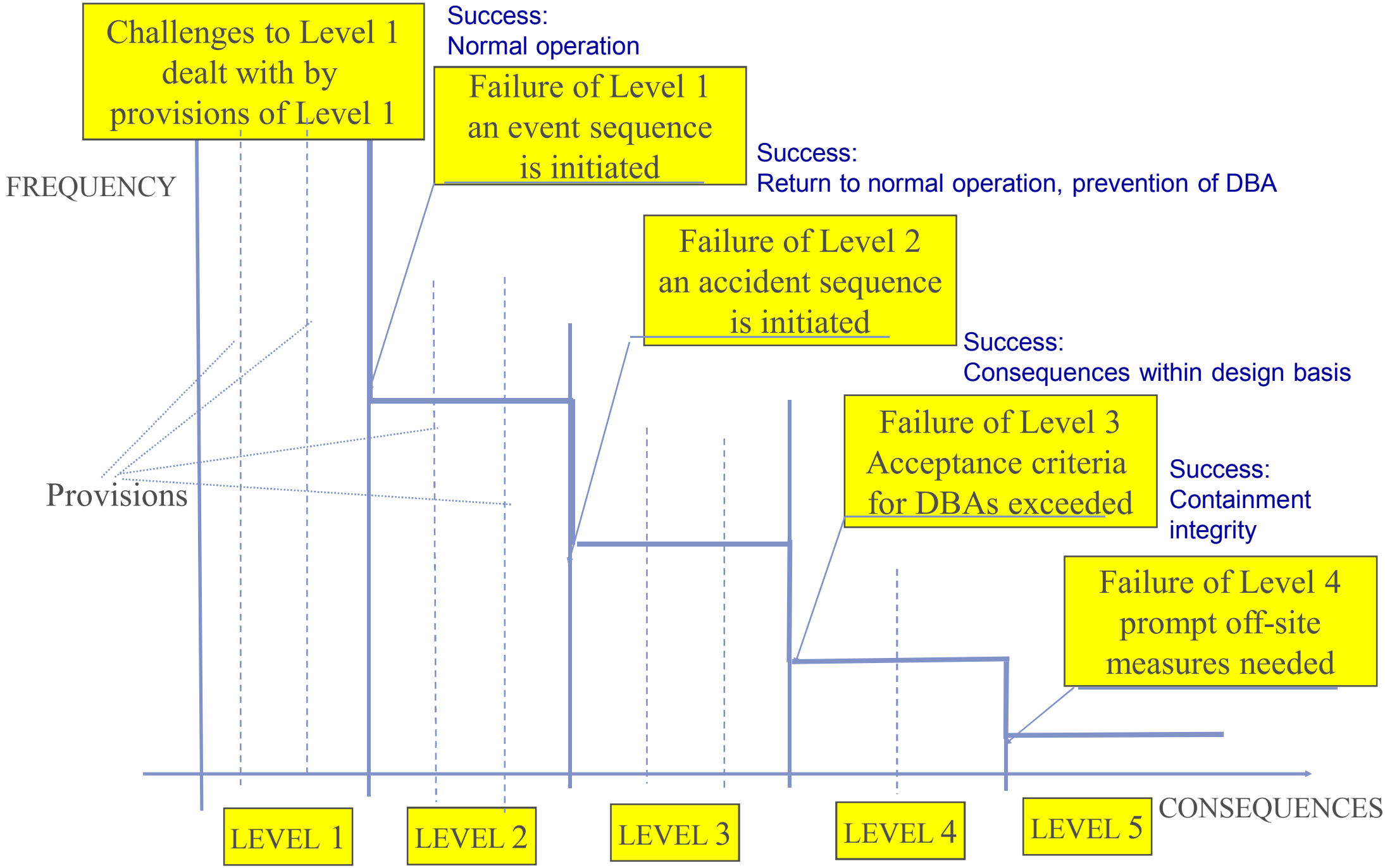
IAEA International Conference on Topical Issues in Nuclear Installation Safety: Defence in Depth — Advances and Challenges for Nuclear Installation Safety

IAEA Vienna, 21-24 October 2013

Content

- **Approach for screening of comprehensiveness of provisions for defence in depth**
- **Scope and limitations of the screening approach**
- **Selected issues associated with strengthening of defence in depth**
  - Practical elimination
  - Consideration of multiple failures
  - Addressing independence and diversity of provisions for different levels of defence in safety analysis
- ***Acknowledgment: Second part of this presentation has been prepared based on the discussion of the ETSON Working Group 11 on "Safety Concepts, Defence-In-Depth"***

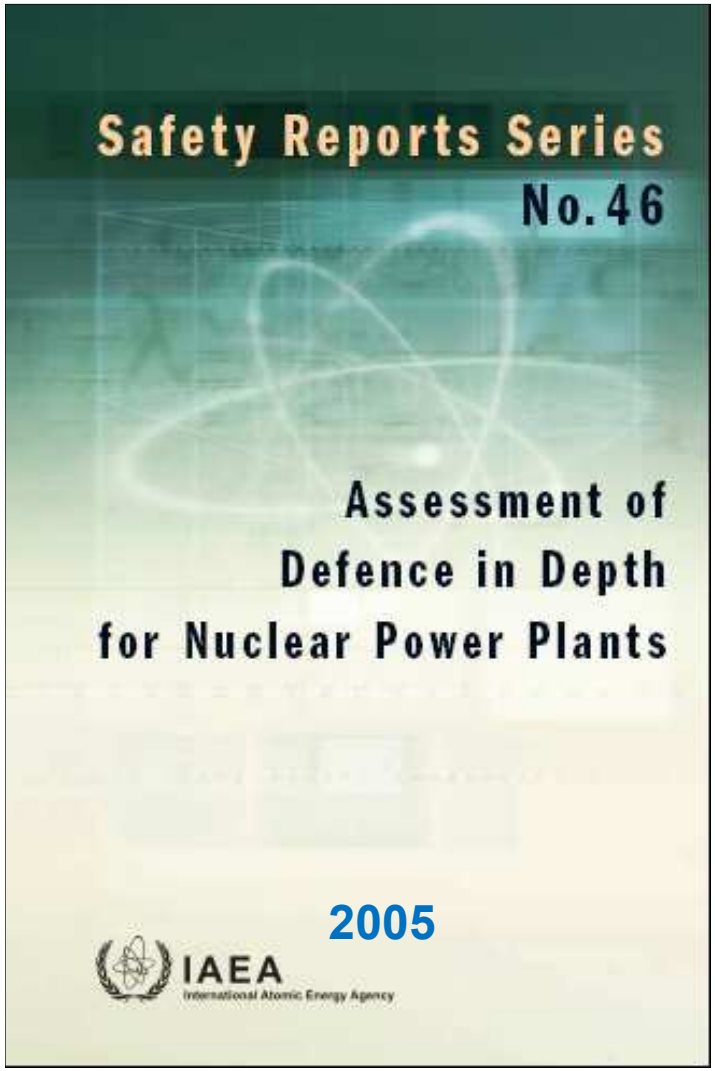
Correlation of levels of defence and success criteria



