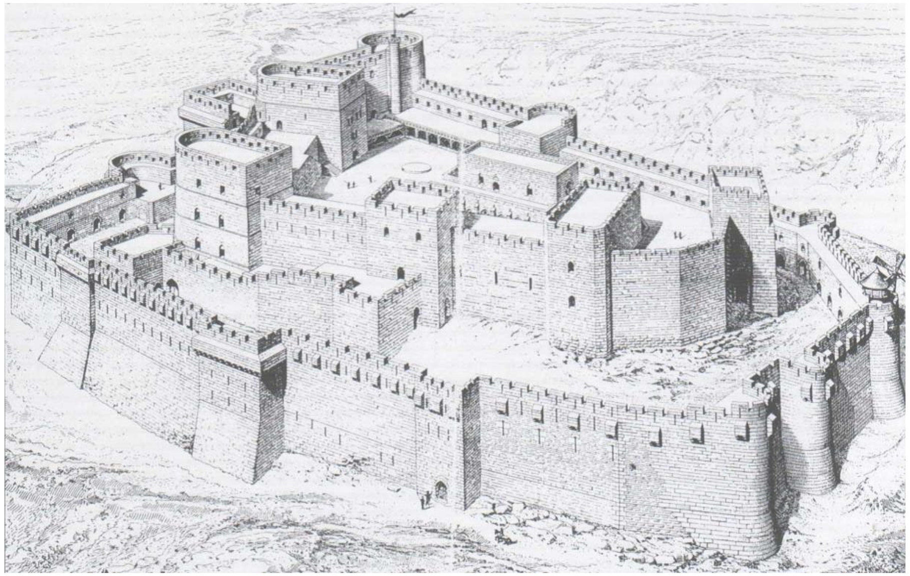
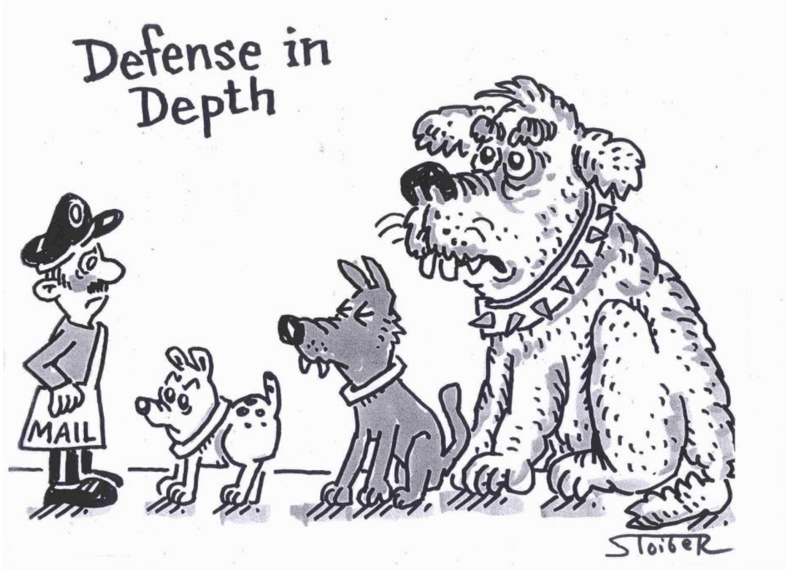
Reinforcing Defence in Depth – A Practical Systemic Approach

Jozef Misak, UJV Rez a.s., Czech Republic,
e-mail: Jozef.Misak@ujv.cz, phone number: +420 602 293 882

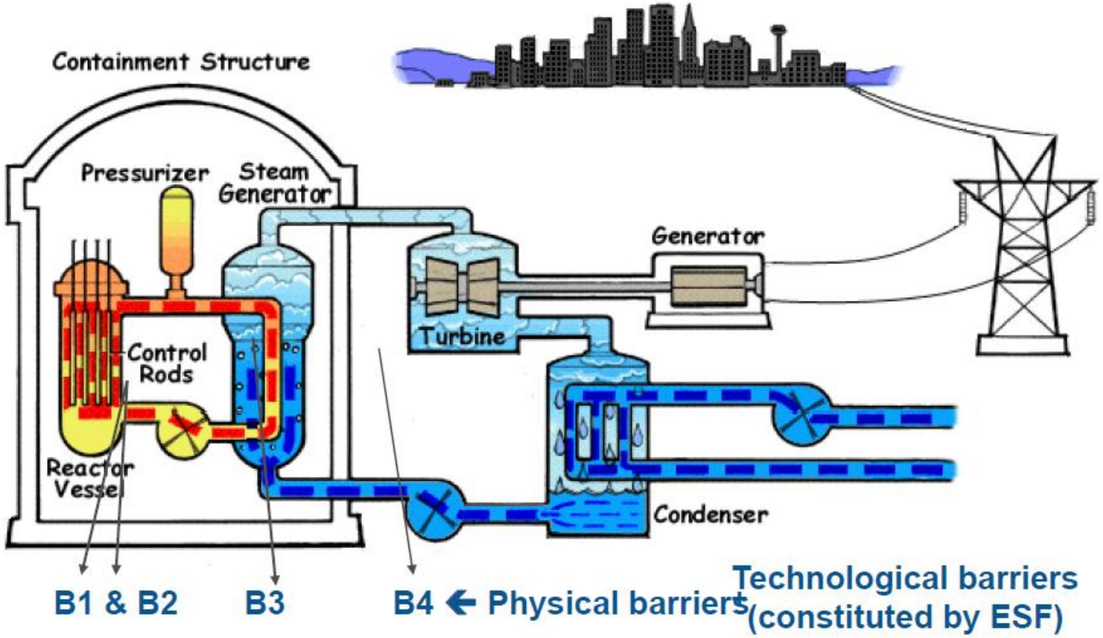
Germaine Watts, Intelligent Organizational Systems, Canada,
e-mail: germainewatts@intelorgsys.com, phone number: 1-506-333-7093

