SAFETY OF GEN-IV REACTORS
Luca Ammirabile
EURATOM
19 February 2019
Meet the presenter

Luca AMMIRABILE works at the European Commission (EC), Joint Research Centre in Petten, the Netherlands, where he is Group Leader of the NUclear Reactor Accident Modelling (NURAM) team of the Nuclear Reactor Safety and Emergency Preparedness Unit. His current research activities are among the others core thermal-hydraulic analyses, deterministic code application and development, and safety assessment of advanced reactors.

Since 2014, he has been co-chair of the working group on Risk and Safety of the Generation IV International Forum. He is also EC representative of the OECD/NEA Working Group on the Analysis and Management of Accidents (WGAMA) and Working Group on the Safety of Advanced Reactors (WGSAR).

Prior to joining the European Commission in 2007, Luca worked at Tractebel Engineering (now Tractebel Engie) in Belgium in the Thermalhydraulics and Severe Accident Section, where he was engaged among other in the development of innovative methodologies in support of the safety assessment of the Belgian Nuclear Power Plants.

Luca received his doctorate from the Imperial College London in 2003 and his master’s degree in nuclear engineering from the University of Pisa, Italy in 1999.

Email: luca.ammirabile@ec.europa.eu
Outline

- GIF safety goals
- Risk and Safety Working Group
- Basis safety approach for Gen-IV reactors
- Integrated Safety Assessment Methodology (ISAM)
- ISAM application
Gen IV Goals

• 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.
Gas-cooled Fast Reactor (GFR)

Lead-cooled Fast Reactor (LFR)

Molten Salt Reactor (MSR)

Sodium-cooled Fast Reactor (SFR)

Supercritical-Water-cooled Reactor (ScWR)

Very-High-Temperature Reactor (VHTR)

Gen IV Systems
# Gen IV Systems

<table>
<thead>
<tr>
<th>System</th>
<th>Neutron Spectrum</th>
<th>Coolant</th>
<th>Pressure (MPa)</th>
<th>Temperature (°C)</th>
<th>Fuel Cycle</th>
<th>Size (MW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>GFR</td>
<td>Fast</td>
<td>Helium</td>
<td>~9</td>
<td>850</td>
<td>Closed</td>
<td>1200</td>
</tr>
<tr>
<td>LFR</td>
<td>Fast</td>
<td>Lead</td>
<td>~0.1+ (atm.)</td>
<td>480–800</td>
<td>Closed</td>
<td>45-1500</td>
</tr>
<tr>
<td>MSR</td>
<td>Fast or Thermal</td>
<td>Fluoride or chloride salts</td>
<td>~0.1+ (atm.)</td>
<td>700–800</td>
<td>Closed</td>
<td>1000-1500</td>
</tr>
<tr>
<td>SFR</td>
<td>Fast</td>
<td>Sodium</td>
<td>~0.1+ (atm.)</td>
<td>550</td>
<td>Closed</td>
<td>50–1500</td>
</tr>
<tr>
<td>ScWR</td>
<td>Thermal or fast</td>
<td>Water</td>
<td>~25</td>
<td>510–625</td>
<td>Once-through or Closed</td>
<td>10–over 1000</td>
</tr>
<tr>
<td>VHTR</td>
<td>Thermal</td>
<td>Helium</td>
<td>~5.5</td>
<td>900–1000</td>
<td>Once-through</td>
<td>250–300</td>
</tr>
</tbody>
</table>

- **Fast**
- **Thermal**
- **Water**
- **Liquid-Metal**
- **Molten-Salt**
- **Inert-Gas**
- **Atm.**
- **Hi-Pressure**
- **Mid. Temp.**
- **Hi-Temp.**
- **Small**
- **Mid.**
- **Large**
Risk and Safety Working Group

- “Promote a consistent approach on safety, risk, and regulatory issues between Generation IV systems”
- Propose safety principles, objectives, and attributes based on Gen-IV safety goals in order to guide safety related R&D plans
- Development and promotion of a technology-neutral Integrated Safety Assessment Methodology (ISAM)
Further improvements are possible through advanced technologies and the early application of a improved safety philosophy for a robust design so that safety is “built-in” rather than “added on”.