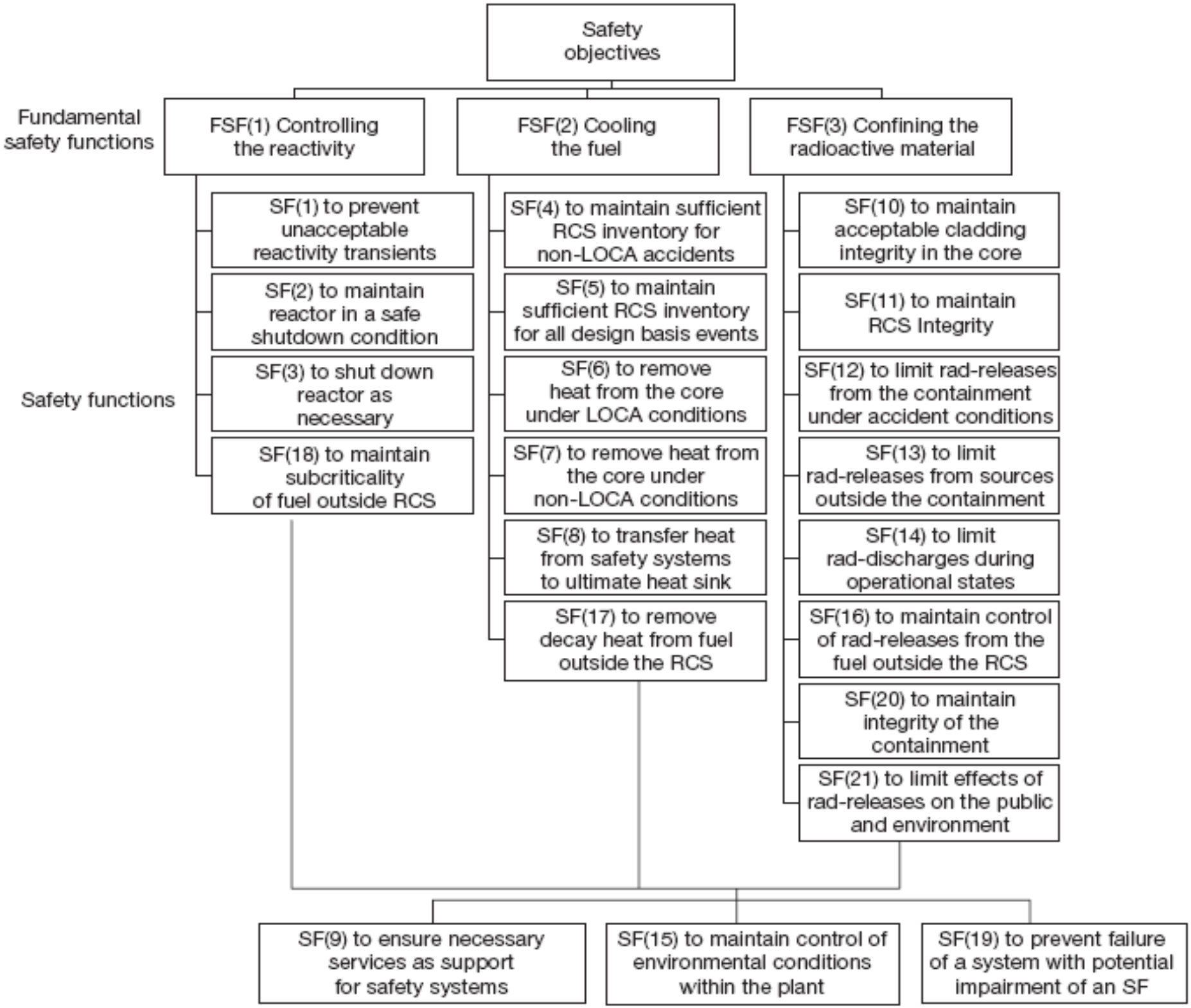
Comprehensiveness of safety provisions (measures)

- **Variety of safety provisions: organizational, behavioural and design measures, namely**
  - inherent safety characteristics
  - safety margins
  - active and passive systems
  - operator actions specified in procedures and guidelines
  - organizational measures
  - safety culture aspects
- **All NPPs declare to be built in accordance with defence in depth concept**
- **How to ensure that a set of provisions is comprehensive enough?**
- **A reference method to screen the comprehensiveness of implementation of defence in depth is needed**
- **How to ensure that a set of provisions is adequate?**

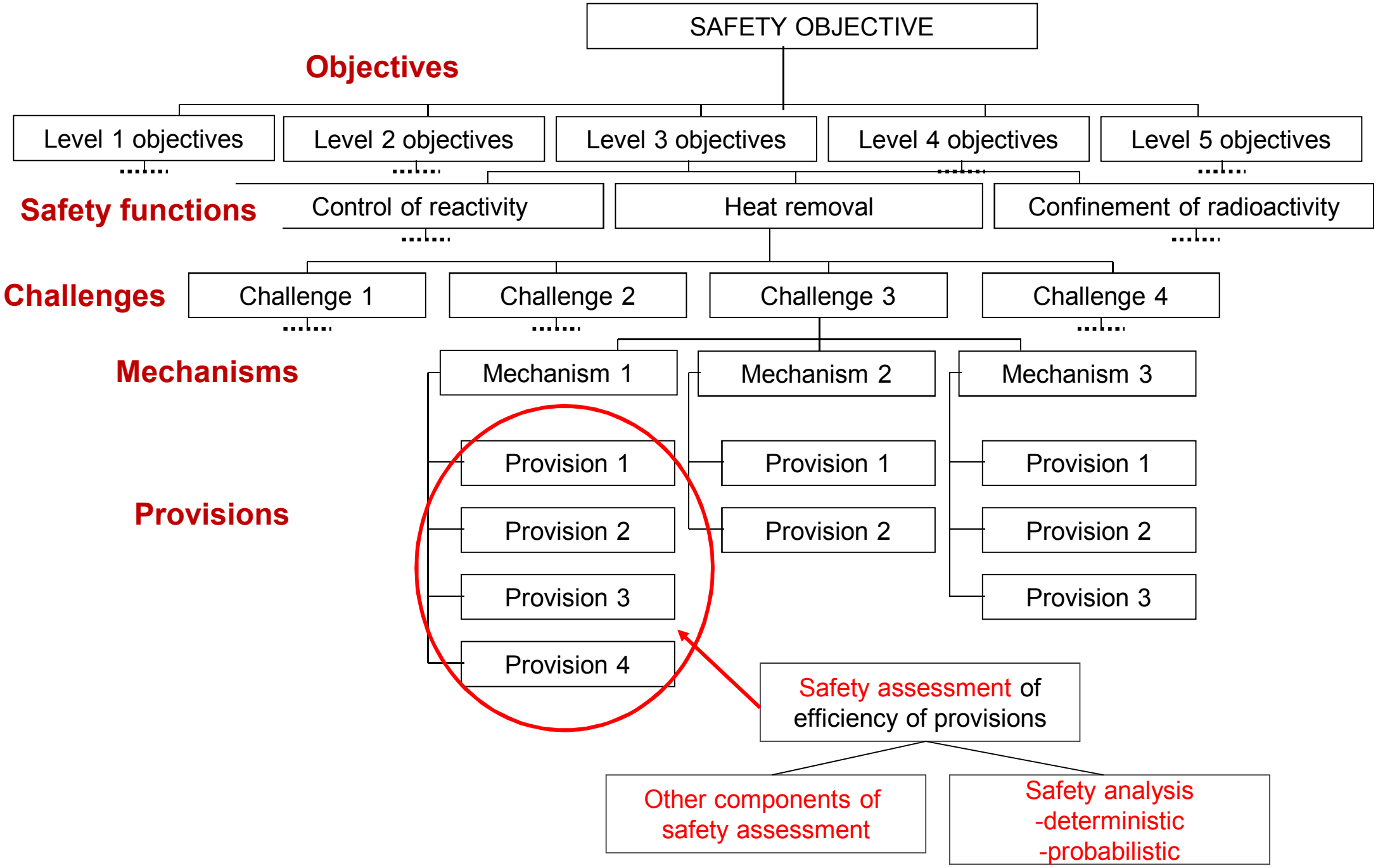
Safety Reports Series No. 46



- **In 2005, IAEA published a report in Safety Report Series (#46) 'Assessment of Defence in Depth for Nuclear Power Plants'**
  - Description of 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


