



Content

- Generation IV International Forum (GIF) – safety objectives
- GIF Risk and Safety Working Group Integrated Safety Assessment Methodology
- Objective Provision Tree (OPT) – a tool to assess the application of the Defence in Depth Principle
- Need for strengthening safety assessment tools after Fukushima?



Generation IV International Forum (GIF)

➤ International initiative since 2003 (currently 10 members) to support R&D, within a time frame from 15 to 20 years



- The 5 GIF fundamental criteria :
- ✓ Sustainability
 - ✓ Non-Proliferation and physical protection
 - ✓ Safety and reliability
 - ✓ Minimization of waste production
 - ✓ Economics

- Designed for different applications
- ✓ Electricity, Hydrogen
 - ✓ Desalinated water, Heat













The GIF
Framework
Agreement

JRC: implementing Agent
for EURATOM



ESNII

										
VHTR	◆	◆	◆	◆	◆	◆	◆	◆	◆	
GFR		◆	◆	◆			◆			
SFR		◆	◆	◆	◆			◆	◆	◆
LFR		◆		◆	◆			◆		
SCWR	◆	◆		◆					◆	
MSR		◆	◆					◆		

- GFR** – Gas-Cooled Fast Reactor (System Arrangement)
- LFR** – Lead-Cooled Fast Reactor (MOU)
- MSR** – Molten Salt Reactor (MOU)
- SFR** – Sodium-Cooled Fast Reactor (SA)
- SCWR** – Supercritical Water-Cooled Reactor (SA)
- VHTR** – Very-High-Temperature Reactor (SA)

◆ Co-chair

◆ Interest

Joint Research Centre JRC: Implementing Agent of Euratom



Aim of the EURATOM participation in GIF

- To represent all EU Member States (except France, a direct GIF member) in such a major R&D international collaboration
- Consequently, to allow all interested EU organizations to contribute to GIF R&D projects and to obtain all projects results, while respecting the GIF IPR rules
- To enhance the international dimension of R&D of new reactor systems, and of their safety design criteria: it is the aim of all GIF members to achieve highest safety standards
- Today the EURATOM contribution to GIF comes mainly from the **FP Indirect Action projects and from direct JRC contributions**; MS direct contributions are possible as well

