Risk & Safety Working Group

L. Ammirabile, R. Nakai

3rd GIF Symposium, Makuhari Messe, Japan, 19 May 2015

Outline

- ***Background***
- ***Safety Assessment***
- ***Integrated Safety Assessment Methodology (ISAM)***
- ***Practical example of ISAM application***

Purpose of Risk & Safety Working Group

- ***Primary objective***
  - *Provide an effective and harmonised approach to the safety assessment of Generation IV systems in collaboration with and in support of all six System Steering Committees*
- ***Work Scopes***
  - *Propose safety principles, objectives, and attributes based on Gen-IV safety goals to guide R&D plans*
  - *Provide consultative support to SSCs and other Gen IV entities and undertake appropriate interactions with regulators, IAEA, and other stakeholders*
  - ***Development of a Safety Assessment Methodology***

Safety Assessment

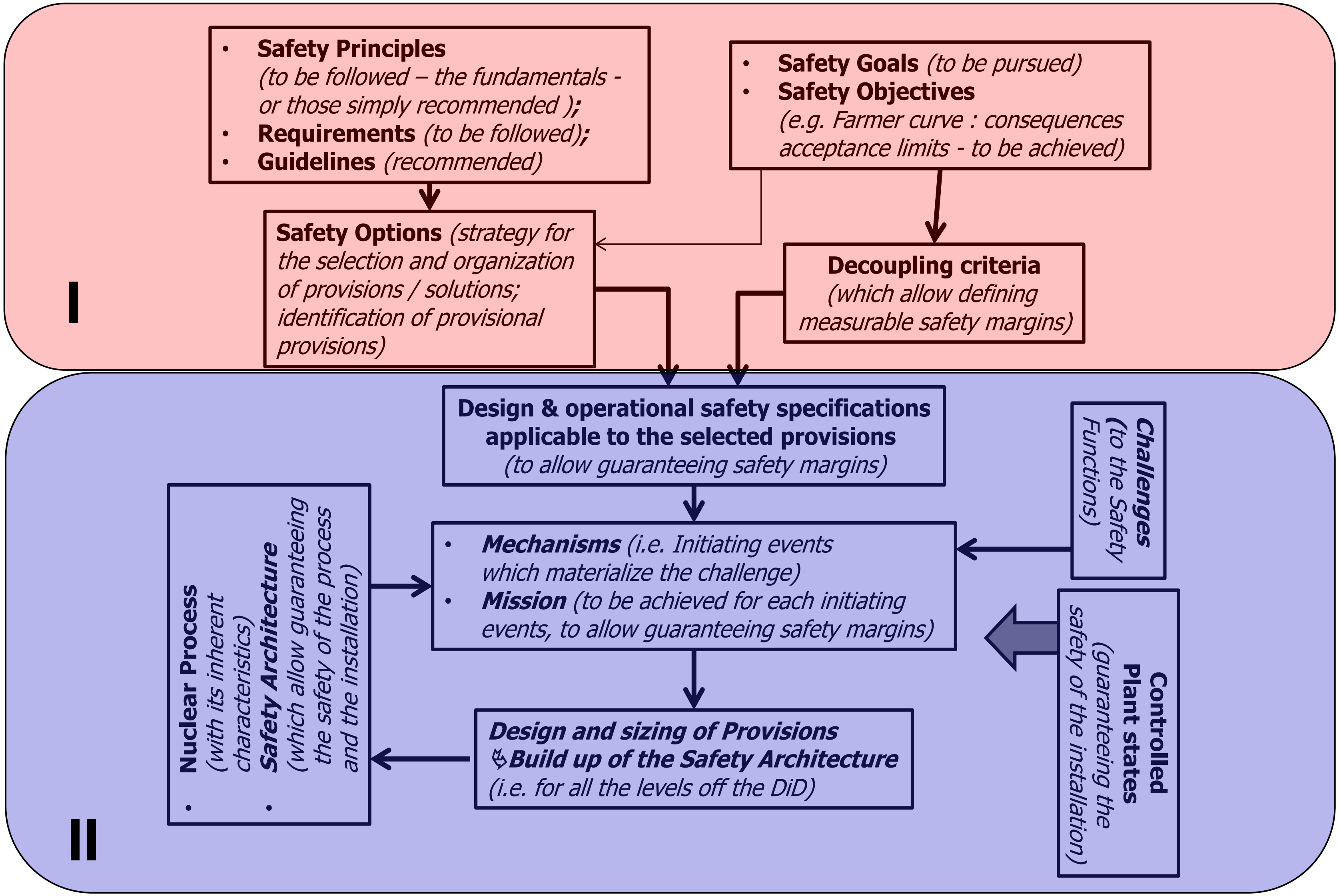
Following the indications of IAEA safety assessment is

"*The systematic process that is carried out throughout the design process to ensure that all the relevant safety requirements are met by the proposed (or actual) design of the plant………The design and the safety assessment are part of the same iterative process….. which continues until a design solution meets all the requirements…..and that a comprehensive safety analysis has been carried out".*

In this approach we can, therefore, identify two phases:

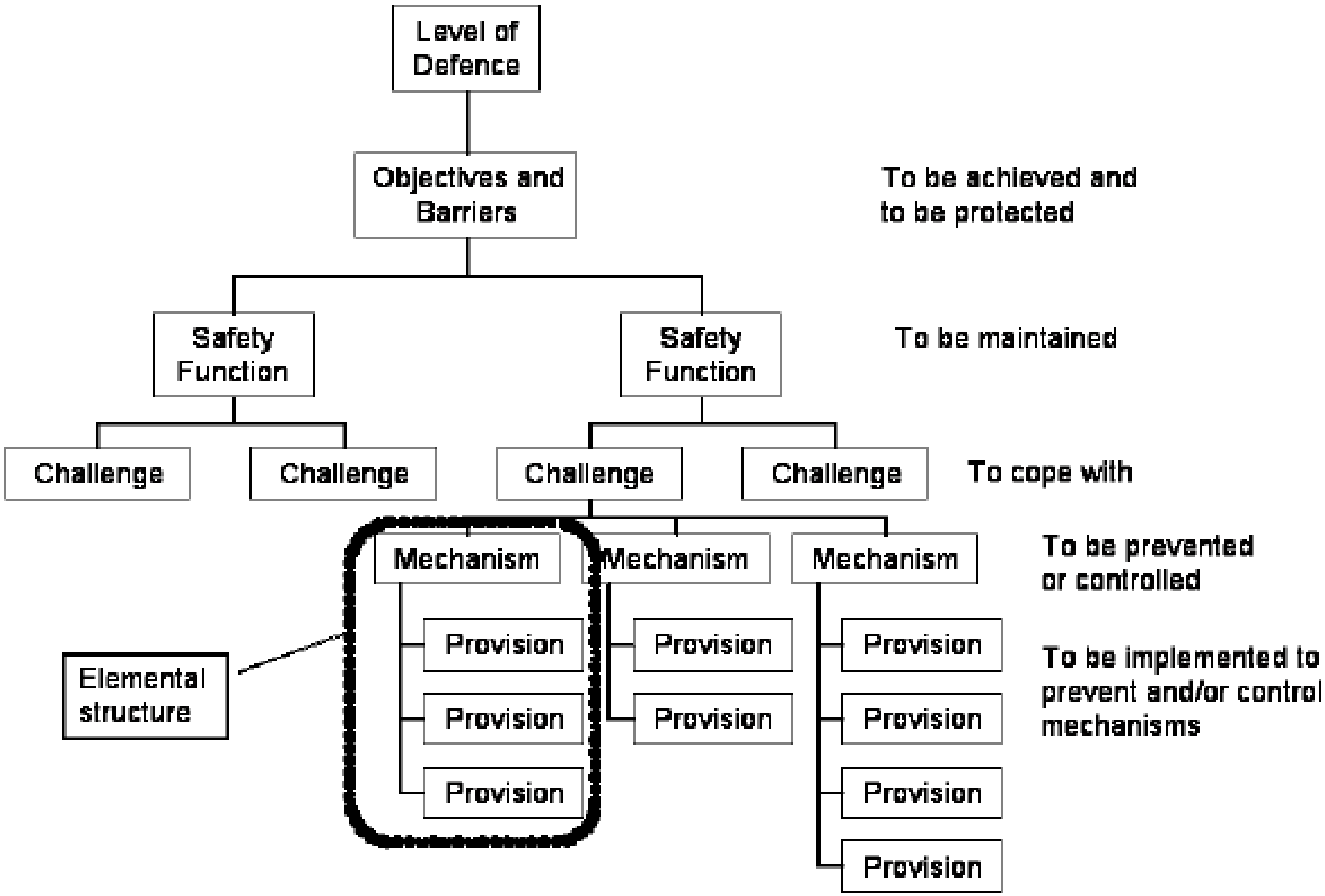
I. **Verification of the compliance** of the system with the principles, the requirements, the guidelines