Defence in depth: Multiple physical barriers + levels of protection: A strategy to defeat a much stronger enemy

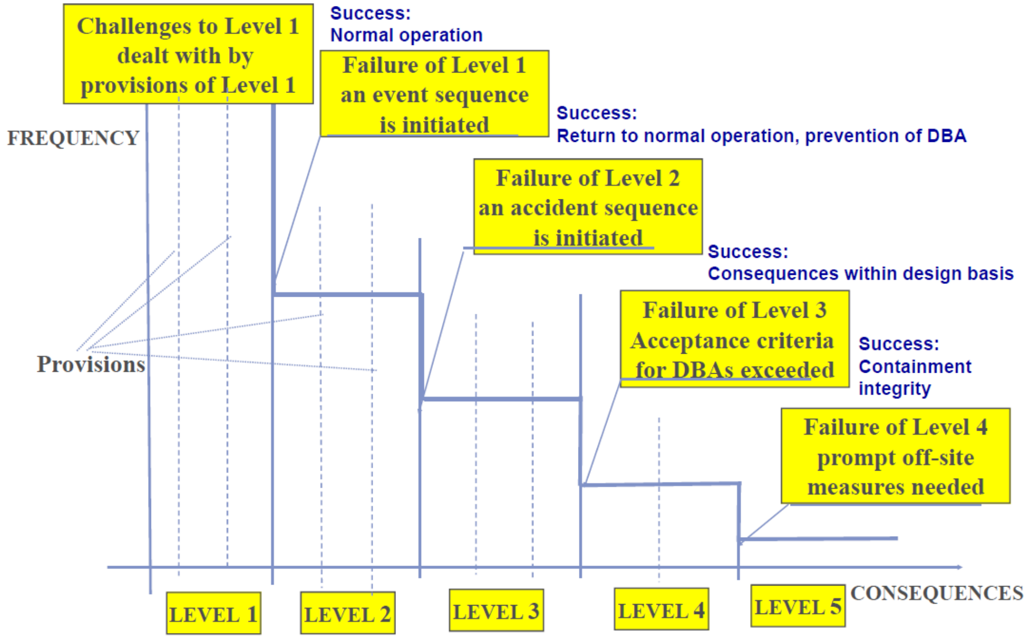




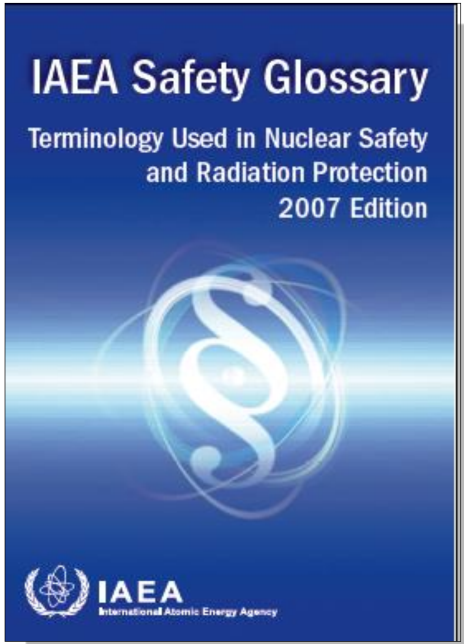
Physical obstacles to the release of radioactivity: B1, B2, B3, B4 & ESF

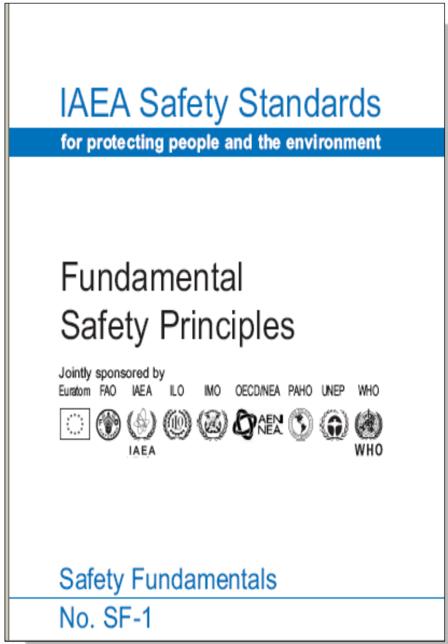


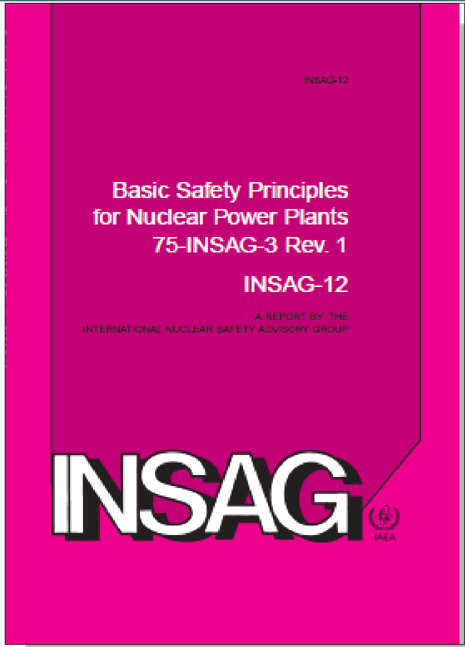
Correlation of levels of defence and success criteria