Safety objectives
Fundamental safety functions
FSF(1) Controlling the reactivity
FSF(2) Cooling the fuel
FSF(3) Confining the radioactive material
Safety functions
SF(1) to prevent unacceptable reactivity transients
SF(2) to maintain reactor in a safe shutdown condition
SF(3) to shut down reactor as necessary
SF(18) to maintain subcriticality of fuel outside RCS
SF(4) to maintain sufficient RCS inventory for non-LOCA accidents
SF(5) to maintain sufficient RCS inventory for all design basis events
SF(6) to remove heat from the core under LOCA conditions
SF(7) to remove heat from the core under non-LOCA conditions
SF(8) to transfer heat from safety systems to ultimate heat sink
SF(17) to remove decay heat from fuel outside the RCS
SF(10) to maintain acceptable cladding integrity in the core
SF(11) to maintain RCS Integrity
SF(12) to limit rad-releases from the containment under accident conditions
SF(13) to limit rad-releases from sources outside the containment
SF(14) to limit rad-discharges during operational states
SF(16) to maintain control of rad-releases from the fuel outside the RCS
SF(20) to maintain integrity of the containment
SF(21) to limit effects of rad-releases on the public and environment
SF(9) to ensure necessary services as support for safety systems
SF(15) to maintain control of environmental conditions within the plant
SF(19) to prevent failure of a system with potential impairment of an SF

General approach to safety of NPPs – objective tree



Selected definitions

- ***Safety Principles:*** Commonly shared safety concepts stating how to achieve safety objectives at different levels of defence in depth (INSAG definition)
- ***Mechanisms:*** Elementary physical processes or situations whose consequences might create challenges to the performance of safety functions
- ***Challenges:*** Generic processes or circumstances (conditions) that may impact the intended performance of safety functions; a set of mechanisms having consequences which are similar in nature
- ***Provisions:*** Inherent plant characteristics, safety margins, system design features and operational measures contributing to the performance of the safety functions; aimed at prevention of the mechanisms to occur
- ***Objective Tree:*** Graphical presentation, for each of the five levels of defence, of the following elements, from top to bottom: 1) the objective of the level, 2) the relevant safety functions, 3) the identified challenges, 4) constitutive mechanisms for each of the challenges, 5) the list of provisions preventing the mechanism to occur

Objectives and scope of the screening approach

Objective of the approach:

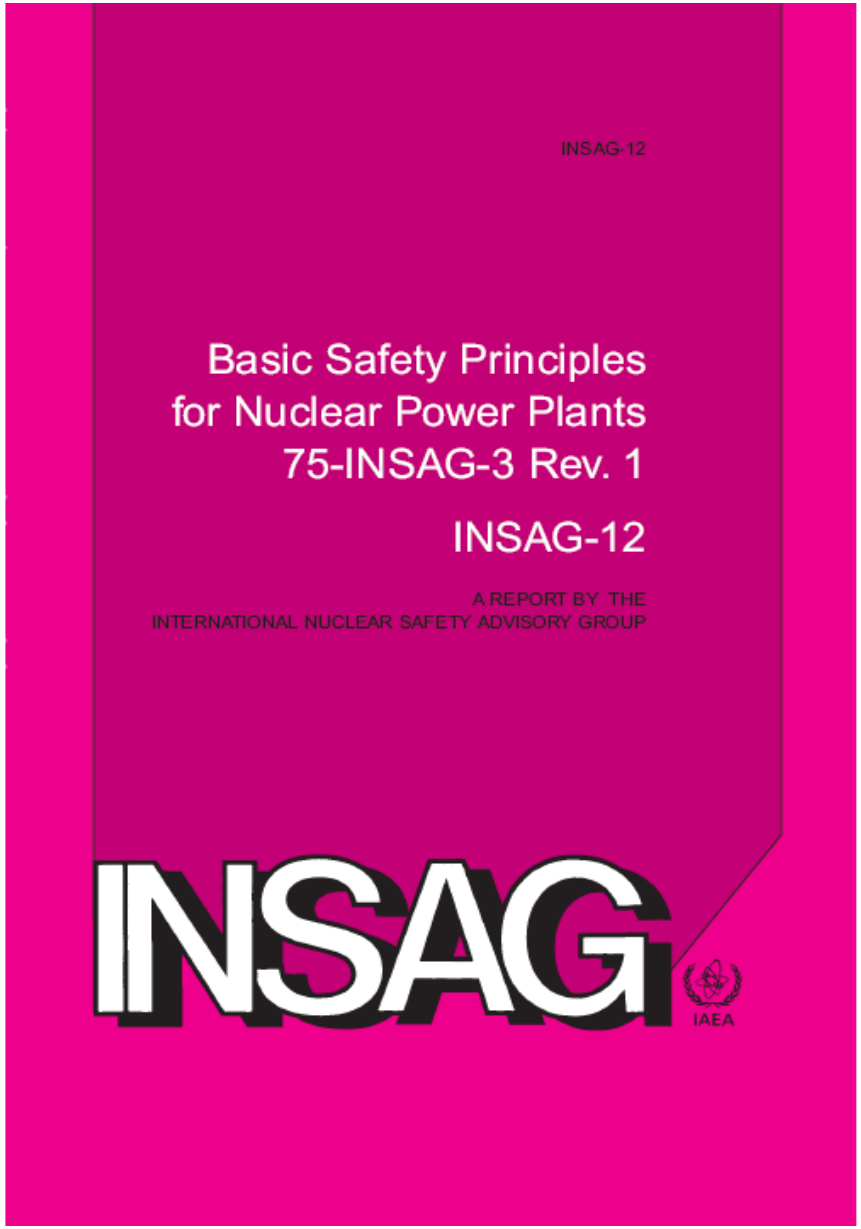
- The **reference approach for the comprehensiveness** of implementation of the concept of defence in depth
- **Overview of challenges /mechanisms/provisions** for all levels of defence
- **No evaluation of safety signif**icance of omissions nor prioritization of provisions
- Directly **applicable to existing PWRs** and their spent fuel facilities within the site
- **Main stages of the NPP lifetime covered** – siting, design, construction, operation (not decommissioning), application for specific consideration of long term operation under preparation

INSAG Basic Safety Principles

INSAG-12:

- **Safety Principles:** Commonly shared safety concepts stating how to achieve safety objectives at different levels of defence in depth (INSAG definition)
- The safety principles do not guarantee that NPPs will be absolutely free of risk, but, **when the principles are adequately implemented, the plants should be very safe**

=>Safety principles together with IAEA Safety Requirements and Guides provide basis for a systematic assessment and are good indicators for comprehensiveness of the defence in depth