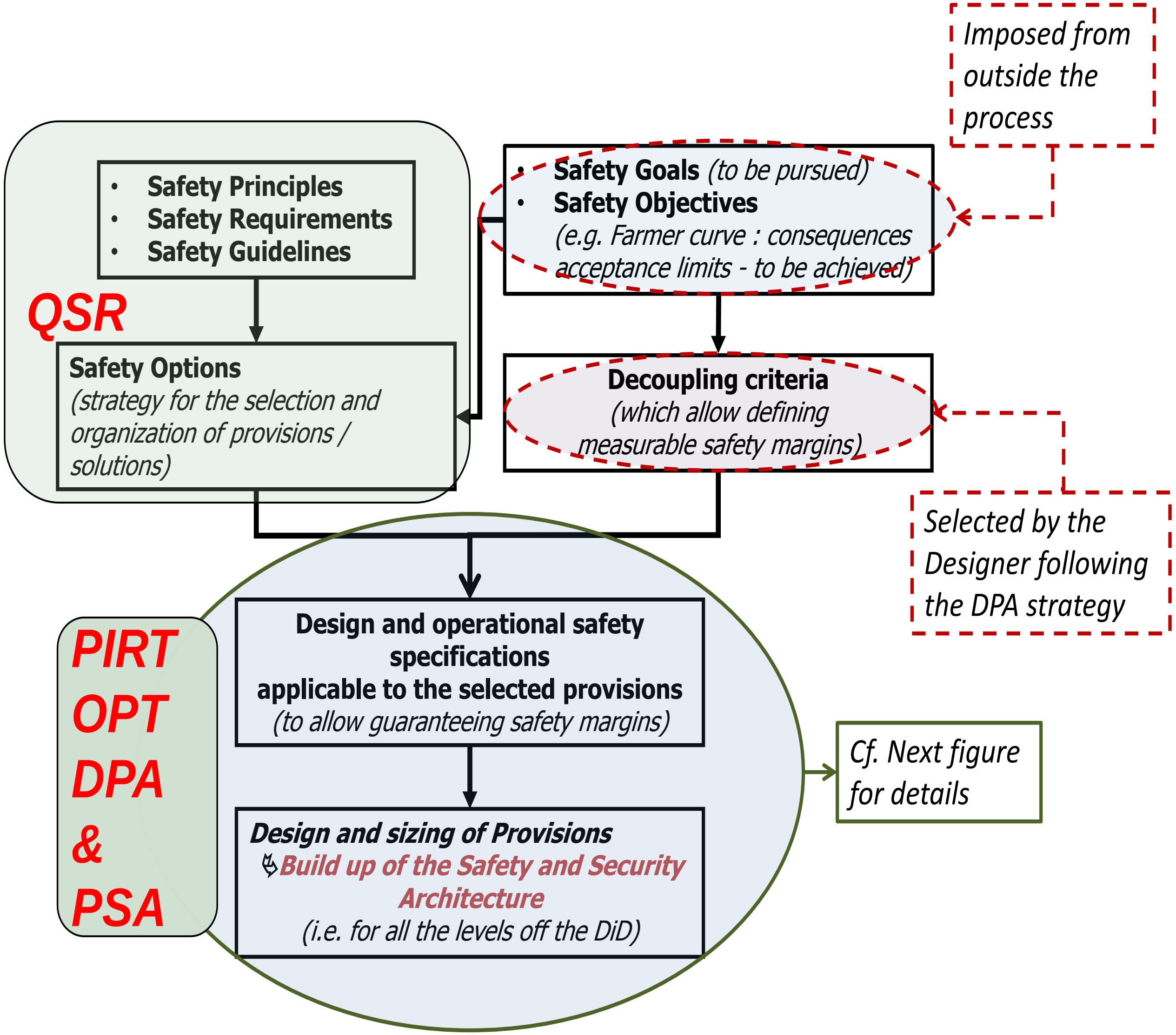
II. **Verification of the conformity** of the safety architecture of the system with the quantitative safety objectives.

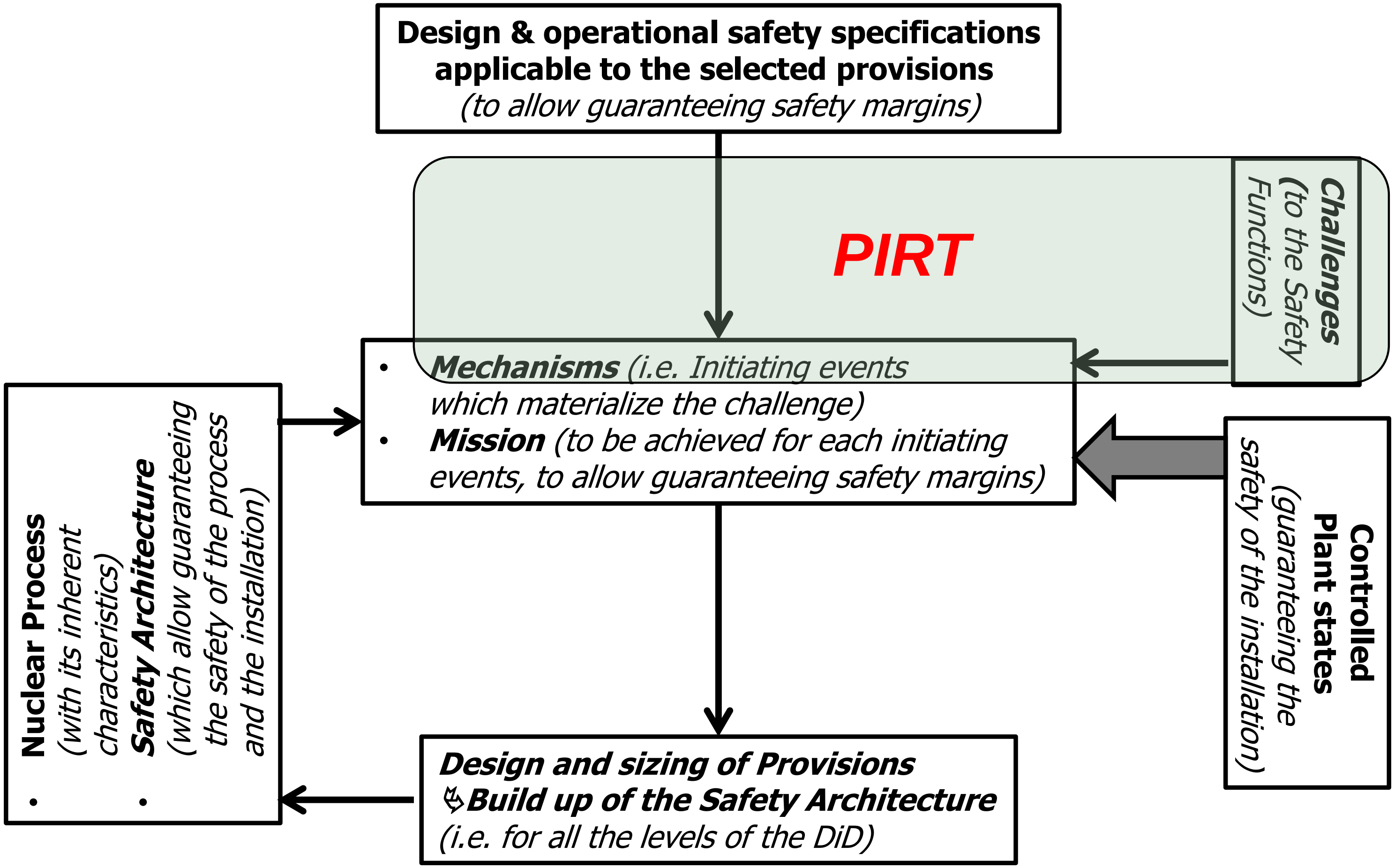


• Safety Principles (to be followed – the fundamentals - or those simply recommended);
• Requirements (to be followed);
• Guidelines (recommended)
• Safety Goals (to be pursued)
• Safety Objectives (e.g. Farmer curve : consequences acceptance limits - to be achieved)
Safety Options (strategy for the selection and organization of provisions / solutions; identification of provisional provisions)
Decoupling criteria (which allow defining measurable safety margins)
I
Design & operational safety specifications applicable to the selected provisions (to allow guaranteeing safety margins)
Challenges (to the Safety Functions)
• Nuclear Process (with its inherent characteristics)
• Safety Architecture (which allow guaranteeing the safety of the process and the installation)
• Mechanisms (i.e. Initiating events which materialize the challenge)
• Mission (to be achieved for each initiating events, to allow guaranteeing safety margins)
Controlled Plant states (guaranteeing the safety of the installation)
Design and sizing of Provisions
Build up of the Safety Architecture
(i.e. for all the levels off the DiD)
II