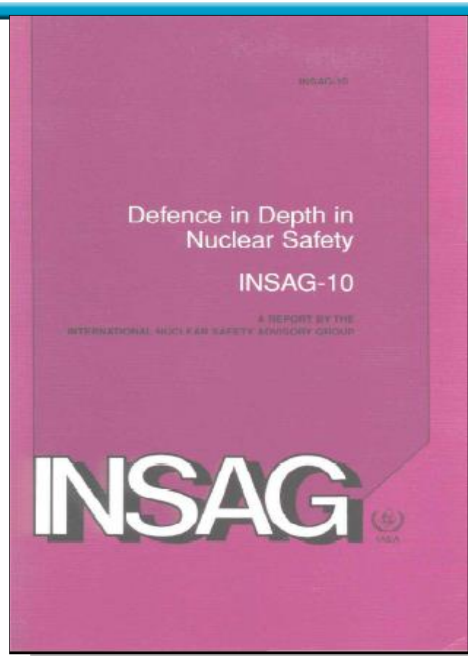


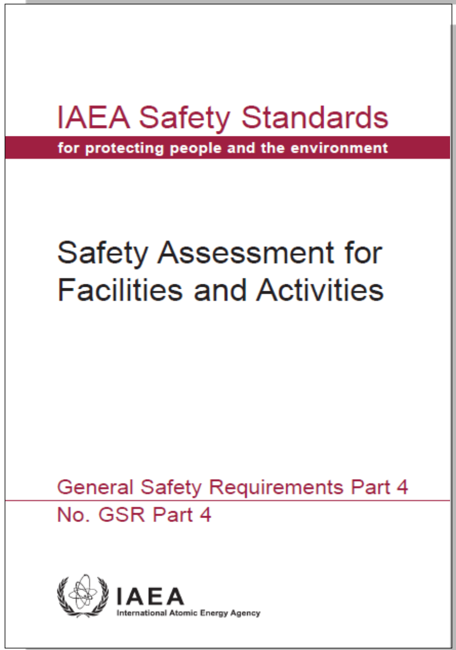
Defence in depth addressed in a number of background IAEA documents

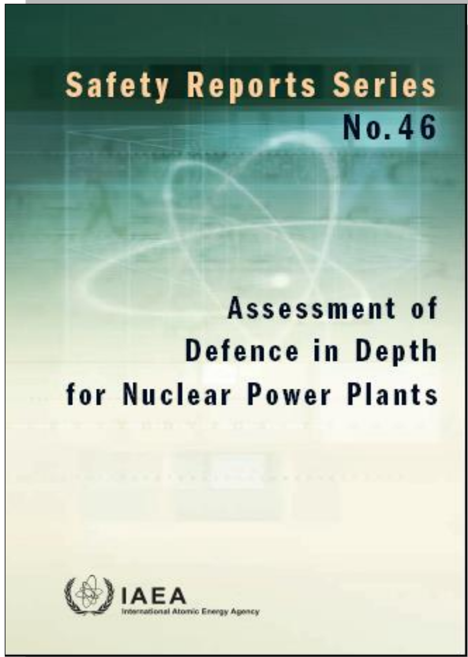


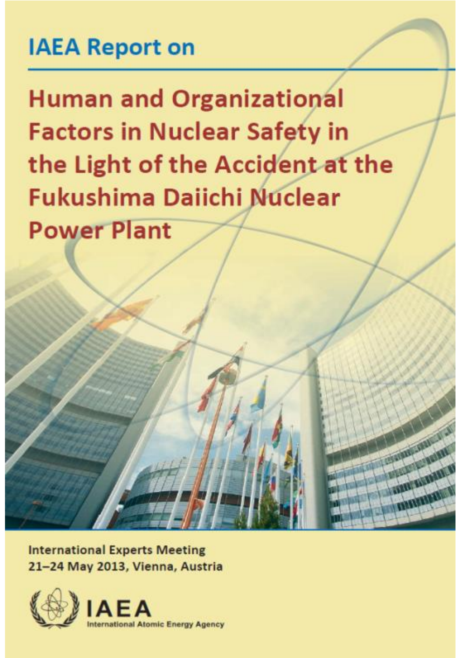












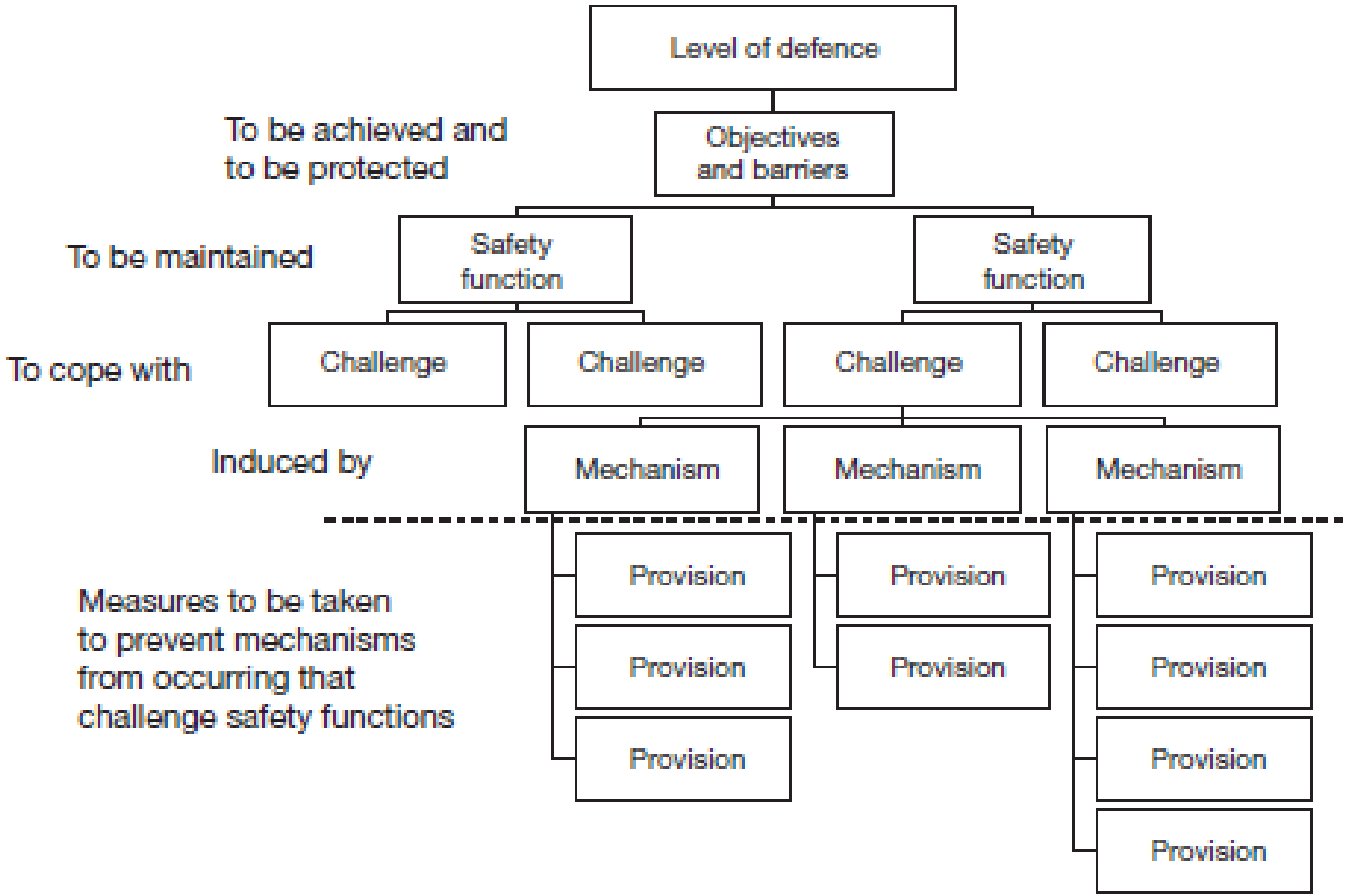
Method of objective trees: Screening of comprehensiveness of defence in depth