Gen IV Goals on Safety

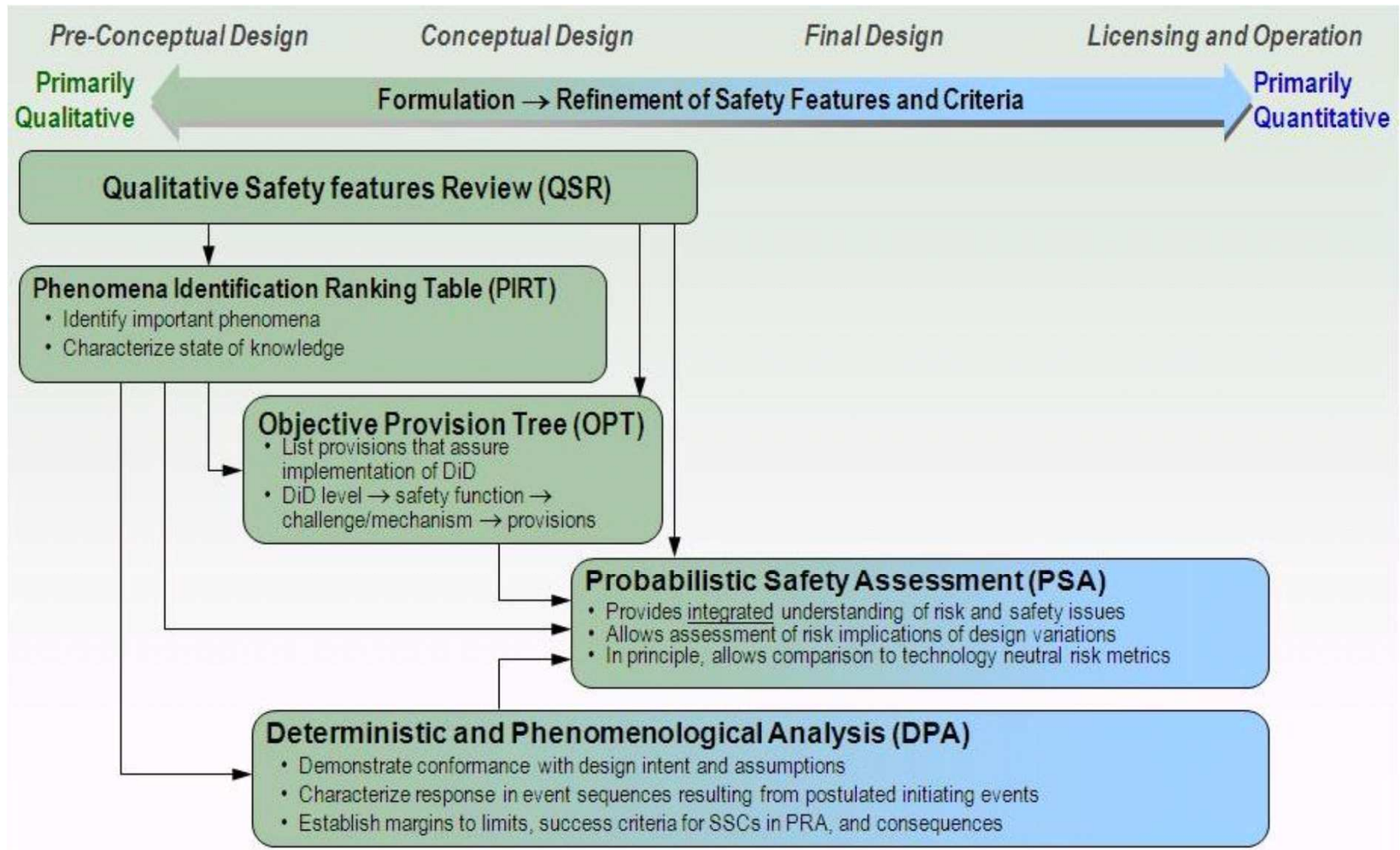


Three specific safety goals “to be used to stimulate the search for innovative nuclear energy systems and to motivate and guide the R&D on Generation IV systems”:

- *Generation IV nuclear energy systems operations will excel in safety and reliability.*
- *Generation IV nuclear energy systems will have a very low likelihood and degree of reactor core damage.*
- *Generation IV nuclear energy systems will eliminate the need for offsite emergency response.*

To help achieving this objectives the Generation IV International Forum Policy Group (GIF-PG) set up the Risk and Safety Working Group (RSWG).

GIF RSWG Integrated Safety Assessment Methodology



Defence-in-Depth



The design & assessment of the safety architecture of nuclear systems needs to integrate the features related to the **Defence-in-Depth** (DiD) principle.

The safety architecture is defined as the set of provisions to:

- Ensure completion of the tasks allocated to the process;
- Prevent, as much as feasible, initiators of accident;
- Detect and control deviations from the normal operation;
- Prevent plant degradation in case abnormal conditions (restoring safe conditions)
- Mitigate the consequences of accidental conditions with plant degradation,