Overview of INSAG-12 basic safety principles

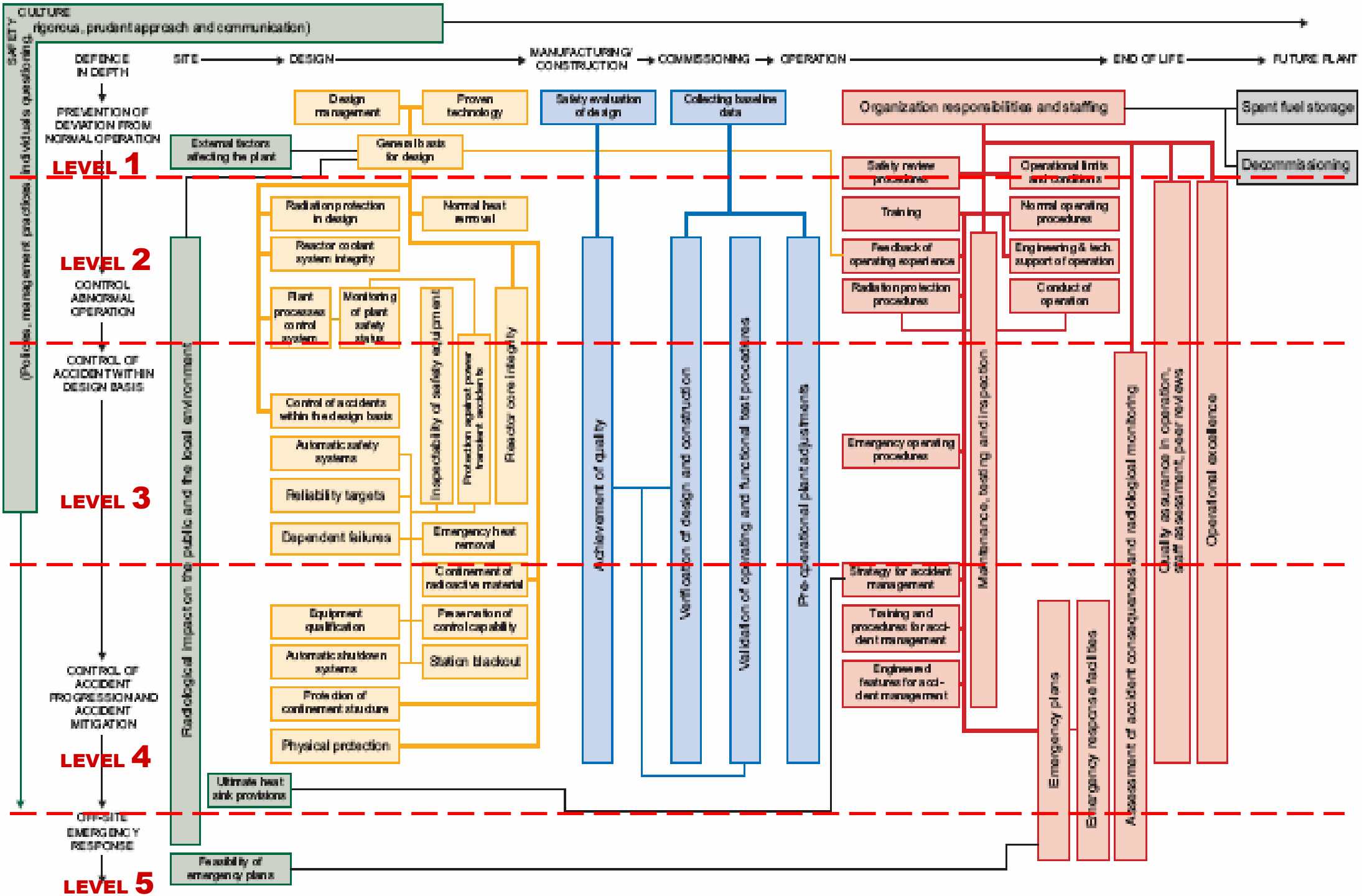
Fundamental principles (16 principles)

- **Management (3 principles)**
- **Strategy of defence in depth (3)**
- **General technical principles (10)**

Specific principles (54)

- Siting (4)
- Design (25)
- Manufacturing and construction (2)
- Commissioning (4)
- Operation (12)
- Accident management (3)
- Emergency preparedness (3)
- Decommissioning (1)

INSAG Basic Safety Principles



Plant life	SP	Safety principle	1	2	3	4	5
OPERATION	265	Organization, responsibilities and staffing	X	X	X	X	X
	269	Safety review procedures	X	X	X	X	
	272	Conduct of operation	X				
	278	Training	X	X	X		
	284	Operational limits and conditions	X	X	X		
	288	Normal operating procedures	X				
	290	Emergency operating procedures		X	X	X	
	292	Radiation protection procedures	X	X	X	X	
	296	Engineering and technical support of operations	X	X	X	X	X
	299	Feedback of operating experience	X	X	X	X	
	305	Maintenance, testing and inspection	X	X	X	X	
	312	Quality assurance in operation	X	X	X	X	
ACCIDENT MANAGE-MENT	318	Strategies for accident management				X	
	323	Training and procedures for accident management				X	
	326	Engineered features for accident management				X	
EMERGENCY PREPARED-NESS	333	Emergency plans				X	X
	336	Emergency response facilities				X	X
	339	Assessment of acc. consequences and rad. monitoring			X	X	X

Assignment of INSAG-12 safety principles to levels of defence

Assignment of safety principles to levels of defence in depth

- **Safety principles are used as ‘reminders’ to ensure completeness** of objective trees, but they are not essential for the approach and **will not appear in the complex objective trees** for each of the levels
- Formal assignment of one safety principle to several levels of defence does not necessarily mean lack of independence; the same principle typically (mainly for general safety principles, such as design management, quality assurance, safety culture) applies to different systems, different manufacturers, different NPP staff and different operating conditions
- However, **assignment of the same safety principle to several levels of defence may indicate interdependency between the levels**; special consideration and justification should be made for each such case
- **Consistency of objective trees with IAEA Safety Requirements is a ‘must’ but trees can go beyond the Requirements**

Example of challenges /mechanisms /provisions

- **Safety principle (192) Levels 1-3**: Protection against power transient accident
- **Challenge:** Insertion of reactivity with potential fuel damage
- **Mechanisms:** 1. CR withdrawal; 2. CR ejection; 3. CR malfunction; 4. Erroneous start-up of a loop; 5. Release of absorber deposits; 6. Incorrect refueling operations; 7. Inadvertent boron dilution
- **Provisions** (only for 1st mechanism):

For Level 1:
- Design margins minimizing need for automatic control
- Operational strategy with most rods out

For Level 2:
- Monitoring of control rod position
- Limited speed of control rod withdrawal
- Limited worth of control rod groups