- **Possible interpretation of the term “defence in depth” is too broad:** all NPPs have physical barriers and means to protect the barriers, while their level of defence can be very different
- **A practical tool for detailed assessment of the comprehensiveness of the provisions for ensuring defence in depth was needed**
- A screening method using so called **“objective trees”** has been developed by the IAEA several years ago to respond to the need
- The reference approach for checking the completeness and quality of implementation of the concept of defence in depth, which includes a comprehensive overview of challenges /mechanisms/provisions for all levels of defence
- **Graphical form of objective trees helps to understand the links between safety provisions and challenges to safety objectives at different levels of defence**
- At the same time the objective trees also illustrate that **the means for protection of the physical barriers against releases of radioactive substances include much more than just NPP technological systems and procedures**

Description of the objective trees (next figure)

- Safety must be ensured by provisions at **all 5 levels at the same time**
- **Each level has its relevant safety objectives** ensured by maintaining integrity of the barriers
- For maintaining integrity of the barriers, the **fundamental (and derived) safety functions should be performed**
- Performance of **safety functions can be affected by a number of mechanisms**; **combination of similar mechanisms represents a challenge** to safety functions
- To prevent mechanisms and challenges affecting the safety functions**, safety provisions of different kinds** should be implemented
- **Links between different components of defence in depth can be graphically depicted in objective trees**

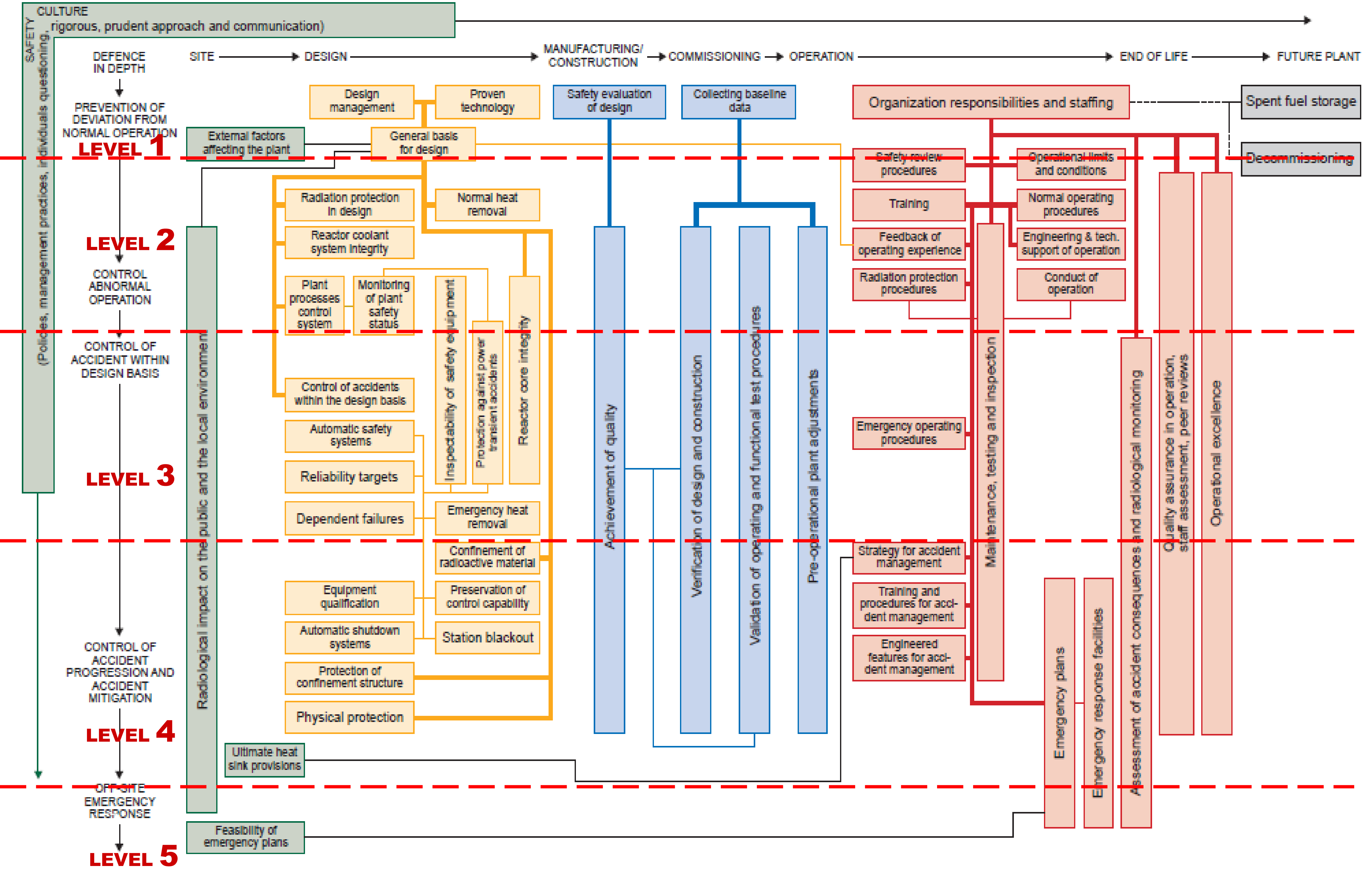
General structure of the objective tree at each level of defence (IAEA SR No. 46)