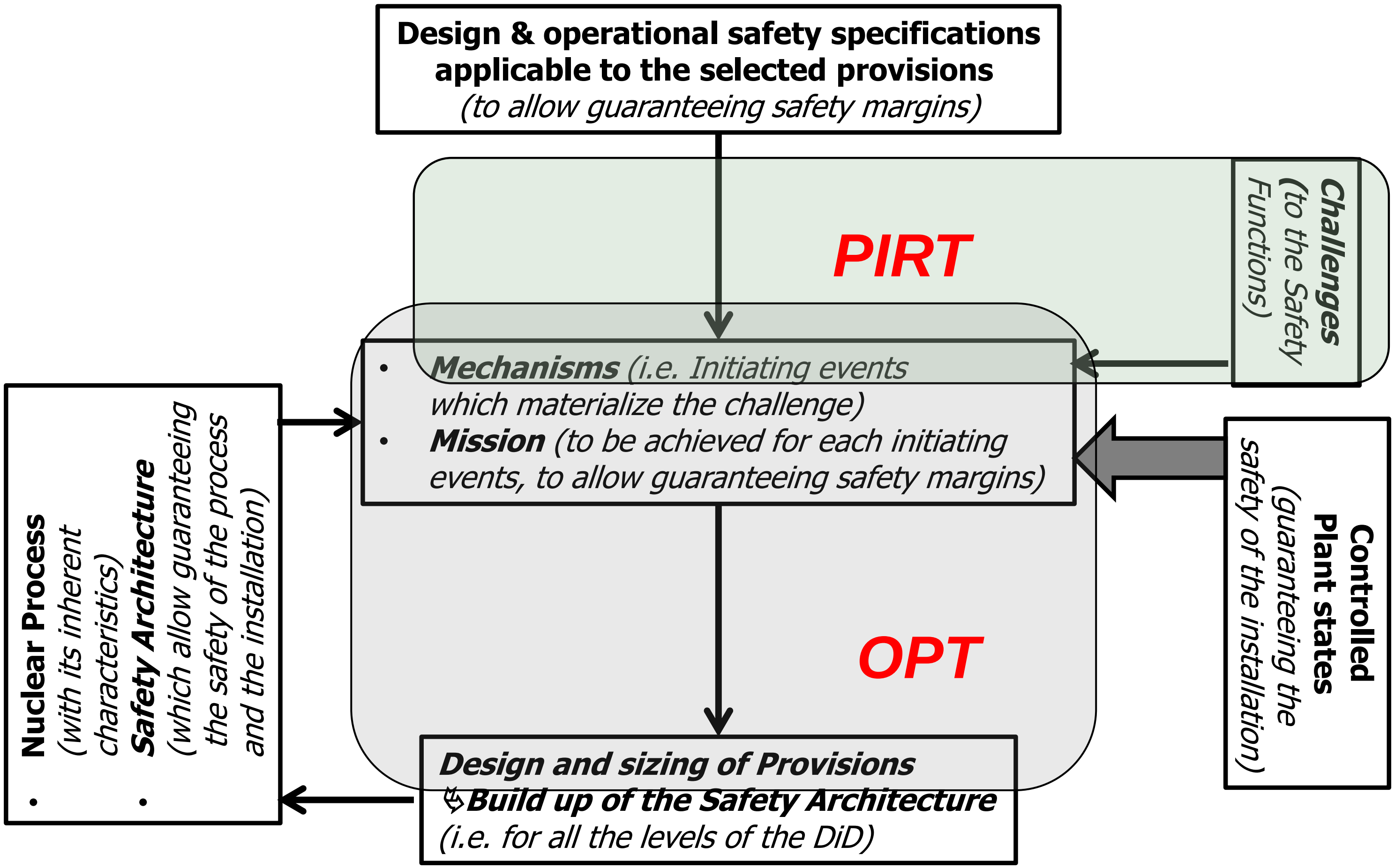
Pre-Conceptual Design | Conceptual Design | Final Design | Licensing and Operation

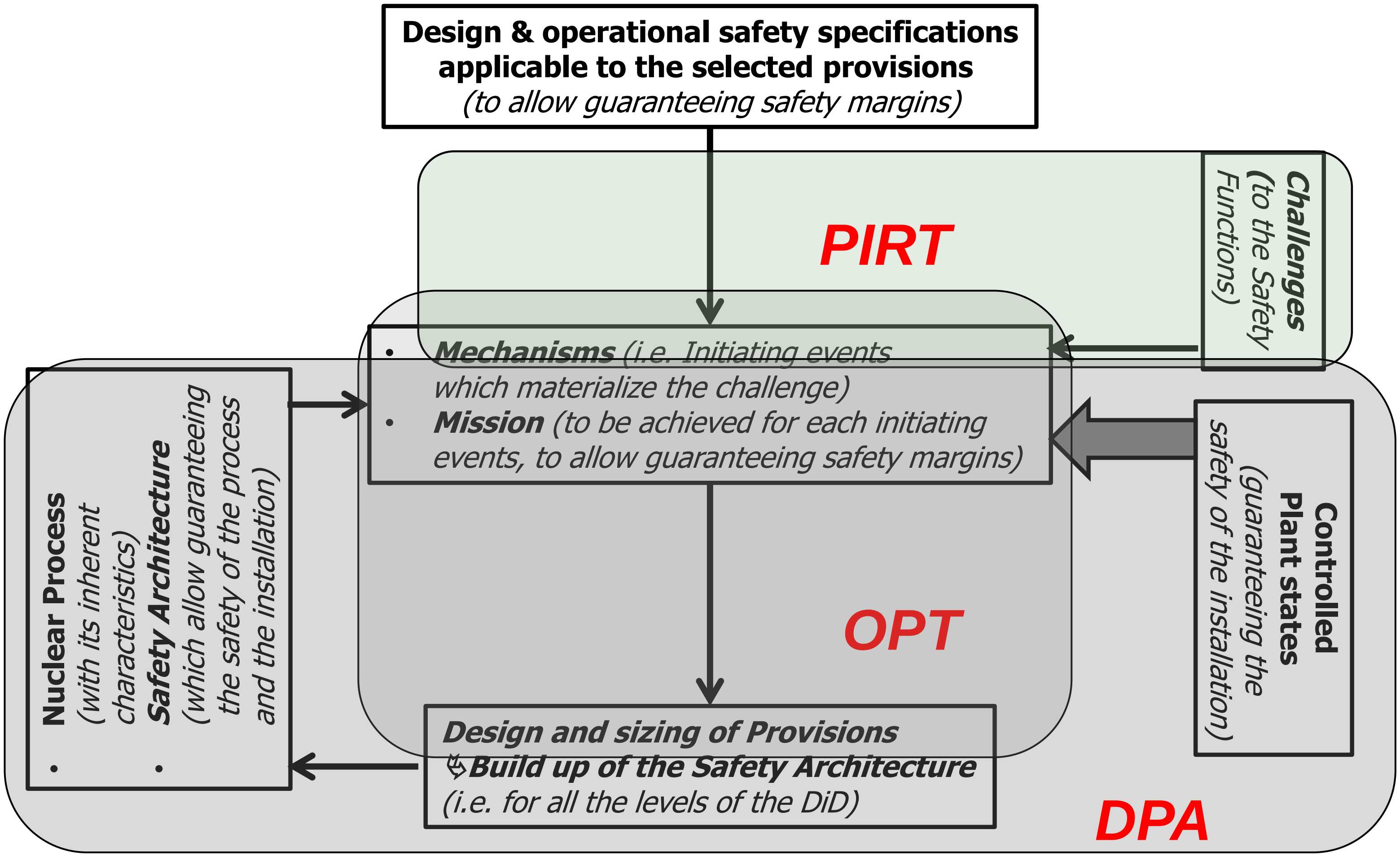



Imposed from outside the process
Safety Principles
Safety Requirements
Safety Guidelines
QSR
Safety Options
(strategy for the selection and organization of provisions / solutions)
Safety Goals (to be pursued)
Safety Objectives
(e.g. Farmer curve : consequences acceptance limits - to be achieved)
Decoupling criteria
(which allow defining measurable safety margins)
Selected by the Designer following the DPA strategy
PIRT
OPT
DPA
&
PSA
Design and operational safety specifications
applicable to the selected provisions
(to allow guaranteeing safety margins)
Design and sizing of Provisions
Build up of the Safety and Security Architecture
(i.e. for all the levels off the DiD)
Cf. Next figure for details