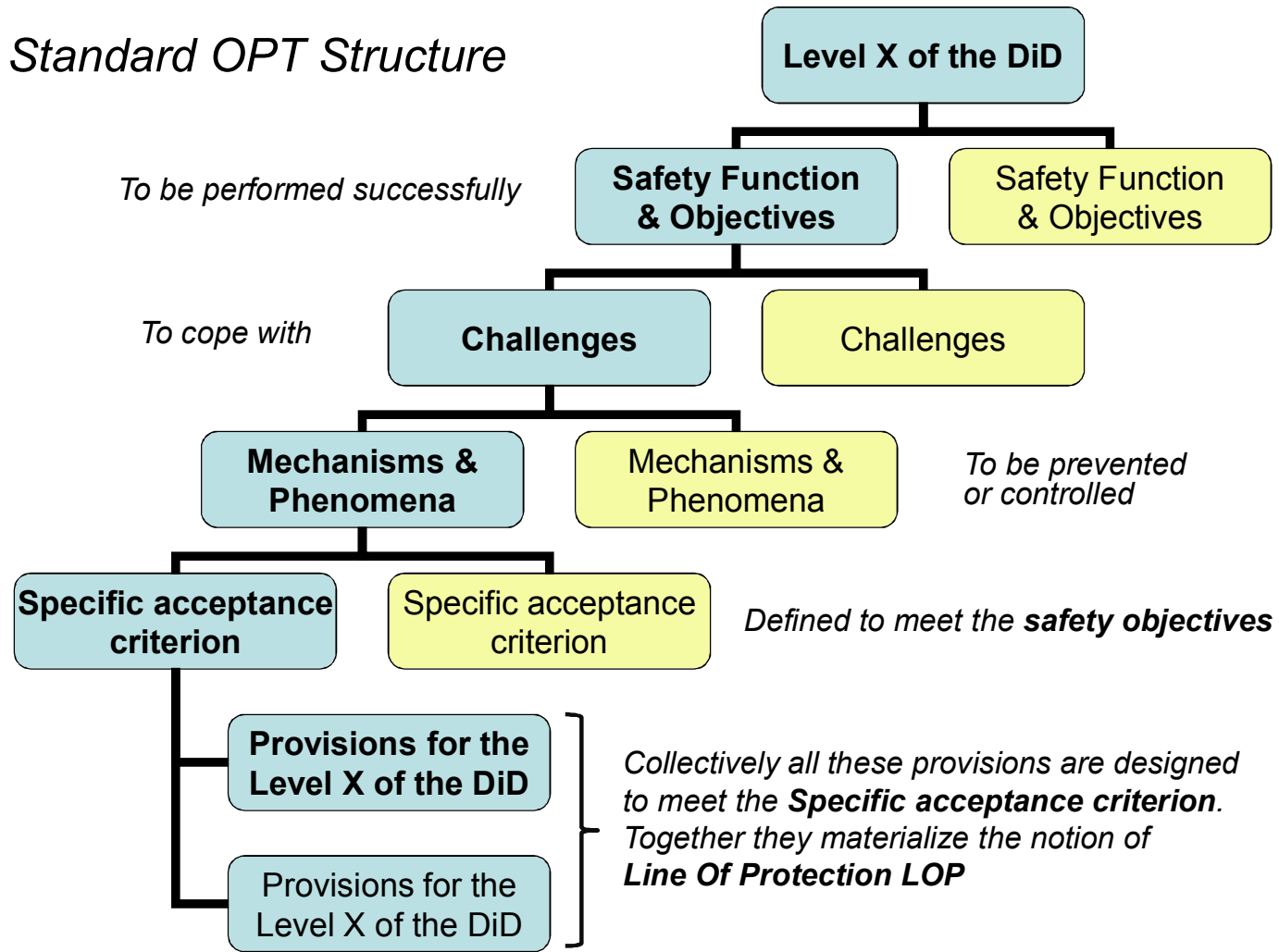
The **Objective Provision Tree** (OPT) -> a useful tool to help designers to:

1. Correctly implement the DiD, and/or
2. Assess DiD application for existing reactor systems

OPT tool for DiD assessment



Standard OPT Structure



OPT Objectives and Scope



The logic of the OPT

The OPT steps are resumed as follow:

↳ **Safety Function:** e.g. reactivity control -> to be performed successfully

↳ **Challenge:** e.g. injection of reactivity -> to cope with

↳ **Mechanism:** e.g. control rod withdrawal -> to be prevented or controlled

Once determined the acceptability criteria which allow managing the appearance of the event and/or to minimize its consequences.

↳ **Provisions:** e.g. a limiting removal device & associated I&C

References:

Considerations in the Development of Safety Requirements for Innovative Reactors: Application to Modular High Temperature Gas Cooled Reactors, IAEA TECDOC 1366, Vienna (2003).