Comprehensiveness of safety provisions (measures) to ensure effectiveness of barriers

- **Variety of safety provisions: organizational, behavioural and design measures, namely**
  - inherent safety characteristics
  - safety margins
  - active and passive systems
  - operating procedures and operator actions
  - human factors and other organizational measures
  - safety culture aspects
- Although plant systems are very important, they are not the only important component of defence in depth
- **How to ensure that a set of provisions is comprehensive enough?** – Basic Safety Principles
- Safety principles form a fundamental set of rules how to achieve nuclear safety objectives and ensure comprehensiveness of provisions

INSAG Basic Safety Principles



Examples 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. Control rod (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:

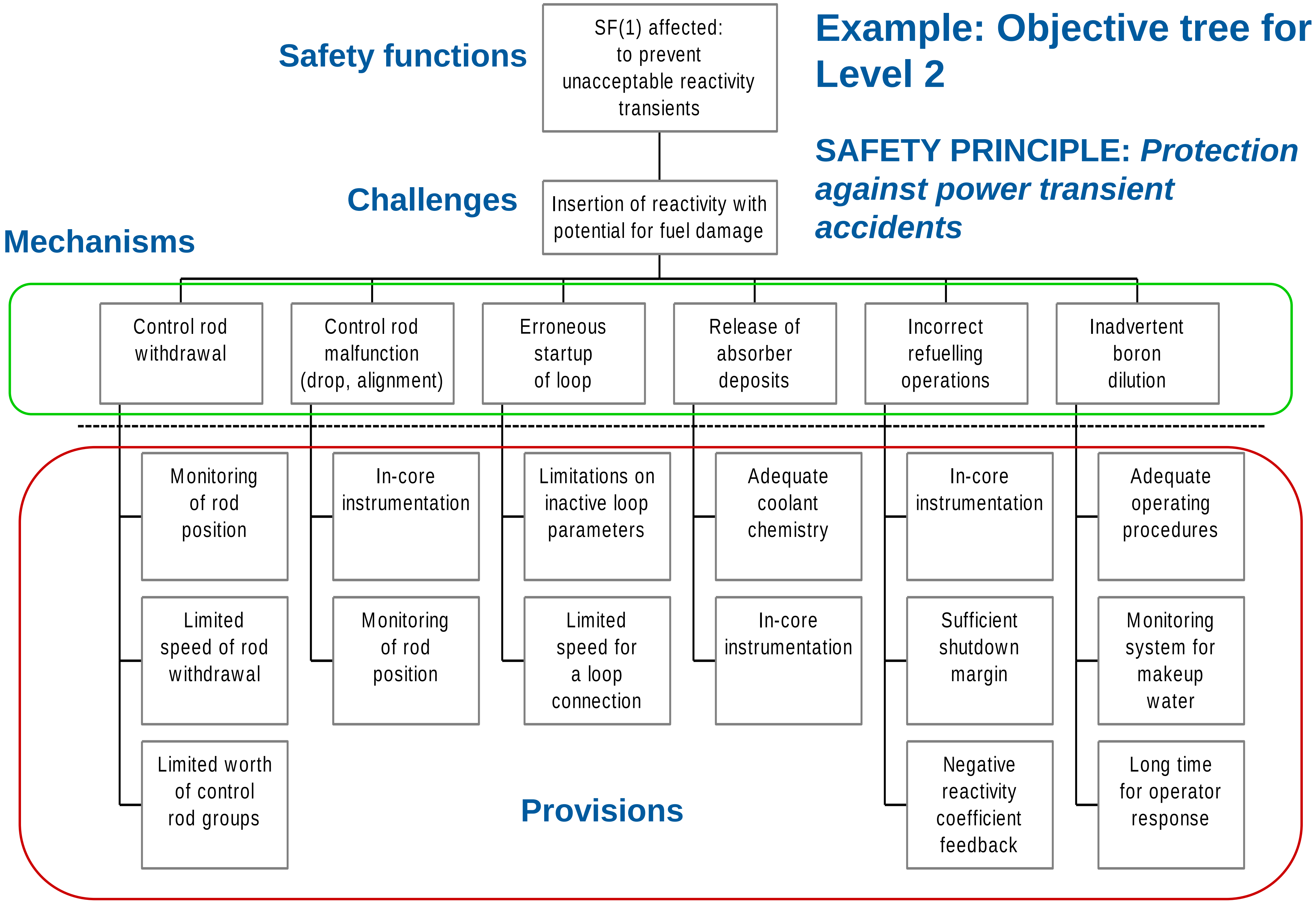
- Design margins minimizing need for automatic control
- Operational strategy with most rods out

For Level 2:

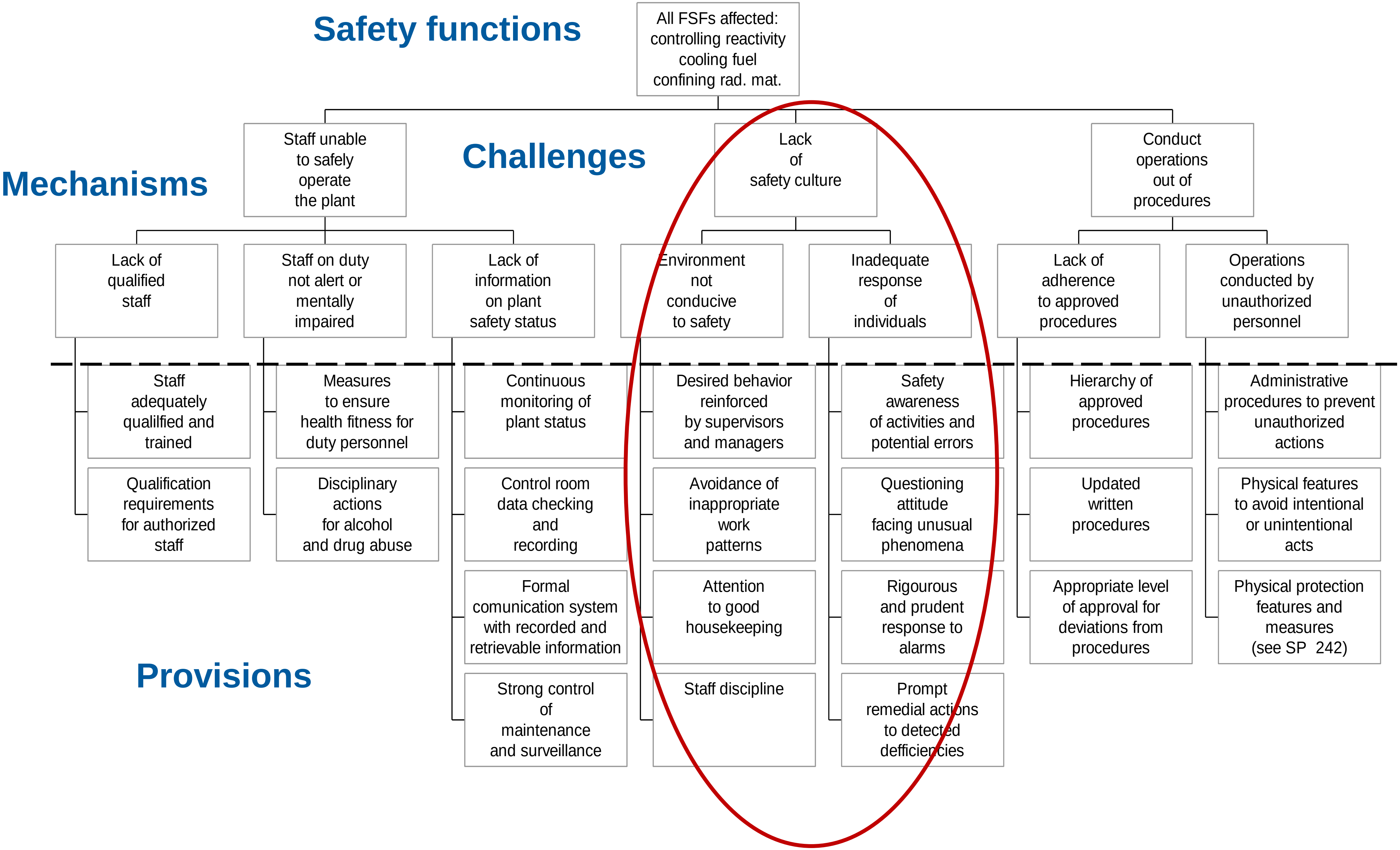
- Monitoring of control rod position
- Limited speed of control rod withdrawal
- Limited worth of control rod groups

For Level 3:

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


Example: Objective tree for Level 2
SAFETY PRINCIPLE: Protection against power transient accidents
Safety functions
SF(1) affected: to prevent unacceptable reactivity transients
Challenges
Insertion of reactivity with potential for fuel damage
Mechanisms
Control rod withdrawal
Control rod malfunction (drop, alignment)
Erroneous startup of loop
Release of absorber deposits
Incorrect refuelling operations
Inadvertent boron dilution
Monitoring of rod position
Limited speed of rod withdrawal
Limited worth of control rod groups
In-core instrumentation
Monitoring of rod position
Limitations on inactive loop parameters
Limited speed for a loop connection
Adequate coolant chemistry
In-core instrumentation
In-core instrumentation
Sufficient shutdown margin
Negative reactivity coefficient feedback
Adequate operating procedures
Monitoring system for makeup water
Long time for operator response
Provisions

Example: Objective tree for Level 1: HOF SAFETY PRINCIPLE
Conduct of operations



Consideration of human and organizational factors in objective trees

- INSAG 12 safety principles indicated **clear role of human and organizational factors** for achieving safety objectives at all levels of defence
- **Defence in depth is often oversimplified focusing on engineering aspects (barriers and their integrity) while "soft" aspects are neglected**
- **Human and organizational issues are associated with large uncertainties, and can affect several levels of defence at the same time**
- Objective trees illustrate clear links between weaknesses in human and organizational factors and challenges to safety objectives and help to identify and eliminate them
- It is obvious that there is always a room for improvements, and comprehensive assessment of Fukushima offers broad opportunity for improvements

Ways for strengthening HOF in defence in depth (IAEA IEM on HOF, 21-24 May 2013)

- Strengthening cooperation among all stakeholders (operators, vendors, regulators, contractors, TSOs, corporate organizations, international organizations) using new communication interfaces
- Strengthening interdisciplinary expertise through involvement of the social and behavioural sciences
- Continuously improving maintenance management and establishing closer cooperation with manufacturers and contractors
- Consideration of human and organizational factors in the planning, conduct and evaluation of emergency drills and exercises
- Identification of additional training, including understanding resilience, for operating personnel
- Enhancing the dialogue between the regulators and operators on topics beyond regulations, on safety practices and policies