Design and safety assessment based on both deterministic and probabilistic approach, over wide-range of plant conditions including severe plant conditions.

Handling of internal and external hazards.

Modelling and simulation should play a large role in the design and the safety assessment.

- Full implementation of “defence in depth” in the design of Gen IV systems.
Excel in Operational Safety and Reliability
Safety during normal operation, anticipated operational events
→ DiD Level 1-2 [N.O., AOO]

Very low likelihood & degree of reactor core damage
Minimizing frequency of initiating internal events, and introducing design features for controlling & mitigating accidents to avoid core damage
→ DiD Level 2-3 [Design for severe accident prevention]

Eliminate the need for offsite emergency response
Comprehensive safety architecture to manage & mitigate severe plant conditions and reducing the likelihood of early or large releases of radiation
→ DiD Level 4 [Design for severe accident mitigation]
Defence-in-Depth

Defence in depth (DiD) is a fundamental principle of nuclear safety for preventing accidents and mitigating their consequences. The principle was introduced in the early 1970s, starting with three levels. Following the accidents at Three Mile Island and Chernobyl, two additional levels were added and the concept was formalised in 1996 in IAEA INSAG-10 with five levels.

<table>
<thead>
<tr>
<th>Levels</th>
<th>Objective</th>
<th>Essential means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Prevention of abnormal operation and failures</td>
<td>Conservative design and high quality in construction and operation</td>
</tr>
<tr>
<td>Level 2</td>
<td>Control of abnormal operation and detection of failures</td>
<td>Control, limiting and protection systems and other surveillance features</td>
</tr>
<tr>
<td>Level 3</td>
<td>Control of accidents within the design basis</td>
<td>Engineered safety features and accident procedures</td>
</tr>
<tr>
<td>Level 4</td>
<td>Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents</td>
<td>Complementary measures and accident management</td>
</tr>
<tr>
<td>Level 5</td>
<td>Mitigation of radiological consequences of significant releases of radioactive materials</td>
<td>Off-site emergency response</td>
</tr>
</tbody>
</table>
Defence-in-Depth

- **Exhaustive**: Identification of the risks, which leans on the fundamental safety functions, should be comprehensive.
- **Progressive**: Accident scenarios should entail the progressive failure of each DiD level without “short” sequences leading directly from level 1 to level 4.
- **Tolerant**: Small deviation of the physical parameters outside their expected range should not lead to severe consequences (i.e. no “cliff edges”).
- **Forgiving**: Assure sufficient grace period for possibility of manual intervention and repair during accidental situations.
- **Balanced**: A specific accident sequence should not contribute to the global frequency of the damaged plant states in an excessive and unbalanced manner.
The design for Gen IV energy systems should cover the full range of plant states including severe conditions.

Special attention to reinforced treatment of severe plant conditions through provisions of measures against such conditions.

Internal-events and internal/external-hazards should be considered.

Uncertainties related to innovative technologies should be factored in.

Specific efforts, both analytical and empirical, should be made for demonstrating the “practical elimination” of sequences associated with the potential for early or large releases.
### Plant States

#### Defense-in-Depth Levels

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational states</td>
<td>Accident conditions</td>
<td>EP&amp;R</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Normal Operation</th>
<th>Anticipated Operational Occurrences</th>
<th>Design Basis Accidents</th>
<th>Design Extension Conditions</th>
<th>Residual risk and practically eliminated accidents</th>
</tr>
</thead>
</table>

#### Plant states considered in design
(safety analyses)

#### Out of the design
(addressed in level-5 of DiD)
Pre-Conceptual Design  
Conceptual Design  
Final Design  
Licensing and Operation

Primarily Qualitative  
Formulation → Refinement of Safety Requirements and Criteria  
Primarily Quantitative

Qualitative Safety Requirements/Characteristic Review (QSR)