Assessment of Defence in Depth for Nuclear Power Plants, Safety Reports Series No 46, IAEA, Vienna (2005)

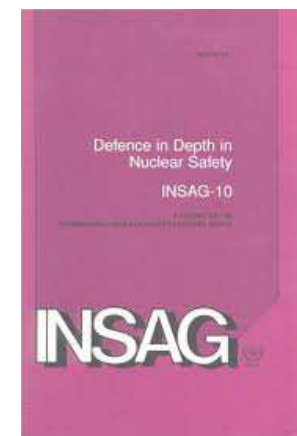
OPT Elements



Levels of the Defence in depth (DiD)

Defence-in-depth is structured in five levels (should one level fail, the subsequent level comes into play)

The objectives for the different levels are defined by, e.g. the INSAG10 or recent WENRA documents.



Safety Functions

Safe design in general is characterized by the simultaneous control of the following safety functions (SF): Containment of hazardous materials; Control of chain reactions; Control of removal of the energy produced; Control of radiation protection; Control of non-nuclear risks.



Safety objectives

The safety architecture guarantees the achievement of a set of safety functions, after a given initiating event, while meeting the safety objectives.

The identified initiating events are categorized following their estimated frequency of occurrence.

For each category, **quantitative safety objectives** are usually suggested by the designer and endorsed by the regulators.

The proposal of WENRA/RHWG shows that there is a direct relationship between the DiD and the "**allowable risk domain**".

The designer can superpose the levels of DiD within the area of allowable risk, and simultaneously, give explicit targets for these levels (i.e success criteria, both in terms of performances and reliability).



Challenges

SF: "Control of removal of the energy produced";

Challenge: (possible loss of integrity of the facility structures)

-> e.g. "degradation of the residual heat removal path"

SF: "Control of Radiation protection";

Challenges: (alterations for protection measures against radiation)

-> e.g. "Abnormal exposure under maintenance conditions"

SF: "Control of Non-nuclear risks";

Challenges: changes that alter the loading on the facility structures

-> e.g. the "Explosion".



Initiating events (mechanisms)

Each challenge is materialized by a set of mechanisms / initiating events.

These initiating events are concept specific (SFR or LFR) and even design specific (e.g. SFR with or without intermediate circuit).

The designer shall **systematically** seek mechanisms/initiating events among the plausible phenomena that are either related to the specific technology under consideration (e.g. sodium fires), or induced by the provisions already implemented (e.g. withdrawal of a control rod).

OPT Elements



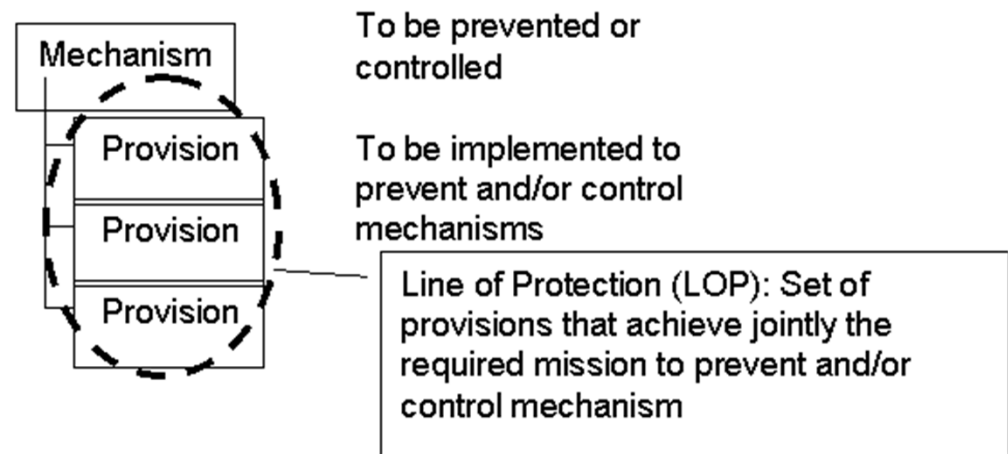
Provisions & LOP

Once identified the initiating events, the designer must specify, for each of them, the provisions that are integrated into the architecture to manage their advent and control /mitigate their consequences.