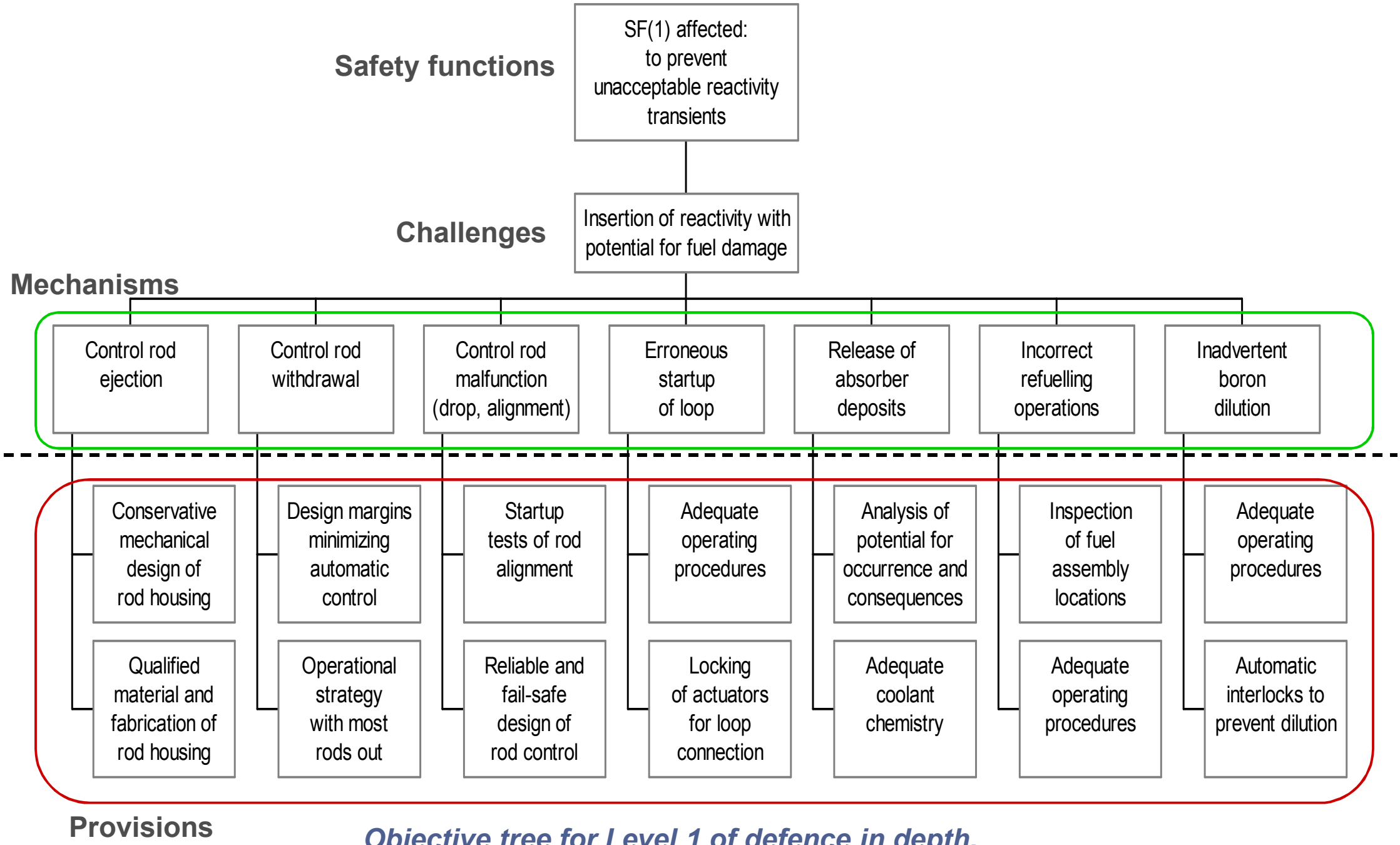
For Level 3:
- Negative reactivity feedback coefficient
- Conservative set-points of reactor protection system
- Reliable and fast shutdown system

Example of challenges /mechanisms /provisions

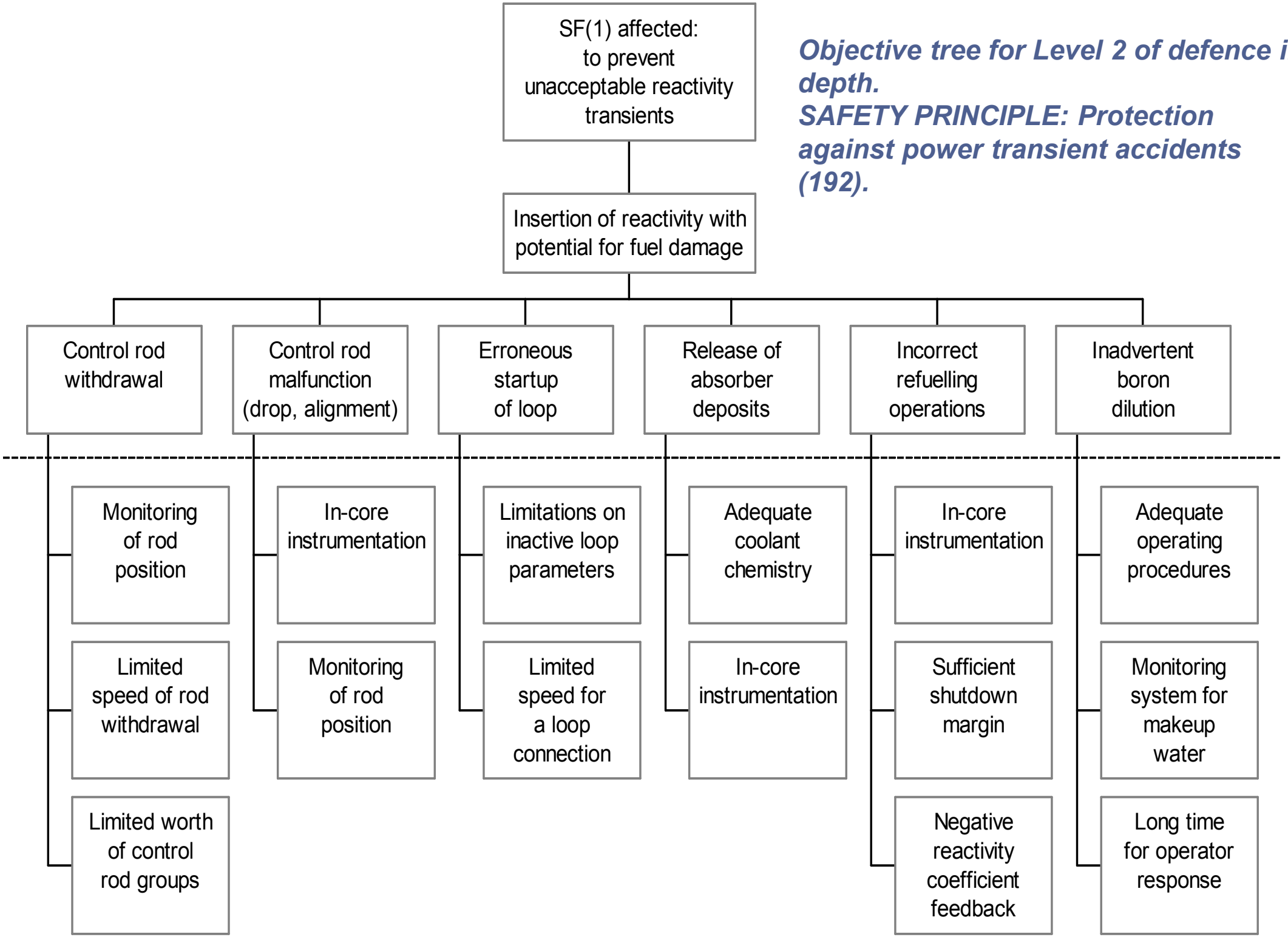
- **Safety principle (249) Levels 1-4:** Achievement of quality
- **Challenge:** Degraded functional capability of items important to safety due to limitations in the achieved quality during manufacturing or construction
- **Mechanisms:**
  1. Inadequate specification for manufacturing/construction of items important to safety
  2. Non-qualified suppliers for items important to safety
  3. Lack of compliance with specified QA requirements by manufacturers or constructors
- **Provisions (**only for 1st mechanism):
  1. Specify codes and standards containing criteria for nuclear industry
  2. Establish competent unit responsible for quality of equipment
  3. Establish safety classification of systems and components
  4. Develop detailed specification for processes and products
  5. Include contractors into QA programme of operating organization
  6. Select organization acting on behalf of operator in quality matters
  7. Arrange for manufacturing/construction staff training

Objective Trees

- **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**
- **68 different objective trees** have been developed for 53 specific safety principles assigned to the five levels of defence.
- **95 different challenges** identified (some of them applicable for several levels)
- **254 different mechanisms** identified
- **941 different provisions indicated**