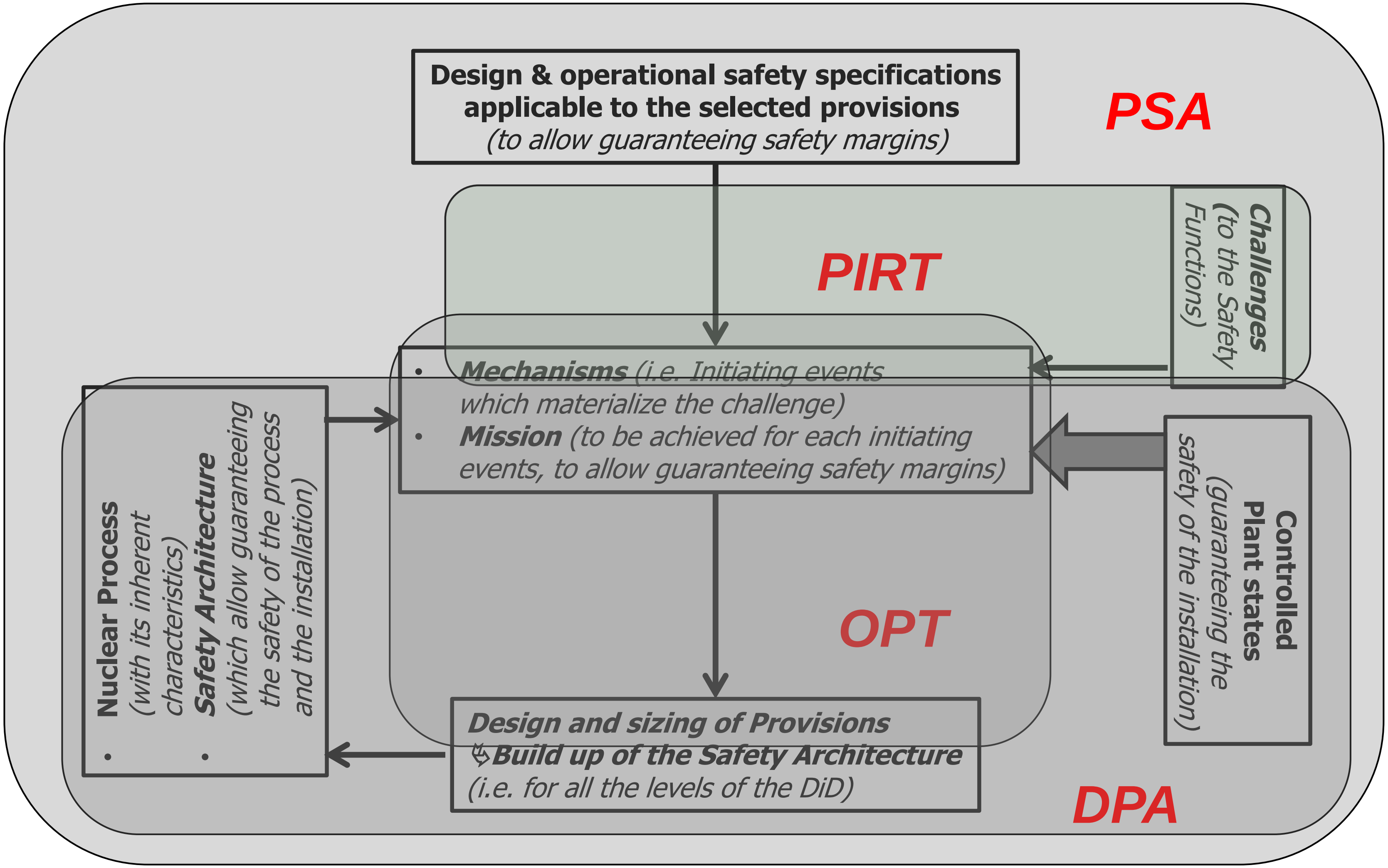


Design & operational safety specifications applicable to the selected provisions
(to allow guaranteeing safety margins)
PIRT
Challenges (to the Safety Functions)
• Mechanisms (i.e. Initiating events which materialize the challenge)
• Mission (to be achieved for each initiating events, to allow guaranteeing safety margins)
Controlled Plant states (guaranteeing the safety of the installation)
• Nuclear Process (with its inherent characteristics)
• Safety Architecture (which allow guaranteeing the safety of the process and the installation)
Design and sizing of Provisions
Build up of the Safety Architecture
(i.e. for all the levels of the DiD)


Design & operational safety specifications applicable to the selected provisions
(to allow guaranteeing safety margins)
PIRT
Challenges
(to the Safety Functions)
• Mechanisms (i.e. Initiating events which materialize the challenge)
• Mission (to be achieved for each initiating events, to allow guaranteeing safety margins)
• Nuclear Process
(with its inherent characteristics)
• Safety Architecture
(which allow guaranteeing the safety of the process and the installation)
Controlled Plant states
(guaranteeing the safety of the installation)
OPT
Design and sizing of Provisions
↳Build up of the Safety Architecture
(i.e. for all the levels of the DiD)



Design & operational safety specifications applicable to the selected provisions
(to allow guaranteeing safety margins)
PIRT
Challenges
(to the Safety Functions)
• Mechanisms (i.e. Initiating events which materialize the challenge)
• Mission (to be achieved for each initiating events, to allow guaranteeing safety margins)
• Nuclear Process
(with its inherent characteristics)
• Safety Architecture
(which allow guaranteeing the safety of the process and the installation)
OPT
Controlled Plant states
(guaranteeing the safety of the installation)
Design and sizing of Provisions
Build up of the Safety Architecture
(i.e. for all the levels of the DiD)
DPA

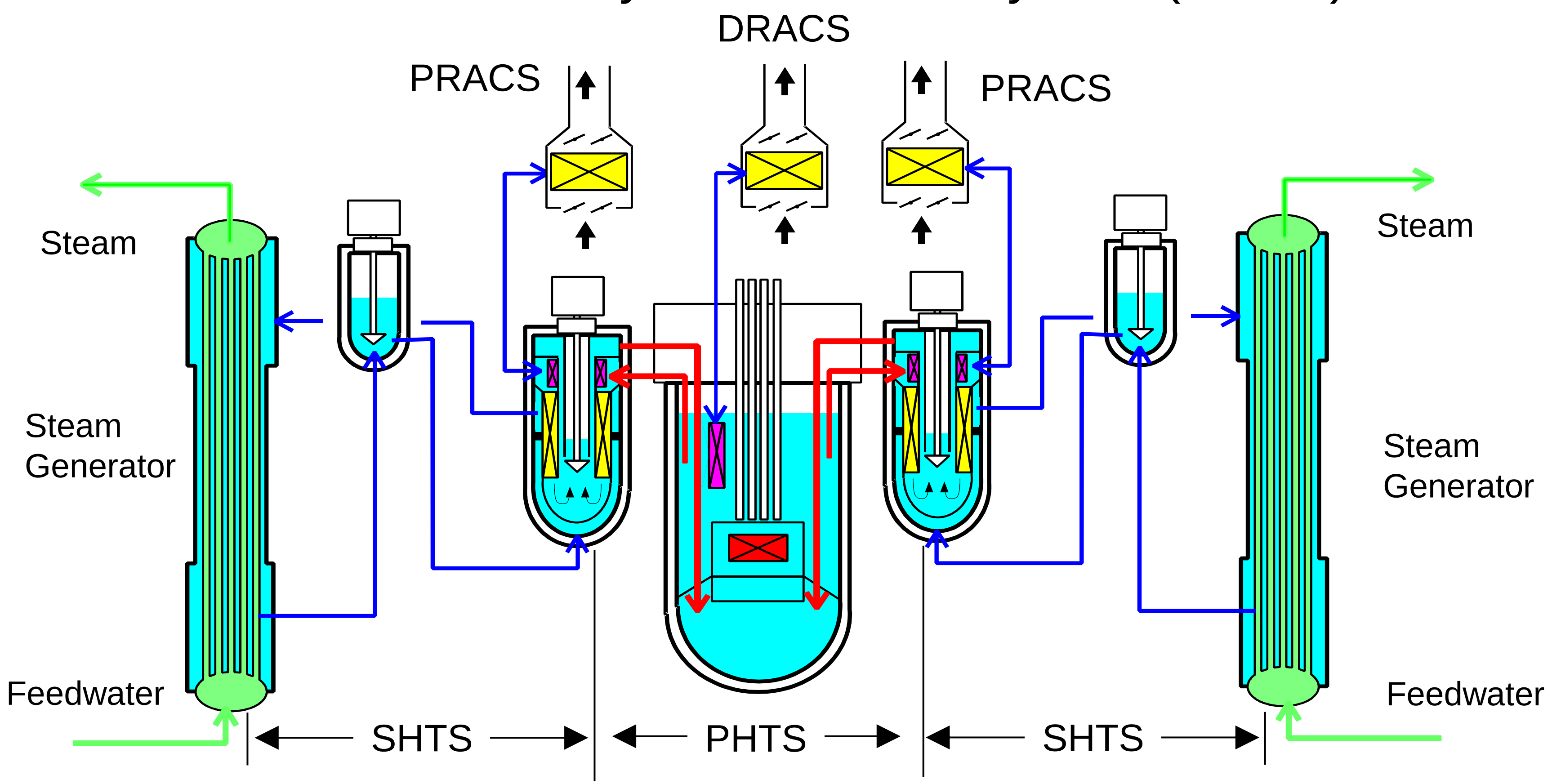


Design & operational safety specifications applicable to the selected provisions
(to allow guaranteeing safety margins)
PSA
PIRT
Challenges (to the Safety Functions)
Mechanisms (i.e. Initiating events which materialize the challenge)
Mission (to be achieved for each initiating events, to allow guaranteeing safety margins)
Nuclear Process (with its inherent characteristics)
Safety Architecture (which allow guaranteeing the safety of the process and the installation)
Controlled Plant states (guaranteeing the safety of the installation)
OPT
Design and sizing of Provisions
Build up of the Safety Architecture
(i.e. for all the levels of the DiD)
DPA