Ways for strengthening HOF in defence in depth (IAEA IEM on HOF, 21-24 May 2013)

- Establishing and maintaining the trust of local communities.
- Implementation of more practical ways for managers to strengthen safety culture supporting prioritization of nuclear safety (in particular, if a NPP is part of a non-nuclear utility)
- Strengthening leadership and management for safety, mainly for top-level managers
- Objectively assessing efforts to strengthen safety and widely informing staff about safety initiatives
- Demonstrating high priority to safety culture by proactively introducing actions and ensuring resources for safety upgrading
- Recognizing the efforts of personnel to protect and ensure the safety of the public, the workers and the plant
- Implementing improvements with regard to decision making and consideration of the use of tools to support decision making in emergency response

Reinforcing Defence in Depth – A Practical Systemic Approach

IAEA IEM on HOF (21-24 May 2013) - *importance of adopting a systemic approach to safety that considers the interaction between individual, technical and organizational factors*.

- investigate the non-linear interactions between the hard and 'soft' logic trees, and to look beyond traditional organizational boundaries

WHY?

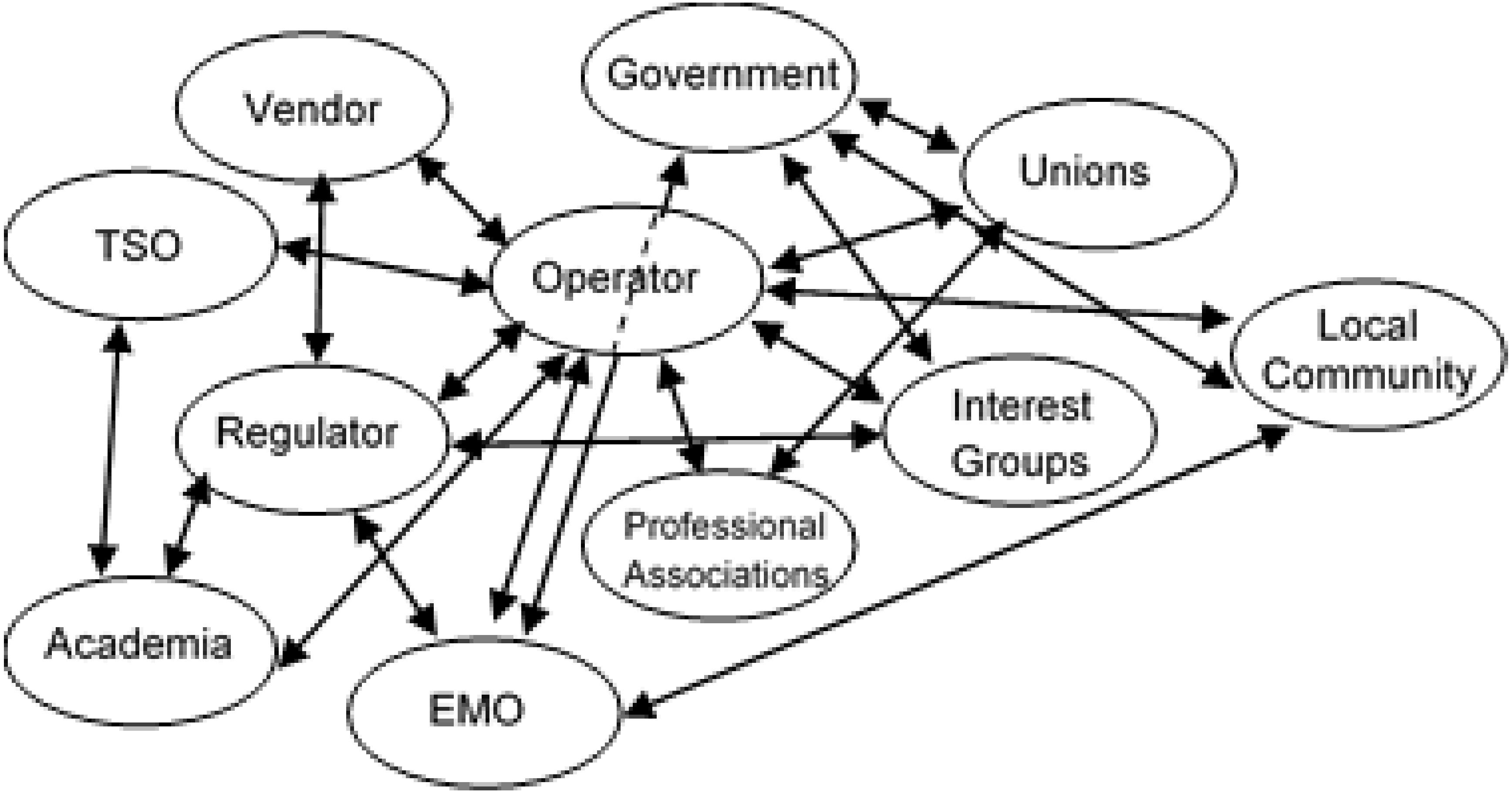
- '**Complicated' systems** – the relationship between cause and effect requires analysis or some other form of investigation and/or the application of expert knowledge (sense-analyse-respond)
  - expert and rational leaders, top-down planning, smooth implementation of policies, and a clock-like organization can ensure flawless operation
- '**Complex' systems** – the relationship between cause and effect can only be fully perceived in retrospect (probe-sense-respond)
  - filled with hundreds of moving parts, potentially thousands of actors with varied expertise and independence, and no central point that orchestrates all these different parts within an ever-changing context