PIRT
- Identify important phenomena
- Characterize state of knowledge

OPT
- List provisions that assure implementation of DID
- DID level → safety function → challenge/mechanism → provisions

Probabilistic Safety Assessment (PSA)
- Provides integrated understanding of risk and safety issues
- Allows assessment of risk implications of design variations
- In principle, allows comparison to technology neutral risk metrics

Deterministic and Phenomenological Analysis (DPA)
- Demonstrate conformance with design intent and assumptions
- Characterize response in event sequences resulting from postulated initiating events
- Establish margins to limits, success criteria for SSCs in PRA, and consequences

Integrated Safety Assessment Methodology

14
ISAM Toolkit

- **Qualitative Safety-characteristics Review (QSR)**
  - A “check-list” as systematic and qualitative means of ensuring that the design incorporates desired safety attributes (preparatory step)

- **Phenomena Identification and Ranking Table (PIRT)**
  - Generates ranked tables for identifying system and component vulnerabilities, and relative contributions to safety and risk
  - Also helps to identify the gaps in knowledge base that require additional research and data for V&V

- **Objective Provision Tree (OPT)**
  - A tool for identifying the provisions for prevention, or control and mitigation, of accidents that could potentially damage the reactor
  - Complimentary to PIRT for selecting the "lines of protection" against the identified phenomena
<table>
<thead>
<tr>
<th>Qualitative assessment</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>X</td>
</tr>
<tr>
<td>N</td>
<td></td>
</tr>
<tr>
<td>U</td>
<td></td>
</tr>
</tbody>
</table>

**1. 1st level: PREVENTION: Prevention of abnormal operation and failures**

1.1. Work out and set up a simple design for the operation and safety behaviour and safety behaviour

1.1.1. Work out and set up a simple neutronic design

1.1.2. Work out and set up a simple thermo hydraulic design

1.1.2.1. **Simplify the thermo hydraulic for the normal operating conditions (heat removal at nominal operating conditions and during nominal operational transients)**

   X  The thermo hydraulic behaviour of the primary circuit will be more complex due to the needed specific EMP regulation to guarantee the stable stratification within the internal volume of the REDAN

1.1.2.2. **Simplify the thermo hydraulic for the normal DHR**

   X  As for the EFR. The DHR loop through the IHX is quite conventional.

1.1.2.3. **Simplify the thermo hydraulic for the safety DHR**

   X  The hydraulic loop to establish and maintain the natural convection is significantly simplified

1.1.2.4. **Separate the normal operating DHR function from the safety DHR**

   X  As for the EFR

1.1.2.5. **Increase the range covered by the functionally redundant DHR systems (forced convection > natural convection)**

   X  The overlapping between normal heat removal (forced convection through the IHX and DRACS) and the heat removal during abnormal conditions (natural convection) is achieved gradually and without sharp modifications of the hydraulic path.

1.1.2.6. **Minimize the number of components per system**

   X  Significant number of EMPs installed on the IHX
ISAM Toolkit

- **Qualitative Safety-characteristics Review (QSR)**
  - A “check-list” as systematic and qualitative means of ensuring that the design incorporates desired safety attributes (preparatory step)

- **Phenomena Identification and Ranking Table (PIRT)**
  - Generates ranked tables for identifying system and component vulnerabilities, and relative contributions to safety and risk
  - Also helps to identify the gaps in knowledge base that require additional research and data for V&V

- **Objective Provision Tree (OPT)**
  - A tool for identifying the provisions for prevention, or control and mitigation, of accidents that could potentially damage the reactor
  - Complimentary to PIRT for selecting the “lines of protection” against the identified phenomena
### Knowledge Level [KL]
### Importance Ranking [IR]