	QSR	PIRT	OPT	DPA	PSA
Regulatory Framework (Goals, objectives, principles, requirements, guidelines)	✓				
Selection of Safety Options and provisional Provisions		✓	✓	✓	✓
1. Compliance / consistency of the design options with the principles, requirements and guidelines	✓				
2. Identification, prioritization and correction (if feasible) of discrepancies,	✓	✓			
3. Identification of challenges to the safety functions,		✓	✓		
4. Identification of mechanisms (initiating events) and selection of significant (envelope) plants conditions to be considered for the design basis,		✓	✓	✓	
5. Identification and selection of needed provisions,	✓	✓	✓		
6. Design and sizing of the provisions,			✓	✓	
7. Response to transients (safety analysis),				✓	✓
8. Final assessment for a safety architecture that should be:					
○ *Exhaustive,*		✓	✓		
○ *Progressive,*			✓	✓	✓
○ *Tolerant,*				✓	✓
○ *Forgiving,*				✓	✓
○ *Balanced.*					✓

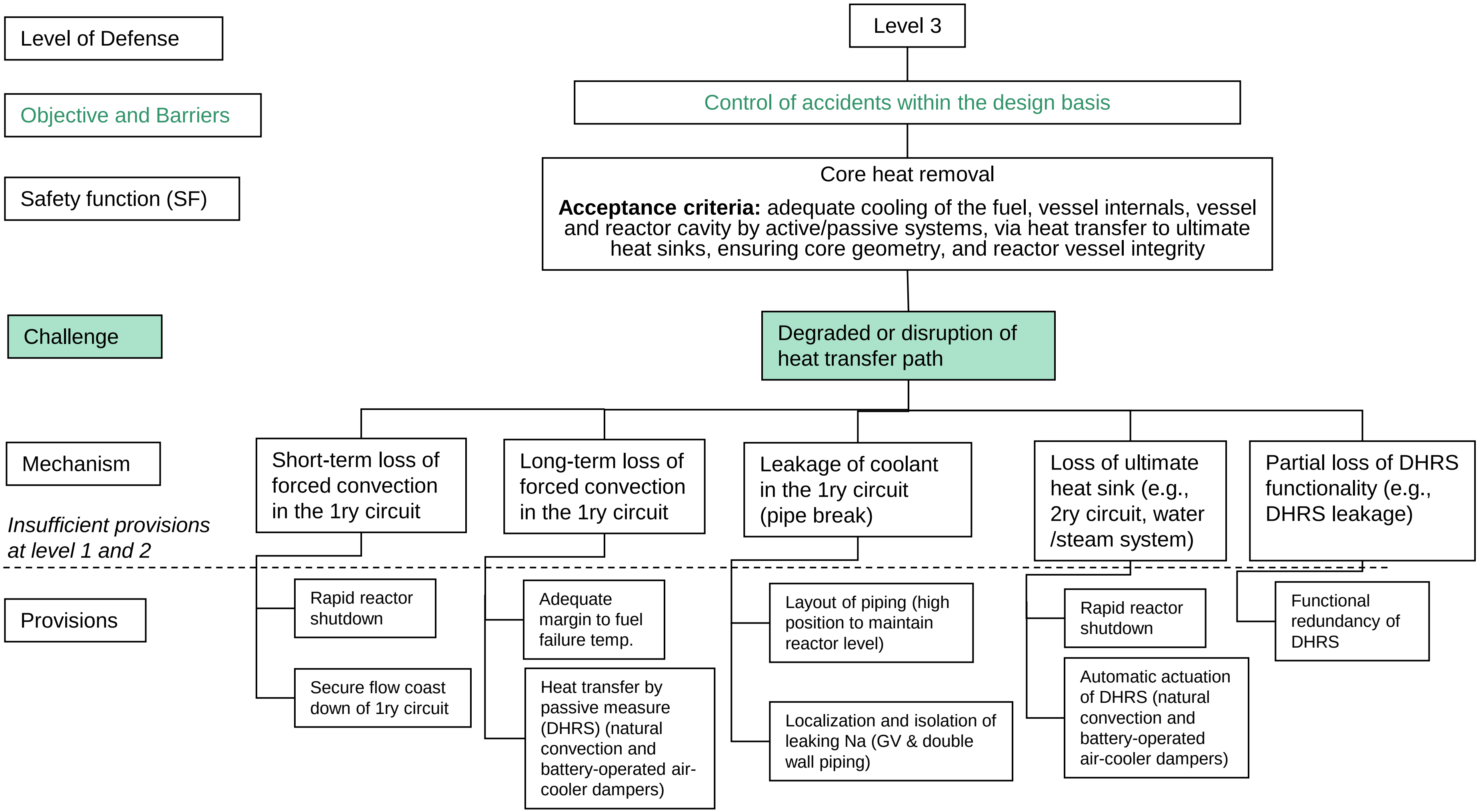
Practical example for the ISAM implementation

Outline of decay heat removal system (DHRS)

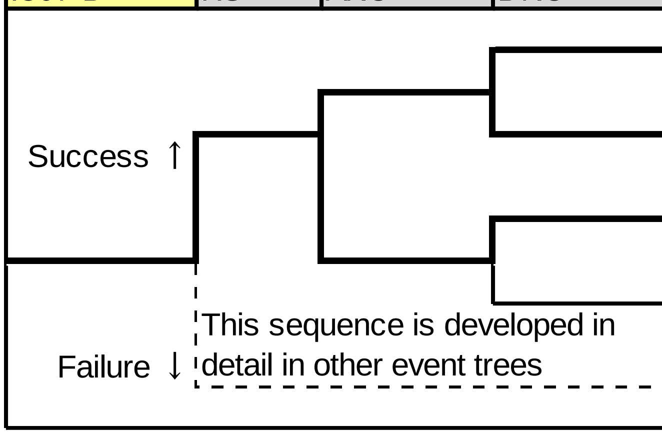


PRACS: Primary Reactor Auxiliary Cooling System
DRACS: Direct Reactor Auxiliary Cooling System
PHTS: Primary Heat Transport System
SHTS: Secondary Heat Transport System

OPT for SF 2 (core heat removal) at Lev.3 of DiD



Identification of the scenarios to be analyzed, which result in success or PLOHS within 24hr based on the event tree model in the JSFR Level-1 PSA



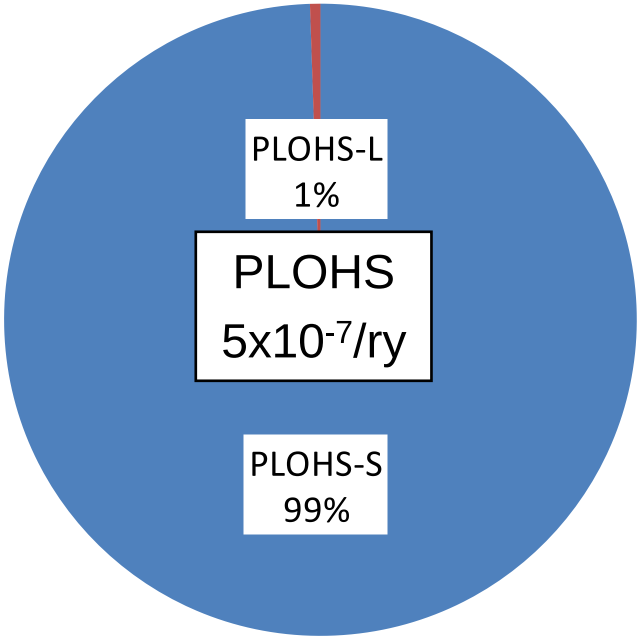
Loss of circulation capability in PRACS-B	Reactor SCRAM	Passive cooling by using PRACS-A *	Passive cooling by using DRACS *	Seq. No.	Accident sequence	Core integrity	
IC07-B	RS	ANC	DNC			Before DPA	After DPA
				1	/RS*/ANC*/DNC (Successful DBA scenario)	**Should be OK (1)**	OK
				2	/RS*/ANC*DNC (Passive cooling by using PRACS-A alone)	**Unknown (1)**	Damage
				3	/RS*ANC*/DNC (Passive cooling by using DRACS alone)	**Unknown (1)**	Damage
				4	/RS*ANC*DNC (Loss of all heat sink)	Damage	Damage
				5	-	-	-

*; This cooling mode relies only on the safety-related systems.

(1) Need to be confirmed by DPA

PLOHS: Protected Loss Of Heat Sink, which includes insufficient heat removal capacity.