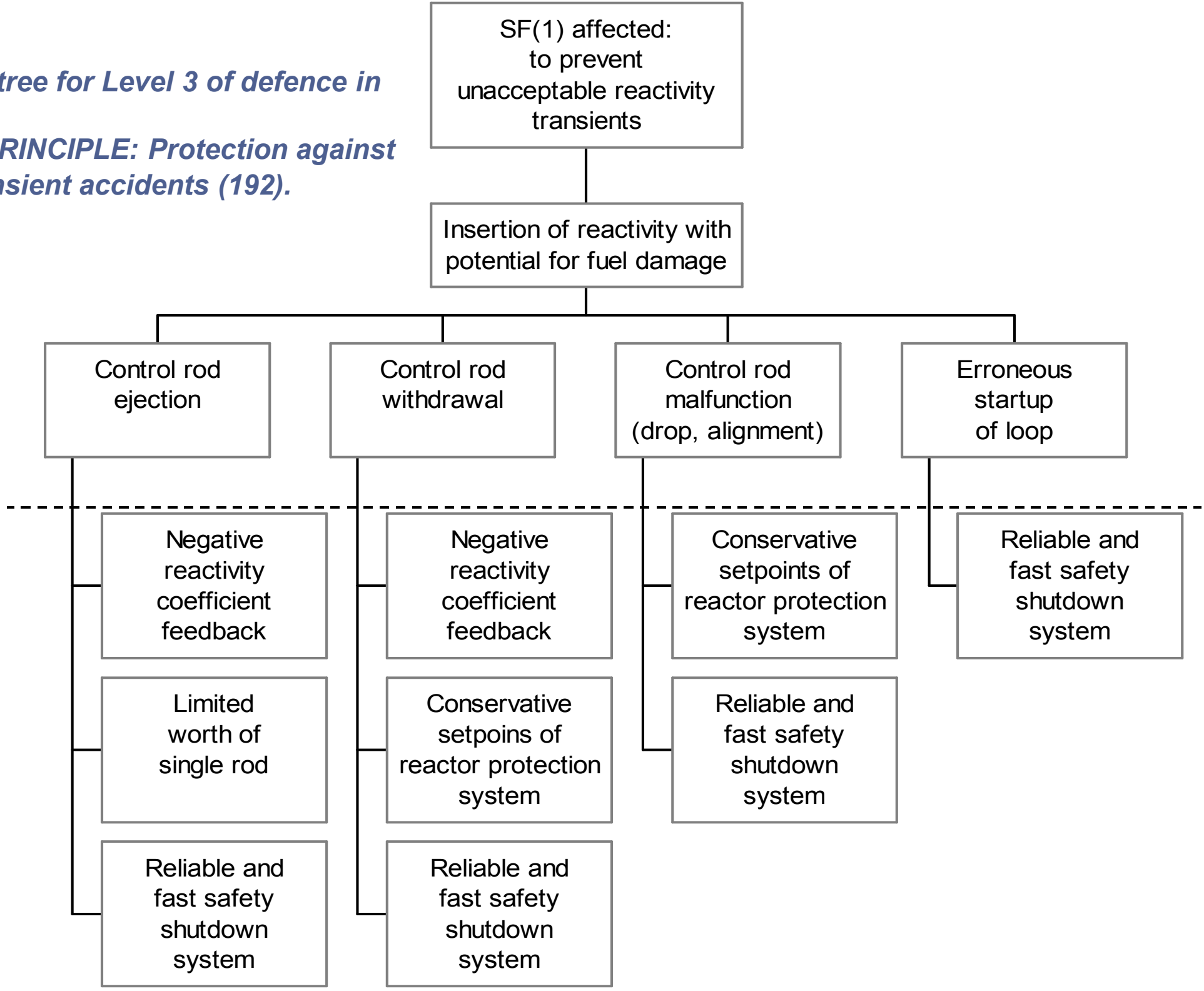


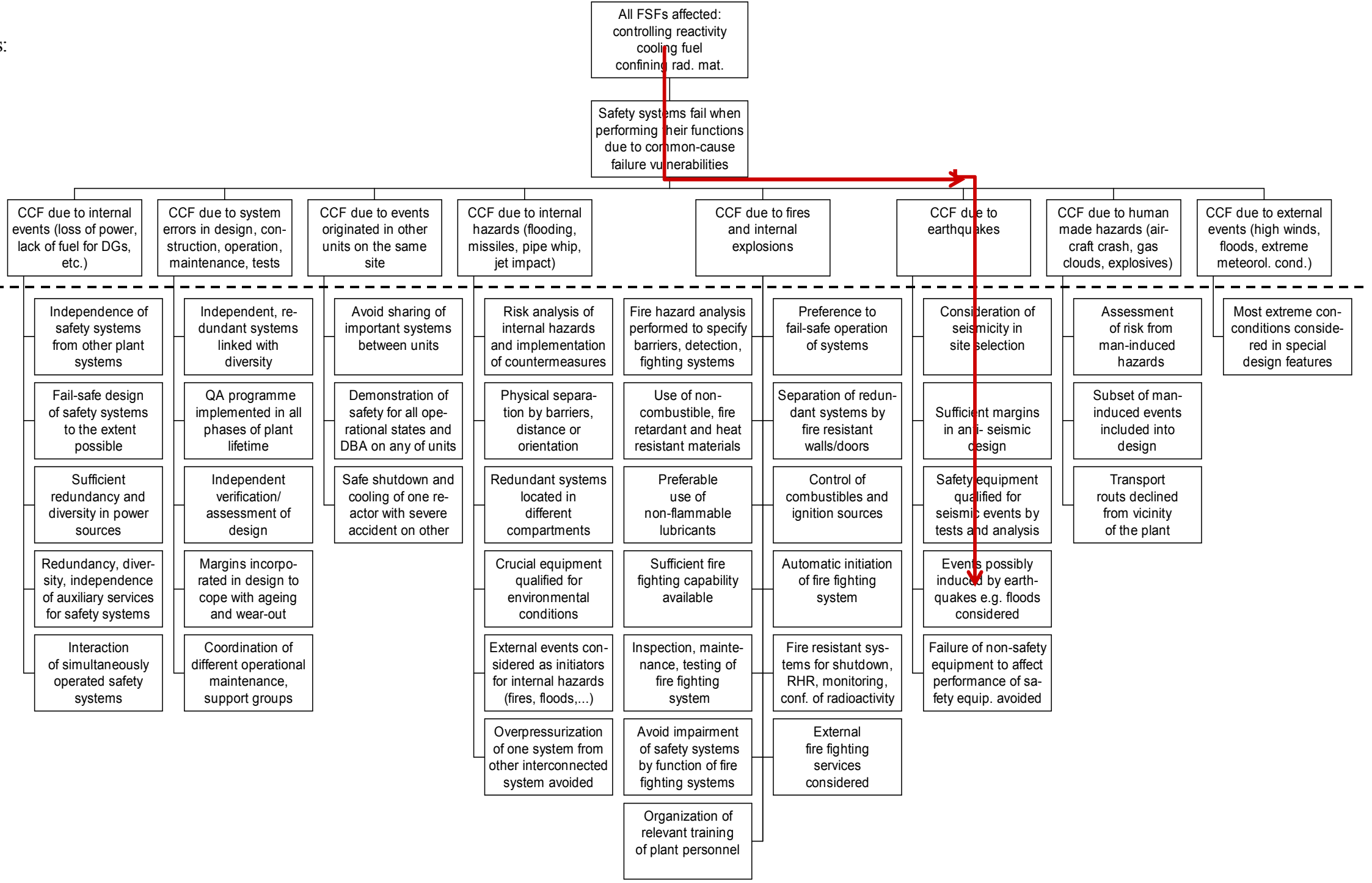
Objective tree for Level 1 of defence in depth.
SAFETY PRINCIPLE: Protection against power transient accidents (192).