Complex Systems

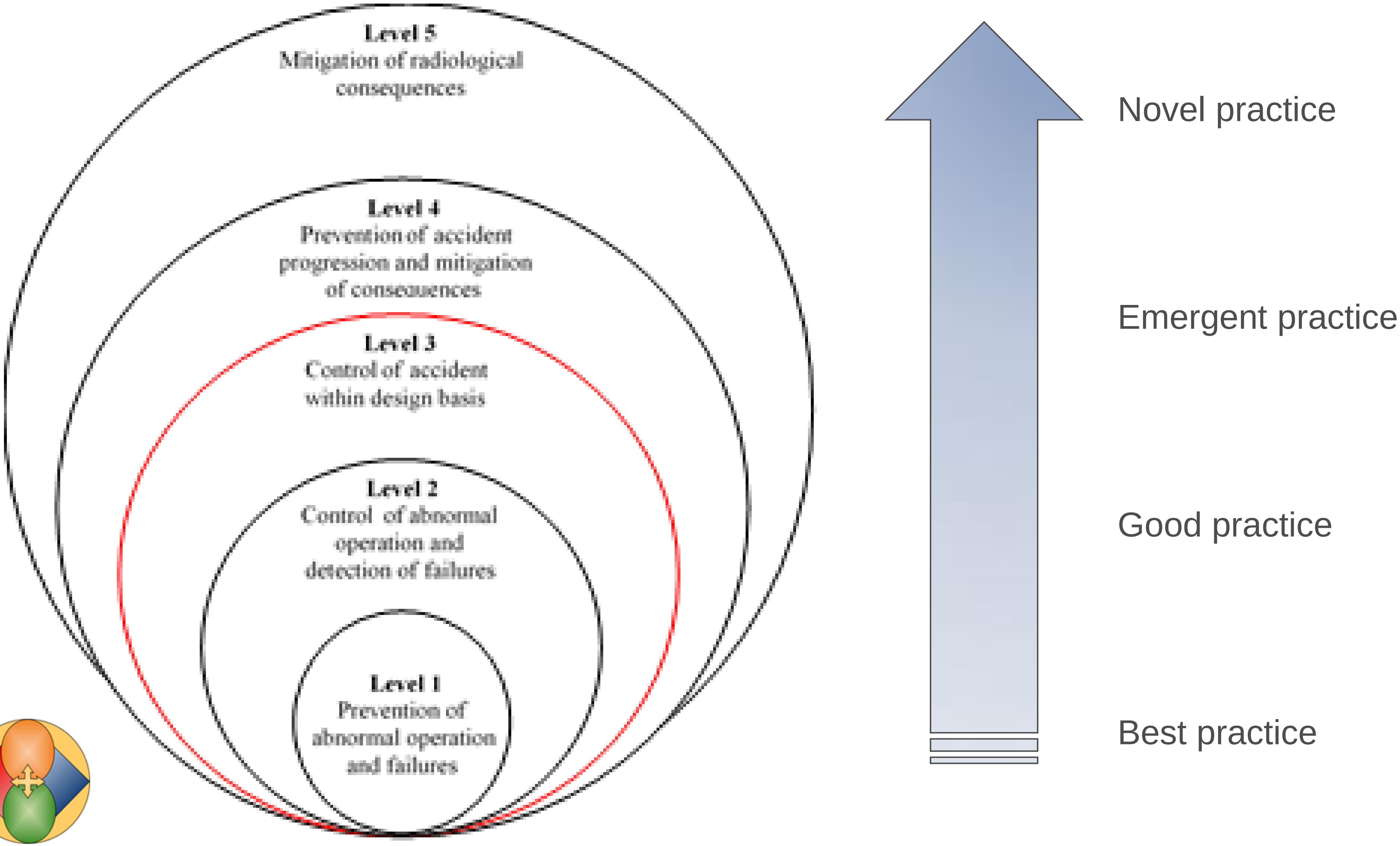
- **Reality:** Behaviour is contextualized: continuously adapt in and evolve with a changing environment; conflict and unplanned changes occur all the time, perceptions and projections have impact
- **Result:** Very high degrees of uncertainty that represent a different risk-management challenge than in technical systems; emergent, fractal property; normal tools for predictability are insufficient
- **Requirement:** Use a screening process that looks at how the entire ‘complex’ system is adapting to changes, dealing with conflicts, and learning as a whole (next slide)
  - Maintain and strengthen *‘virtuous’* cycles to support the ultimate goal of safety conscious decisions and actions,
  - Intervene in *‘vicious*’ cycles that undermine the information flows, cooperation, and conservative decision-making

Systemic Perspective

- A systemic perspective enhances application of the defence in depth concept by screening interactions multi-directionally, and across many organizational boundaries



Example: DiD Resilience - Changing HOF Reality



IAEA Systemic Training Workshop

Purpose

- deepen understanding of human and organizational factors
- demonstrate application of the systemic mapping methodology to real life scenarios
- provide opportunity for participants to explore safety challenges in their own organizations with multi-disciplinary team of facilitators

Target Audience

- middle managers in operating, regulatory and technical support organizations, including non-technical leaders such as performance improvement, training, and leadership or organization development managers

Timing

- March 29 – April 1, 2016

Conclusions

- Defence in depth is an essential strategy to ensure nuclear safety for both existing and new NPPs
- The use of objective trees for screening the comprehensiveness of defence in depth provides a powerful tool for understanding links between technological and organizational provisions for ensuring safety of NPPs
- Defence in depth should not be oversimplified by reducing it to the capacity of barriers to protect against releases of radioactive substances.
- The large uncertainties associated with predicting human behaviour, alongside their sensitivity to organizational factors and societal influences, requires special attention to be given to ‘soft’ logic trees within the defence in depth framework and screening process.

Conclusions

- Defence in depth can be further strengthened by understanding nuclear power programmes as ‘complex’ systems, and by taking into account all the components of the system, from operators, through middle level managers, NPP managers, up to corporate, governmental and even international levels when assessing risk.
- Cross-correlation and mutual interdependence between all components of this complex system’s defence in depth needs to be given considerable attention in the future.
- The use of system mapping for exploring the non-linear interactions between individual, technical and organizational factors can enhance defence in depth by providing a method for screening the multiplicity of dynamics within and between organizations that drive the overall culture for safety within a national nuclear programme.