PSA result: Contribution to PLOHS frequency broken down by time phases with different success criteria

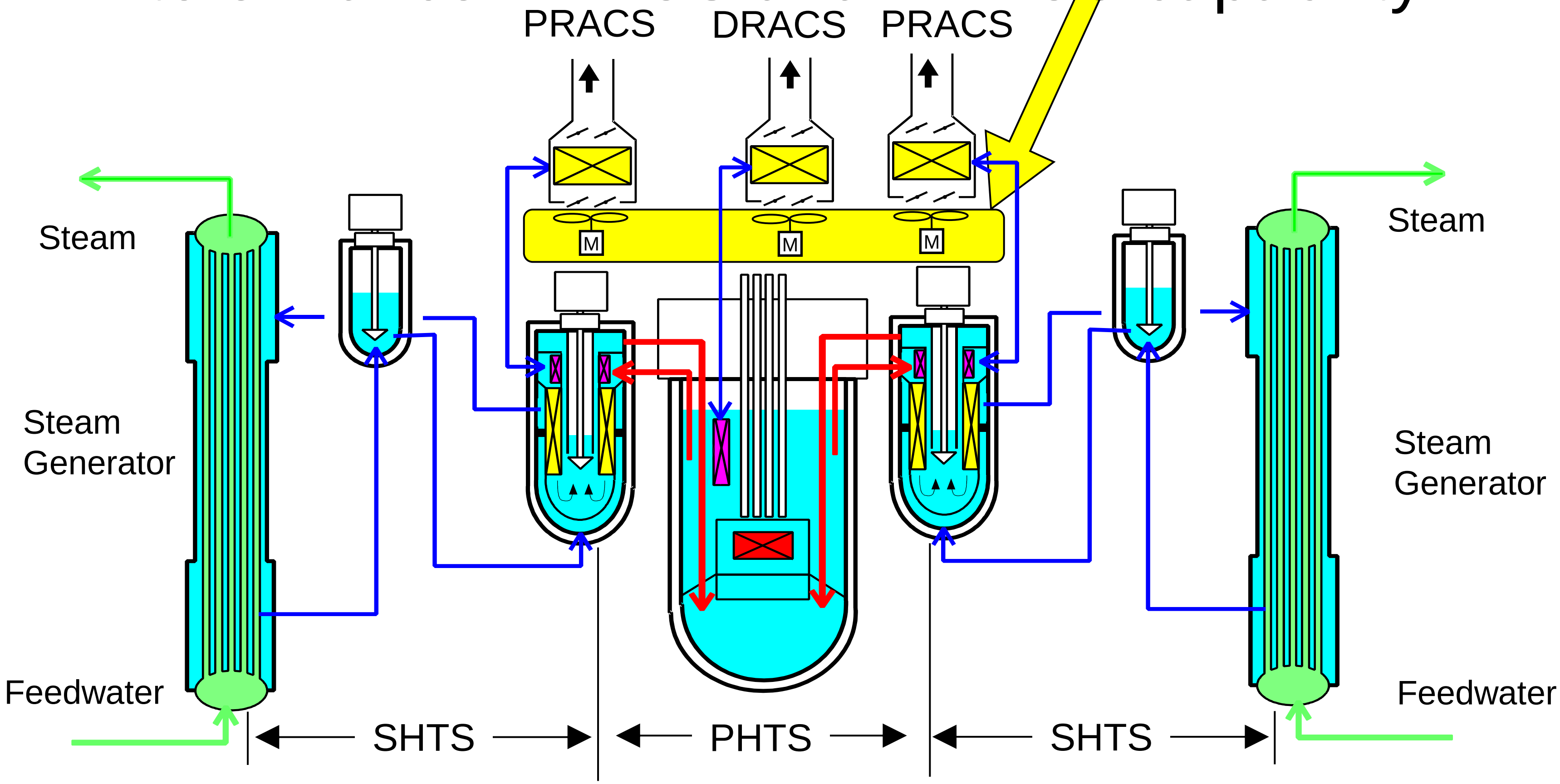


PLOHS-S	PLOHS sequences that occurs within 24hr after reactor shutdown
PLOHS-L	PLOHS sequences that occurs after successful decay heat removal of 24hr within the mission time of 1 month

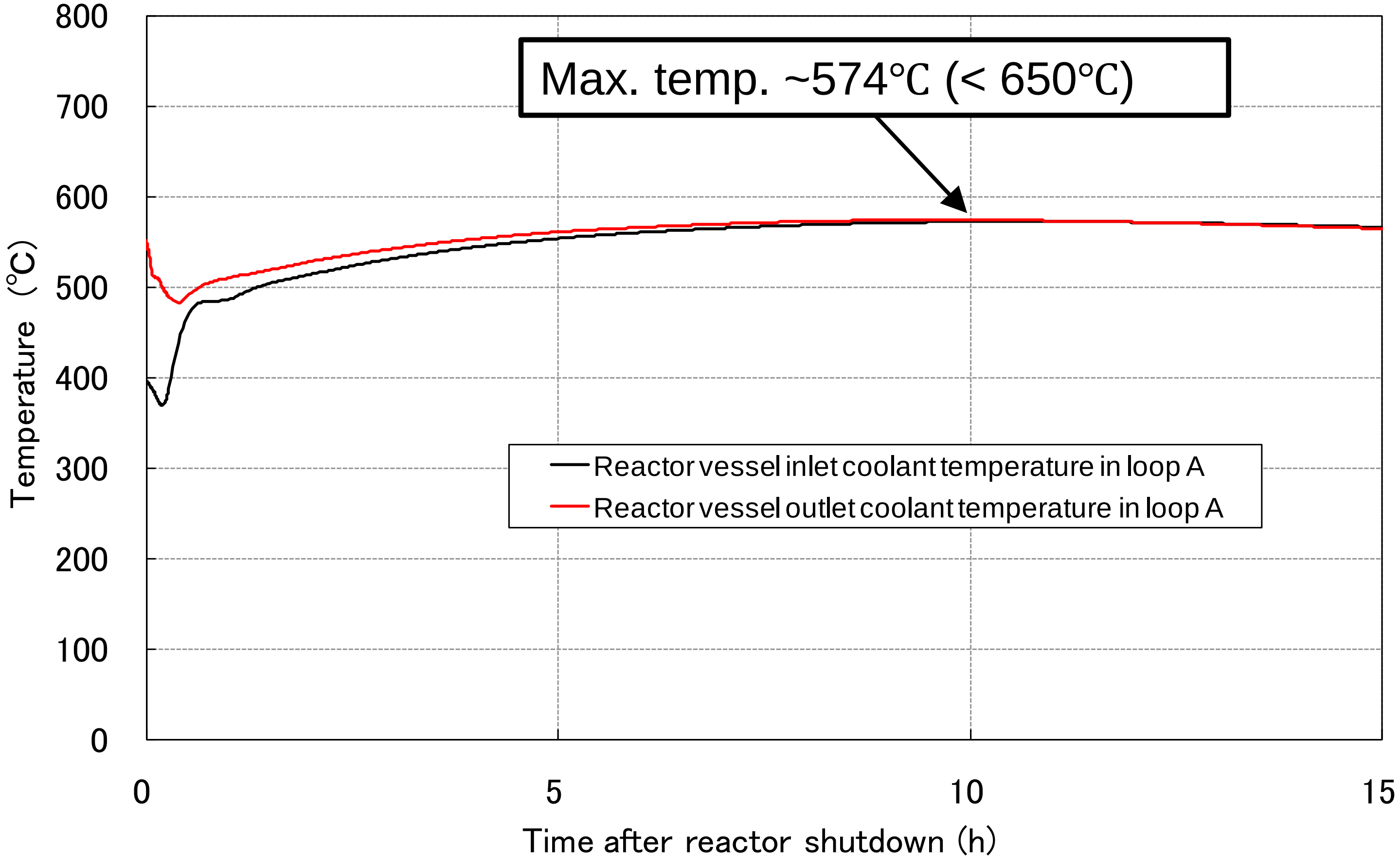
*; ordered by contribution

- The dominant sequence is loss of two out of three trains of DHRS within 24h after reactor shutdown.
- Enhancement of heat removal capacity of a single train of DHRS in this time period has potential to reduce 99% of total PLOHS frequency.