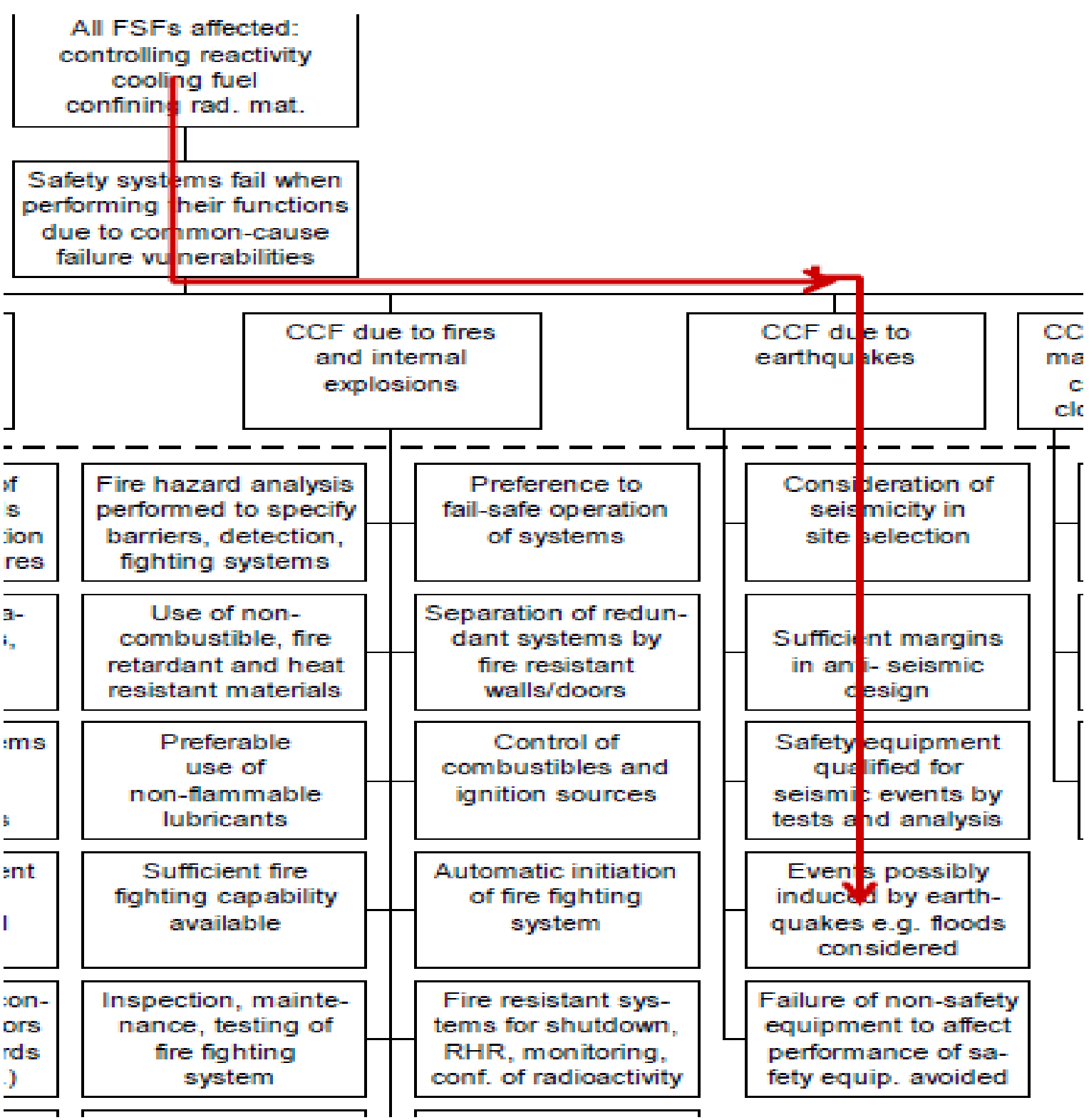
Objective tree for Level 2 of defence in depth.
SAFETY PRINCIPLE: Protection against power transient accidents (192).

Objective tree for Level 3 of defence in depth.
SAFETY PRINCIPLE: Protection against power transient accidents (192).





Objective tree for Level 3 of defence in depth
SAFETY PRINCIPLE: Dependent failures (177)


All FSFs affected: controlling reactivity cooling fuel confining rad. mat.
Safety systems fail when performing their functions due to common-cause failure vulnerabilities
CCF due to fires and internal explosions
CCF due to earthquakes
Fire hazard analysis performed to specify barriers, detection, fighting systems
Use of non-combustible, fire retardant and heat resistant materials
Preferable use of non-flammable lubricants
Sufficient fire fighting capability available
Inspection, maintenance, testing of fire fighting system
Preference to fail-safe operation of systems
Separation of redundant systems by fire resistant walls/doors
Control of combustibles and ignition sources
Automatic initiation of fire fighting system
Fire resistant systems for shutdown, RHR, monitoring, conf. of radioactivity
Consideration of seismicity in site selection
Sufficient margins in anti- seismic design
Safety equipment qualified for seismic events by tests and analysis
Events possibly induced by earthquakes e.g. floods considered
Failure of non-safety equipment to affect performance of safety equip. avoided

Use of the method

- **Bottom up screening** of individual provisions
- **Comparison of provisions** in the objective trees **with capabilities** of the plant
- **Judgment of the level of implementation of each provision** in design and operation
- **Consideration of optional provisions and judgment** whether an absence of a provision leads to the weakness in defence in depth
- **Judgment whether a mechanism can be considered as prevented** to occur
- **Judgment whether a challenge can be considered as prevented** to affect fulfillment of a safety function

Limitations of the method

- The method **does not give preference (prioritization) to individual provisions** nor specifies the way to implement or quantify the efficiency of a provision
- The **adequacy of provisions has to be determined by the user**
- Introduction of new equipment and programmes to implement an additional provision for DiD can also introduce additional complexity to the operation and additional potential failure modes
- The approach **does not include any quantification** of the extent of DiD

Selected issues associated with strengthening of defence in depth

Significantly new provisions in IAEA SSR-2/1 Strengthening of defence in depth

- All plant states shall be **either considered in the design, or practically eliminated**
- **Independence between design provisions at different levels** of defence shall be maintained to the extent possible
- **Multiple failures** shall be considered in the design
- Design extension conditions/**severe accidents are part of the design basis**
- **Dedicated measures** shall be implemented to mitigate **design extension conditions including severe accidents**

Open issues associated with strengthening of defence in depth

- Demonstration of **practical elimination** is not sufficiently defined/harmonized
- **How to address (functional) independence of different levels** of defence in safety analysis is not sufficiently defined
- **Multiple failures** cover too many combinations and need to be postulated
- How to demonstrate **adequacy of dedicated measures separately for each level of defence** is not explicitly defined

Practical elimination of certain accident sequences

Requirement on practical elimination in Safety Requirements on design (SSR-2/1)

- "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 (SF-1 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."

- "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 level of confidence to be extremely unlikely to arise**."