All provisions are grouped in a Line Of Protection (LOP):

LOP reliability and efficiency will realize the mission requirements while meeting the safety objectives.

The representative overall performance for the LOP will be defined the characteristics of the “weakest link”

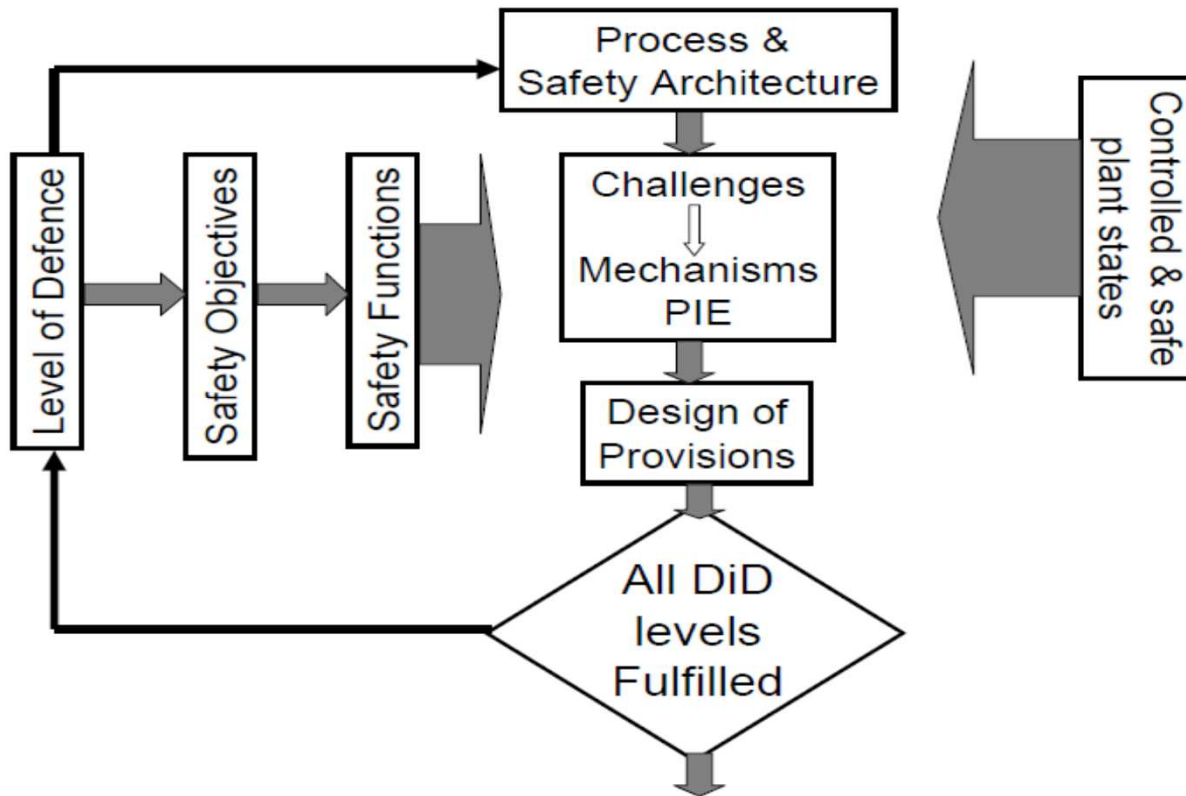


Safety Architecture



The process of identification of the initiators to be considered when sizing the safety architecture, as performed using the OPT, is part of an iterative process.

OPT is completed = safety architecture components identified



OPT Example



Safety Functions & Objectives ⇨
(minimize deviations from normal operating conditions including transient conditions and plant shutdown states)

Level 1 – Objective
 Prevention of deviations from normal operation and failures

SF (1): Control of reactivity
 Acceptance criterion: minimize deviations from normal operating conditions avoiding insertion of reactivity which will demand automatic countermeasures

SF(2) : Energy removal

SF(3) : FP Confinement

Challenges ⇨

Change in core geometry during normal operation

Unexpected reactivity insertion

Temperature Variation

Change in Fuel/ Coolant ratio

Core compactation and or core shacking.