Design improvement: Non-safety-related AC blowers to enhance PRACS and DRACS capability



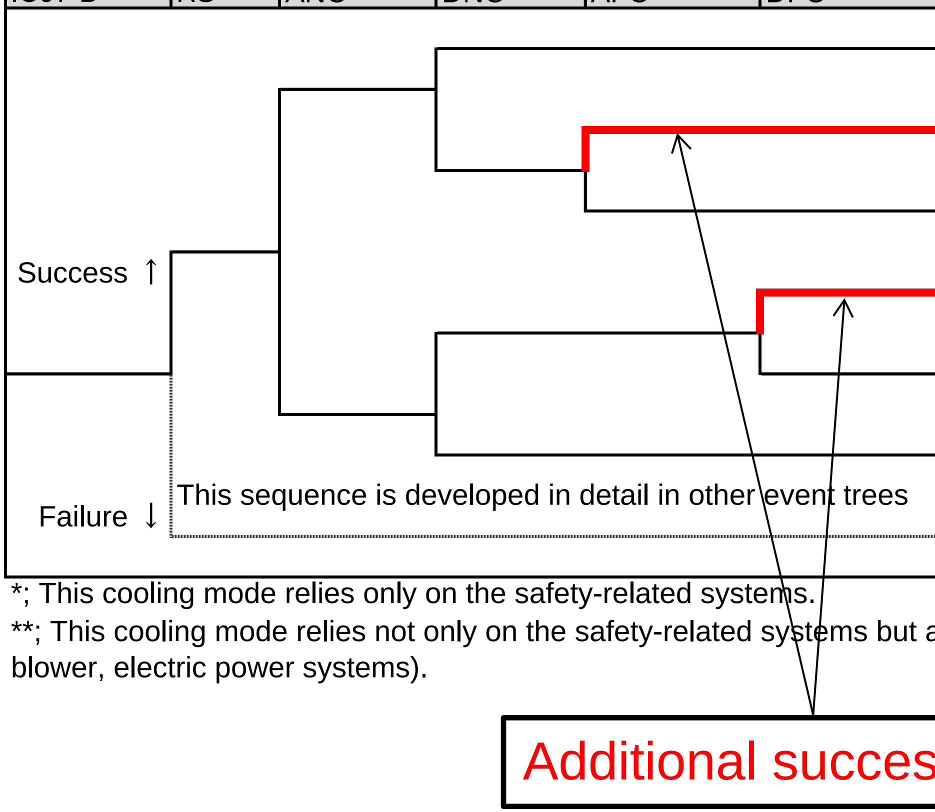
Additional DPA result: Forced-air flow with blower & Na natural circulation cooling scenario by using DRACS alone



This accident sequence results keep the reactor coolant boundary integrity.

DHRS event tree model considering AC blower operation

Loss of circulation capability in PRACS-B	Reactor SCRAM	Passive cooling by using PRACS-A *	Passive cooling by using DRACS *	Forced air flow cooling by using PRACS-A **	Forced air flow cooling by using DRACS **
IC07-B	RS	ANC	DNC	AFC	DFC

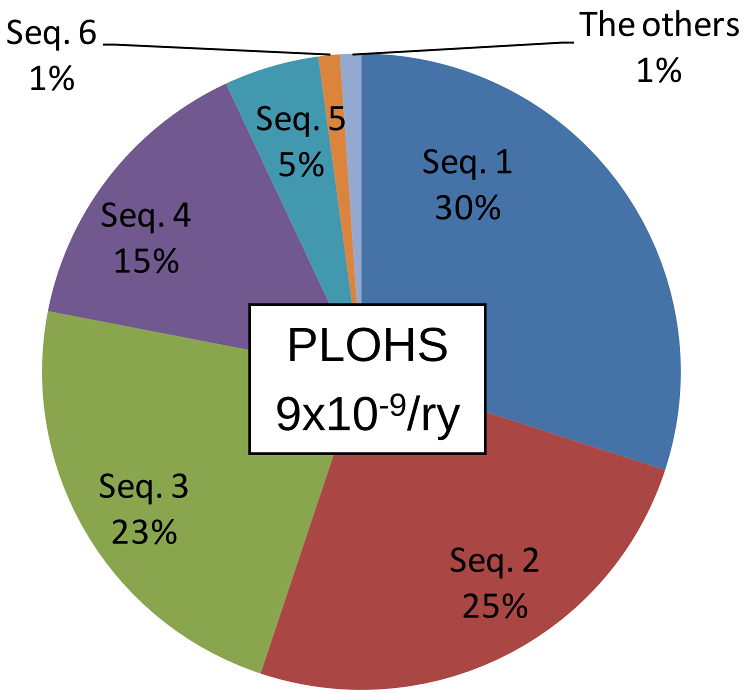


Seq. No.	Accident sequence	Core integrity
1	/ANC*/DNC (Successful DBA scenario)	OK
2	/ANC*DNC*/AFC (**Forced air flow cooling by using PRACS-A alone**)	OK
3	/ANC*DNC*AFC (Passive cooling by using PRACS-A alone)	Damage
4	ANC*/DNC*/DFC (**Forced air flow cooling by using DRACS alone**)	OK
5	ANC*/DNC*DFC (Passive cooling by using DRACS alone)	Damage
6	ANC*DNC (Loss of all heat sink)	Damage
7	-	-

*; This cooling mode relies only on the safety-related systems.

**; This cooling mode relies not only on the safety-related systems but also on automatic actuation of the non-safety-related systems (i.e., air blower, electric power systems).

PSA result: Major contributors to PLOHS frequency broken down by combination of loss of mitigation systems



Seq. 1	Loss of passive cooling function in 2 loops & failure to start AC blower in the other loop
Seq. 2	Loss of all electric power & human error in manual damper operation
Seq. 3	Loss of passive cooling function in 3 loops (after 24h)
Seq. 4	Common cause failure of PRACS dampers & failure to start AC blower in DRACS
Seq. 5	Common cause failure of PRACS dampers & loss of active cooling function in DRACS AC
Seq. 6	Na leakage in one loop of DHRS & DHRS actuation signal failure in one loop & human error in manual damper operation & failure to start AC blower in the other loop

*; ordered by contribution

PSA combined with DPA showed quantitatively that introduction of AC blowers in both PRACS and DRACS can improve reliability of decay heat removal significantly.

Final Considerations

- *ISAM vs Safety Assessment*
- *No new tools but a systematic methodology*
- *Built-in rather than added-on*
- *Help designer in the licensing process (safety case)*
- *Extended pilot application desirable*

Thank you

Website: https://www.gen-4.org/gif/jcms/c_9366/risk-safety

Back-up slides

Review of RSWG methodology against the lessons learned from Fukushima accident

Reviewed documents:

- Nuclear Regulation Authority (NRA)
- Japan Nuclear Safety Institute (JANSI) which, itself, organized a synthesis of different contributions
- American Society of Mechanical Engineer (ASME)
- Institute of *Nuclear* Power Operations (INPO)
- International Atomic Energy Agency (IAEA)
- OECD - Nuclear Energy Agency (AEN)
- Western European Nuclear Regulator Association (WENRA)

General Considerations

- The foundation of ISAM remains the notion of defence in depth (DiD) and its principles:
  - The need for an approach that complies fully with the principles of DiD to address internal and external events;
  - The requirement for a deep knowledge of the safety architecture.
- The safety architecture consists of SSCs (material provisions) and also of immaterial provisions (e.g. inherent characteristics and / or procedures)
- No critical showstoppers are identified for the application of ISAM in domains outside the reactor design and in particular as concerns the irradiated fuel storage pool.

Qualitative safety Review - QSR

1. The QSR tables should firstly be reviewed to take into account the revised version of the IAEA requirements formulated within the N°SSR 2/1;
2. The technical recommendations and foreseen characteristics and features that address the integration of Design Extension Conditions (DEC A & DEC B) as formulated by WENRA should be considered.
3. Specific effort should be implemented to translate into specific recommendations and characteristics the need for the practical elimination of the 4th level of the DiD.

Phenomena Identification Ranking Table - PIRT

1. Extend PIRT investigation to cover extremely rare events and the corresponding phenomenology.
2. Expand to plant conditions looking for the possible cliff-edge effects.
3. Consider plausible interaction between units on the same site
4. Extend PIRT to specific sequences as cyberterrorism.

Deterministic and Phenomenological Analysis - DPA

1. The analytical models should be improved coherently with the indication provided by other tools (PIRT, PSA) (e.g. for the integration of external hazards).

Objective Provision Tree – Line of Protection OPT/LOP

The OPT/LOP methodology should evolve to better consider the request for practical elimination of the failure of the 4th level of the DiD.