The issue of practical elimination (IAEA Consultancy 21-23 March 2011, ETSON WG 11)

- **The "practical elimination"** of accident situations which could lead to large early releases **is a matter of judgment** and each type of sequence must be assessed separately, taking into account the uncertainties due to the limited knowledge of some physical phenomena.
- Although probabilistic targets can be set, **"practical elimination" cannot alone be demonstrated by the compliance with a general "cut-off" probabilistic value.**
- In addition to low probability, availability of multiple additional measures with sufficient time for their implementation, based on diverse symptoms, etc ??? should be available
- ***Definition proposed:***
- ***The possibility of conditions occurring that could result in high radiation doses or 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. Rigorous deterministic considerations should be applied to achieve a probabilistic target of lower than 1x 10^{-7} per reactor year for the practical elimination of each of the conditions identified.***

The issue of practical elimination
(IRSN, France)

- Fast reactivity accidents
- Accident sequences involving containment bypassing (via the steam generators or via circuits connected to the primary system which exit the containment)
- Fuel melting in the spent fuel pool
- Selected single initiating events (vessel or large component rupture)
- High pressure core melt situations
- Global hydrogen detonations and steam explosion threatening the containment integrity
- Core melt sequences with consequential steam generator tube failures

The issue of practical elimination
(IAEA Consultancy, 21-23 March 2011, ETSON WG 11)

- The considerations for practical elimination should include:
  - Severe accident conditions that could lead to **early damage of the containment** as a result of direct containment heating, steam explosion or hydrogen detonation or **in a late phase** as a result of basemat melt-through or containment overpressurization;
  - Severe accident conditions with an **open containment** in shutdown states;
  - Severe accident conditions with **containment bypass**, such as conditions relating to the rupture of a steam generator tube or an interfacing system LOCA.
- The **practical elimination remains an issue** to be better determined for NPP safety
- **Collection of practical examples what can be accepted as practical elimination can help**

Independence between different levels of defence

Independence of the different levels of defense (IAEA Consultancy, 21-23 March 2011, ETSON WG 11)

- Objective of independence is to ensure that the **failure of one level should not cause the failure of the subsequent levels**
- This is achieved by **incorporating design features such as redundancy and diversity, physical separation, functional isolation where there is a need to overcome CCF**
- The effective independence should demonstrate that the first line of defence expected to respond is not jeopardized by the initiating event, and in case of its non response at least one additional and independent function should exist
- Independence should apply both to systems and I&C systems.
- **Discussion is ongoing how strict should be the rule of independence, since there are examples when too strong separation is not necessarily in favour to safety**
- For safety analysis there is an issue, **how to demonstrate adequacy of each level and independence between the levels**

But… specific considerations/ limits (examples by IRSN, France)

1. **Emergency AC power supply**: Additional diverse emergency AC power shall be designed for level 3b and may be used in level 4, or there can be less demanding power source for Level 4
2. **Separation of cable** already exists in redundant systems and between safety and non safety systems: it may be not reasonably practicable to introduce systematically additional separation
3. **Reactor protection system** should be independent from other I&C systems. However scram may be also level 3 and 2, Diverse I&C shall be designed for DiD level 3b to face common cause failure of the RPS,
4. **Containment** need for containment on each level of DiD for confinement safety function. It would not be reasonably practicable to require independence for different level of DiD
5. **Reactor pressure vessel** may be used to accomplish several safety function on several DiD levels. It would not be reasonably practicable to require independence for different level of DiD

Use of diversity between levels of defence
(IAEA Consultancy, 21-23 March 2011, ETSON WG 11)

- CCF are the faults which may cause the **coincidental failure of several or all channels** of a single function when is triggered by a specific event
- The demonstration that any design is proven to be **error free may always be disputed**
- Analysis **proving that vulnerabilities of the plant design to CCF have been adequately addressed is expected**
- **For low vulnerability to CCF diversity is a necessary** and supplementary design feature to redundancy and independence aiming at limiting the influence of CCF to one system only

Use of diversity between levels of defence
(IAEA Consultancy, 21-23 March 2011, ETSON WG 11)

- **CCF should be postulated** with the goal to prevent the core melt or to mitigate the radiological consequences to an acceptable **level in case of a non response of the DiD level 3 functions**
- Level 4 of DiD is required to mitigate the consequences of Design Extension Conditions which most of them could only exist if CCF making inoperable the level 3 occurred.
- **Diversity of provisions at the Level 4 is important to ensure that the safety function is unlikely to be subject to the same common cause failure which led to failure of Level 3**
- **Consequently if all functions designed to overcome CCF are implemented in the DiD level 4, reinforcing Did Level 3 by introducing diversity among its redundancies should not be necessary**

Consideration of multiple failures as a new category of NPP states

Defense-in-Depth (Revised structure proposed by WENRA Reactor Harmonization Working Group)

	Level of defence in depth	Objective of the level	Essential means	Associated plant condition categories	Radiological consequences
Original design of the plant	Level 1	Prevention of abnormal operation and failure	Conservative design and high quality in construction and operation	Normal operation	Regulatory operating limits for discharge
	Level 2	Control of abnormal operation and failure	Control, limiting and protection systems and other surveillance features	Anticipated operational occurrences	Regulatory operating limits for discharge
	Level 3 (1)	Control of accident to limit radiological releases and prevent escalation to core damage conditions (2)	Safety systems Accident procedures	DiD Level 3.a Postulated single initiating events	No off-site radiological impact or only minor radiological impact (see NS-G-1.2/4.102)
		Control of accident to limit radiological releases and prevent escalation to core melt conditions (3)	Engineered safety features (4) Accident procedures	DiD Level 3.b **Selected multiples failures events** including possible failure or inefficiency of safety systems involved in DiD level 3.a	
	Level 4	**Practical elimination of situation that could lead to early or large releases of radioactive materials** **Control of accidents with core melt to limit off-site releases**	**Engineered safety features to mitigate core melt** **Management of accidents with core melt (severe accidents)**	**Postulated core melt accidents (short and long term)**	Limited protective measures in area and time
Emergency planning	Level 5	Mitigation of radiological consequences of significant releases of radioactives materials	Off-site emergency response Intervention levels	-	Off site radiological impact necessitating protective measures

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 may be included in the revised Safety Guides for Design and Safety Assessment **More attention should be paid to design extension external hazards**
- 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	

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

Demonstration of adequacy of provisions at different levels of defence

Extending scope of safety analysis

- Current scope of **safety analysis is focused on Level 3** of defence
- **Only safety systems are assumed to work correctly**, with consideration of single failure, plant control systems are assumed to fail, or work towards worsening the situation
- For Level 4, use of dedicated and non-dedicated systems is often assumed
- For **comprehensive demonstration of adequacy of defence in depth** it should be shown, that in case of transient plant control systems if working correctly are capable to prevent initiation of safety systems
- Similarly, compliance with the relevant criteria should be demonstrated by using only dedicated systems for mitigation of severe accident
- **Demonstration of adequate reliability of systems at each level of defence separately**

Conclusions

- **Defence in depth is expected to remain an essential strategy** to ensure nuclear safety for both existing and new plants
- A demonstration of defence in depth by the proposed **screening approach in a comprehensive and systematic way** may provide reassurance that safety strategy is sound and well balanced among the levels of defence
- The approach **does not include any quantification** of the extent of defence nor a prioritisation of the provisions of defence
- **Integration of probabilistic considerations** into deterministic defence in depth in the future would be helpful
- **Updating of the screening approach described in SR 46 and making it more user friendly** taking into account Fukushima and new IAEA Safety Standards would be appropriate

Conclusions

- There are several **issues associated with strengthened implementation of defence in depth**: practical elimination, independence of levels, multiple failures, scope of safety demonstration
- **Practical elimination can not be solely based on probabilistic exclusion criteria**; it should be combined with careful deterministic assessment all potential mechanisms leading to large releases
- Works on clarification of the issues of practical elimination and independence of levels are **ongoing through different channels** (EUR, WENRA, ETSON), IAEA should be also involved
- Broader international **consensus on postulation of multiple failures** in reactor designs is needed
- **Broadening of the scope of safety analysis** for licensing is needed to demonstrate adequacy/efficiency of provisions at each level of defence separately