<table>
<thead>
<tr>
<th>System</th>
<th>Component</th>
<th>Phenomena/Characteristics/State variables</th>
<th>R</th>
<th>KL₁</th>
<th>KL₂</th>
</tr>
</thead>
<tbody>
<tr>
<td>BRSS</td>
<td>SASS</td>
<td>SASS actuation temperature</td>
<td>H</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Coolant transport delay time from core outlet to around SASS</td>
<td>H</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Time constant of temperature response delay from coolant around SASS to SASS device</td>
<td>M</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Upper core region</td>
<td>around SASS</td>
<td>Core outlet temperature of the coolant that flows to around SASS</td>
<td>H</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Doppler reactivity</td>
<td>M</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fuel temperature/reactivity</td>
<td>L</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Reactor</td>
<td>Reactor core</td>
<td>Fuel cladding temperature reactivity</td>
<td>M</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Coolant temperature reactivity</td>
<td>H</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Coolant flow rate halving time</td>
<td>H</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Power distribution</td>
<td>M</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Flow rate distribution among core assemblies</td>
<td>M</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Coolant temperature at the core inlet and outlet</td>
<td>L</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fuel pin gap heat transfer coefficient</td>
<td>M</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fuel pellet thermal conductivity</td>
<td>L</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Thermal material property of fuel cladding and coolant</td>
<td>L</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>RPCS</td>
<td>Temperature &amp;C</td>
<td>Coolant temperature to be used reactor power control</td>
<td>M</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Pump</td>
<td>Pump rotating inertia</td>
<td>M</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Pressure loss in the reactor and PHTS</td>
<td>M</td>
<td>4</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

### Knowledge Base Gap Determination

<table>
<thead>
<tr>
<th>Adequacy of knowledge</th>
<th>Rank of Phenomenon</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>GAP</td>
</tr>
<tr>
<td>M</td>
<td>GAP</td>
</tr>
<tr>
<td>L</td>
<td>GAP</td>
</tr>
<tr>
<td>I</td>
<td>GAP</td>
</tr>
</tbody>
</table>

- **(4) Fully known; small uncertainty**
- **(3) Known; moderate uncertainty**
- **(2) Partially known; large uncertainty**
- **(1) Very limited knowledge; uncertainty cannot be characterized**
Qualitative Safety-characteristics Review (QSR)

- A “check-list” as systematic and qualitative means of ensuring that the design incorporates desired safety attributes (preparatory step)

Phenomena Identification and Ranking Table (PIRT)

- Generates ranked tables for identifying system and component vulnerabilities, and relative contributions to safety and risk
- Also helps to identify the gaps in knowledge base that require additional research and data for V&V

Objective Provision Tree (OPT)

- A tool for identifying the provisions for prevention, or control and mitigation, of accidents that could potentially damage the reactor
- Complimentary to PIRT for selecting the “lines of protection” against the identified phenomena
• **Deterministic and Phenomenological Analyses (DPA)**
  - Traditional safety analyses to assess the system’s response to known safety challenges and guide concept/design development
  - Involves the use of conventional safety analysis codes and provides input to PSA

• **Probabilistic Safety Analysis (PSA)**
  - Assures a broader coverage of the accident space
  - Performed and iterated, beginning in the late pre-conceptual design phase, and continuing through the final design stages
  - A structured means of providing answers to three basic questions:
    • What can go wrong?
    • How likely is it?
    • What are the consequences?
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)

Safety Principles
Safety Requirements
Safety Guidelines

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 of the DiD)

QSR

Safety Options
(strategy for the selection and organization of provisions/solutions)