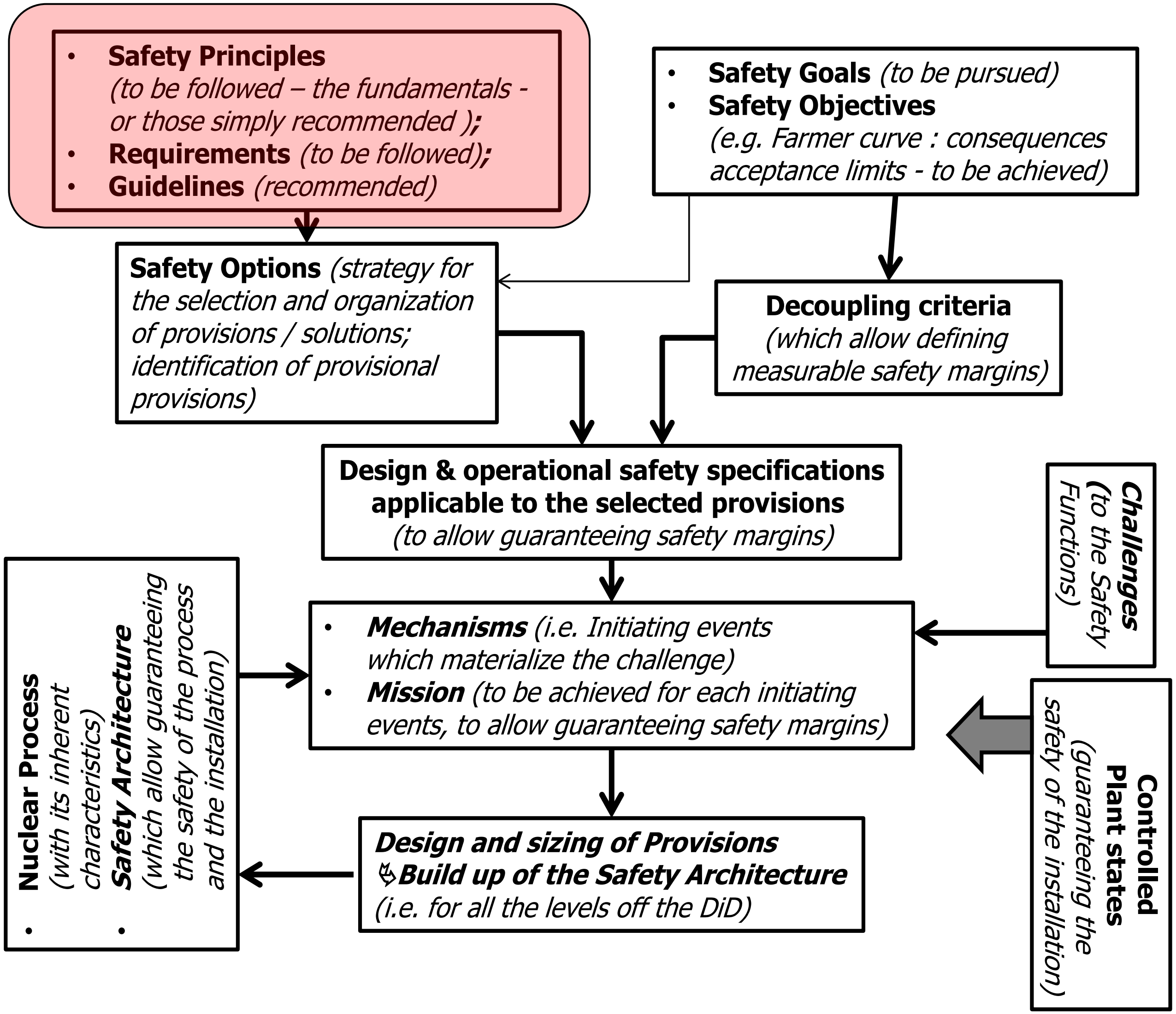
To cover the off-site emergency preparedness, a complementary step devoted to the 5th level of the DiD could be added.

The harmonization of safety and security, will likely lead to adjustments and improvements for the OPT/LOP approach

N.B. It is interesting to point out that the OPT methodology was implemented by JANSI to survey and evaluate the severe accident (SA) measures after the Fukushima accident. exercise allowed identifying provisions to be added to the current safety architecture.

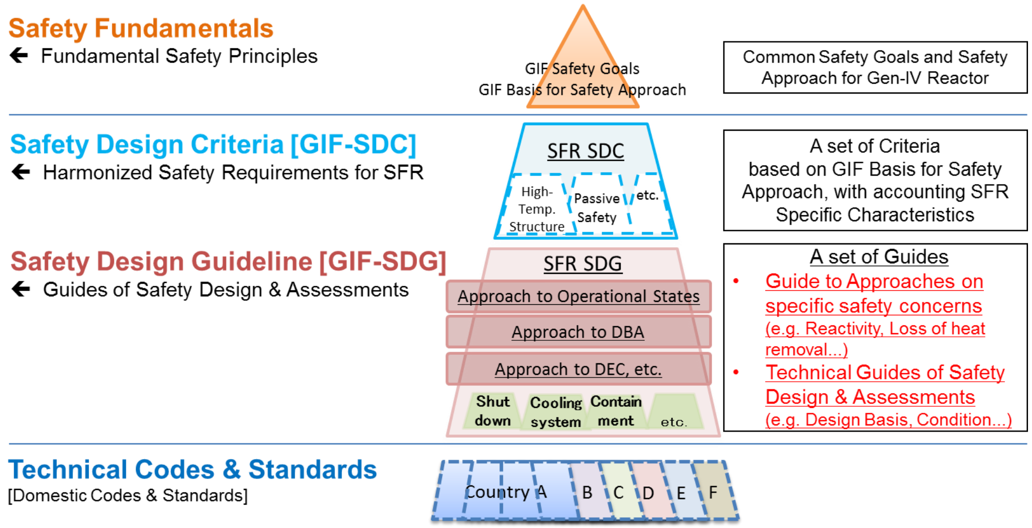
Probabilistic safety assessment - PSA

1. Deficiencies in PSA L1 & L2 for rare events and their combinations;
2. In addition to singular events, the scope of the PSA studies should cover their plausible combinations;
3. The evolution of the mode of analysis must be done in accordance with the risk Informed logic;
4. Sensitivity analyses to evaluate uncertainty and consolidate the robustness of the demonstration excluding any risk of cliff edge effect.
5. The need for extension of PSA studies at Level 3 to assess consequences of degraded situations on the environment limited in time and space.



• Safety Principles (to be followed – the fundamentals - or those simply recommended);
• Requirements (to be followed);
• Guidelines (recommended)
• Safety Goals (to be pursued)
• Safety Objectives (e.g. Farmer curve : consequences acceptance limits - to be achieved)
Safety Options (strategy for the selection and organization of provisions / solutions; identification of provisional provisions)
Decoupling criteria (which allow defining measurable safety margins)
Design & operational safety specifications applicable to the selected provisions (to allow guaranteeing safety margins)
Challenges (to the Safety Functions)
• Mechanisms (i.e. Initiating events which materialize the challenge)
• Mission (to be achieved for each initiating events, to allow guaranteeing safety margins)
Controlled Plant states (guaranteeing the safety of the installation)
• Nuclear Process (with its inherent characteristics)
• Safety Architecture (which allow guaranteeing the safety of the process and the installation)
Design and sizing of Provisions
Build up of the Safety Architecture
(i.e. for all the levels off the DiD)

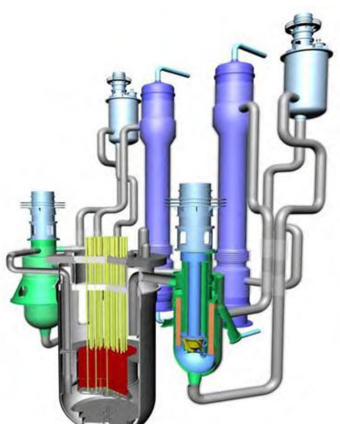
RSWG's support to SFR SDC-TF Activities



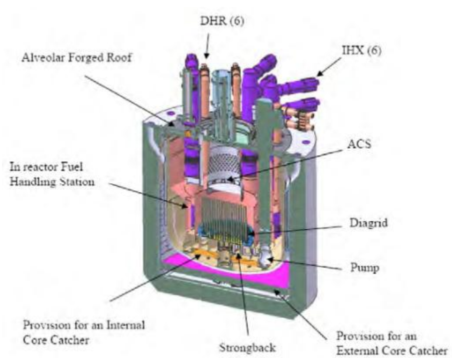
- *SDC "harmonization" is increasingly important for:*
  - ❑ *Realization of enhanced safety designs common to SFR systems,*
  - ❑ *Preparation for the forthcoming licensing in the near future*
  - ❑ *Because Gen-IV SFR are progressing into conceptual design stage*
- *RSWG's review will be from the technology neutral position.*

The SDC is the Reference criteria

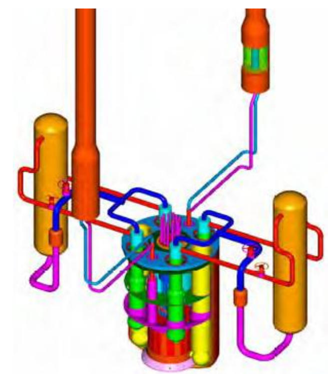
- *Of the designs of safety-related Structures, Systems & Components, that are specific to the SFR system,*
- *For clarifying the requisites systematically & comprehensively,*
- *When the developers apply the basic safety approach and use the codes & standards for conceptual design of the Gen-IV SFR system*



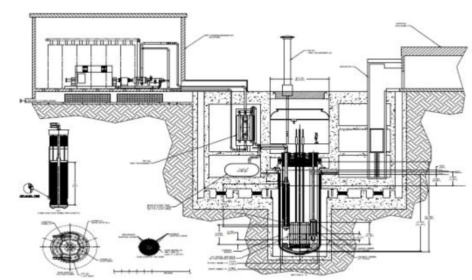
Large Loop



Large Pool



Intermediate-to-Large Loop



Small Modular

XXXXXXX

- ***xxxxx***