Human error on core configuration

Na voiding

Na vaporization

Mechanisms & Phenomena

Wrong positioning of a fuel assembly or absorber

Error in the nature of the implemented materials

No allowed wrong positioning

Meeting of the allowed ranges in terms of materials characteristics

Avoidance by design of the possibility for loading absorbers in the fuel positions and vice versa

Quality assurance provisions during fuel and absorber fabrication

Quality assurance provisions during fuel and absorber loading (and shifting)

⇨ Specific acceptance criterion

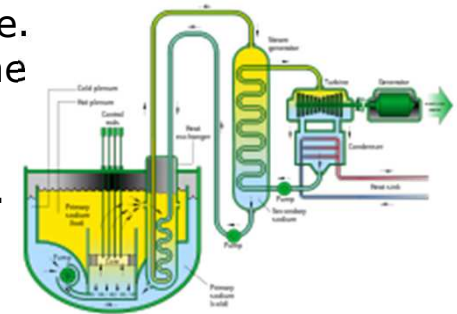
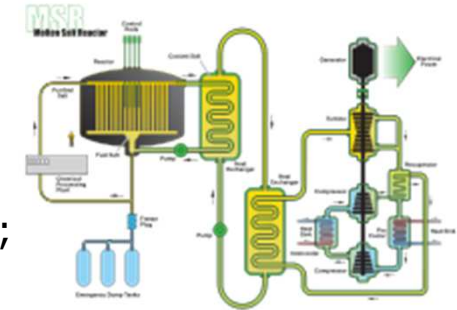
Provisions for the Level 1 of the Did

OPT Implementation



The OPT method is applicable to concepts at different stage of development:

- The OPT is used to identify initiators and to build the safety architecture for concepts at a preliminary design stage (e.g. MSR);
- To finalize the design of an advanced/completed reactor (e.g. the JSFR), the OPT can be used to check:
 - that all the initiators are adequately addressed;
 - that all levels of DiD are properly structured and organized (i.e. the necessary provisions are in place and adequate to fulfill the mission);
 - that the mutual independence of the DiD levels is guaranteed.



Note: A provision can be used for different initiating events and / or at different levels of the DiD if the events which require the provision under consideration are completely **independent**.

The OPT facilitates the identification of possible conflicts and allows to verify the acceptability of the final architecture.



The integration of safety and security concerns should be searched at the design level (as can be used as a [tool to address also the security concerns](#))

With logic similar to that of OPT -> Specific security provisions for the control of security concerns, through the consideration of "security functions" such as, for example:

- control of flows of hazardous materials;
- protection against malevolent hazards.

The comparison of the representation of the safety and security architecture will be helpful to fulfill and prove the effective integration.



The role and place of the OPT within ISAM is defined on interactions with the other ISAM tools :

- with the **QSR** to check the compliance with principles requirements and guidelines,
- with the **PIRT** for the identification of the initiators to be considered for the design of the installation,
- with the **DPA** safety analysis which allow checking the achievement of safety objectives.

Finally the OPT has to be considered as a **preliminary step** for the preparation and the realization of the **PSA**.

Safety Assessment Tools after Fukushima



- Critical Analysis is needed to assess the adequacy of the current tools? Why Safety Assessments so far were not able to point out to Fukushima likewise events?
- What is to be done after Fukushima? – after TMI we added PSA to DBA, After Chernobyl we added the "safety culture" concept; after Fukushima - ? Extreme events? Tools to assess the implementation of DiD ? Can OPT help?
- How the new safety assessments will have to be presented –Need to think of a new structure of the SARs and define the full set of events to be considered within the SARs?
- The exhaustiveness of the NPP Safety Assessment has to be demonstrated



Thank you for your attention