PIRT
OPT
DPA
&
PSA

Cf. Next figure for details

Imposed from outside the process

Selected by the Designer following the DPA strategy
<table>
<thead>
<tr>
<th>Regulatory Framework (Goals, objectives, principles, requirements, guidelines)</th>
<th>✓</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selection of Safety Options and provisional Provisions</td>
<td>✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>1. Compliance / consistency of the design options with the principles, requirements and guidelines</td>
<td>✓</td>
</tr>
<tr>
<td>2. Identification, prioritization and correction (if feasible) of discrepancies</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>3. Identification of challenges to the safety functions</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>4. Identification of mechanisms (initiating events) and selection of significant (envelope) plants conditions to be considered for the design basis</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>5. Identification and selection of needed provisions</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>6. Design and sizing of the provisions</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>7. Response to transients (safety analysis)</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>8. Final assessment for a safety architecture that should be:</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>o Exhaustive</td>
<td>✓</td>
</tr>
<tr>
<td>o Progressive</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>o Tolerant</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>o Forgiving</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>o Balanced</td>
<td>✓</td>
</tr>
<tr>
<td>QSR</td>
<td>PIRT</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
</tr>
<tr>
<td>Regulatory Framework (Goals, objectives, principles, requirements, guidelines)</td>
<td>✔</td>
</tr>
<tr>
<td>Selection of Safety Options and provisional Provisions</td>
<td>✔</td>
</tr>
<tr>
<td>1. Compliance / consistency of the design options with the principles, requirements and guidelines</td>
<td>✔</td>
</tr>
<tr>
<td>2. Identification, prioritization and correction (if feasible) of discrepancies</td>
<td>✔</td>
</tr>
<tr>
<td>3. Identification of challenges to the safety functions,</td>
<td>✔</td>
</tr>
<tr>
<td>4. Identification of mechanisms (initiating events) and selection of significant (envelope) plants conditions to be considered for the design basis,</td>
<td>✔</td>
</tr>
<tr>
<td>5. Identification and selection of needed provisions,</td>
<td>✔</td>
</tr>
<tr>
<td>6. Design and sizing of the provisions,</td>
<td>✔</td>
</tr>
<tr>
<td>7. Response to transients (safety analysis),</td>
<td>✔</td>
</tr>
<tr>
<td>8. Final assessment for a safety architecture that should be:</td>
<td></td>
</tr>
<tr>
<td>o Exhaustive,</td>
<td>✔</td>
</tr>
<tr>
<td>o Progressive,</td>
<td>✔</td>
</tr>
<tr>
<td>o Tolerant,</td>
<td></td>
</tr>
<tr>
<td>o Forgiving,</td>
<td></td>
</tr>
<tr>
<td>o Balanced.</td>
<td></td>
</tr>
<tr>
<td>Regulatory Framework (Goals, objectives, principles, requirements, guidelines)</td>
<td>QSR</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Selection of Safety Options and provisional Provisions</td>
<td>✓</td>
</tr>
<tr>
<td>1. Compliance / consistency of the design options with the principles, requirements and guidelines</td>
<td>✓</td>
</tr>
<tr>
<td>2. Identification, prioritization and correction (if feasible) of discrepancies</td>
<td>✓</td>
</tr>
<tr>
<td>3. Identification of challenges to the safety functions,</td>
<td>✓</td>
</tr>
<tr>
<td>4. Identification of mechanisms (initiating events) and selection of significant (envelope) plants conditions to be considered for the design basis,</td>
<td>✓</td>
</tr>
<tr>
<td>5. Identification and selection of needed provisions,</td>
<td>✓</td>
</tr>
<tr>
<td>6. Design and sizing of the provisions,</td>
<td>✓</td>
</tr>
<tr>
<td>7. Response to transients (safety analysis),</td>
<td>✓</td>
</tr>
<tr>
<td>8. Final assessment for a safety architecture that should be:</td>
<td>✓</td>
</tr>
<tr>
<td>o Exhaustive,</td>
<td>✓</td>
</tr>
<tr>
<td>o Progressive,</td>
<td>✓</td>
</tr>
<tr>
<td>o Tolerant,</td>
<td>✓</td>
</tr>
<tr>
<td>o Forgiving,</td>
<td>✓</td>
</tr>
<tr>
<td>o Balanced.</td>
<td>✓</td>
</tr>
<tr>
<td>QSR</td>
<td>PIRT</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
</tr>
<tr>
<td>Regulatory Framework (Goals, objectives, principles, requirements, guidelines)</td>
<td>✓</td>
</tr>
<tr>
<td>Selection of Safety Options and provisional Provisions</td>
<td>✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>1. Compliance / consistency of the design options with the principles, requirements and guidelines</td>
<td>✓</td>
</tr>
<tr>
<td>2. Identification, prioritization and correction (if feasible) of discrepancies,</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>3. Identification of challenges to the safety functions,</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>4. Identification of mechanisms (initiating events) and selection of significant (envelope) plants conditions to be considered for the design basis,</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>5. Identification and selection of needed provisions,</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>6. Design and sizing of the provisions,</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>7. Response to transients (safety analysis),</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>8. Final assessment for a safety architecture that should be:</td>
<td></td>
</tr>
<tr>
<td>o Exhaustive,</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>o Progressive,</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>o Tolerant,</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>o Forgiving,</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>o Balanced.</td>
<td>✓ ✓</td>
</tr>
</tbody>
</table>

Design & operational safety specifications applicable to the selected provisions (to allow guaranteeing safety margins)
### Regulatory Framework (Goals, objectives, principles, requirements, guidelines)

<table>
<thead>
<tr>
<th>QSR</th>
<th>PIRT</th>
<th>OPT</th>
<th>DPA</th>
<th>PSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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 of ISAM use

Decay Heat Removal System of JSFR: 2 PRACS and 1 DRACS, each 100% heat removal capacity, with Final heat sink of Air

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

Objective and Barriers

Safety function (SF)

Challenge

Mechanism

Provisions

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path

Level 3

Control of accidents within the design basis

Core heat removal

Acceptance criteria: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sinks, ensuring core geometry, and reactor vessel integrity

Degraded or disruption of heat transfer path
✓ Scenarios analyzed by DPA was "identified by PSA", in advance of DPA
✓ PSA, based on event tree model, gives “Success” or “failure within 24hours”

<table>
<thead>
<tr>
<th>Loss of circulation capability in PRACS-B</th>
<th>Reactor SCRAM</th>
<th>Passive cooling by using PRACS-A</th>
<th>Passive cooling by using DRACS</th>
<th>Seq. No.</th>
<th>Accident sequence</th>
<th>Core integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC07-B</td>
<td>RS</td>
<td>ANC</td>
<td>DNC</td>
<td></td>
<td>RS*/ANC*/DNC</td>
<td>Should be OK (1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>(Successful DBA scenario)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RS*/ANC* DNC</td>
<td>Unknown (1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>(Passive cooling by using PRACS-A alone)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RS*/ANC* DNC</td>
<td>Unknown (1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>(Passive cooling by using DRACS alone)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RS<em>ANC</em>DNC</td>
<td>Damage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>(Loss of all heat sink)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(1) Need to be confirmed by DPA

*PLOHS: Protected Loss Of Heat Sink. Insufficient heat removal capacity event included.
DPA of Sequence No.1 (identified by PSA)

The DPA results are “input (returned) to “PSA”;

<table>
<thead>
<tr>
<th>Loss of circulation capability in PRACS-B</th>
<th>Reactor SCRAM</th>
<th>Passive cooling by using PRACS-A</th>
<th>Passive cooling by using DRACS</th>
<th>Seq. No.</th>
<th>Accident sequence</th>
<th>Core integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC07-B</td>
<td>RS</td>
<td>ANC</td>
<td>DNC</td>
<td></td>
<td></td>
<td>OK(1)</td>
</tr>
</tbody>
</table>

Success ↑

- 1/RS*/ANC*/DNC (Successful DBA scenario)
- 2/RS*/ANC*/DNC (Passive cooling by using PRACS-A alone)
- 3/RS*ANC*/DNC (Passive cooling by using DRACS alone)

Failure ↓

This sequence is developed in detail in other event trees

- 4/RS*ANC*/DNC (Loss of all heat sink)
- 5- (Loss of all coolant)

- Damaged(2)
- Damage
PLOHS-S: PLOHS sequences that occurs within 24 hours after reactor shutdown

PLOHS-L: PLOHS sequences that occurs after successful decay heat removal during 24 hours and within the mission time of 1 month

- Option for risk reduction
  Enhance heat removal capacity of a single train of DHRS within 24 hours

PSA result
Initial design
Initial design

PLOHS-L 1%

PLOHS 5x10^{-7}/ry

PLOHS-S 99%

Improved design

1/50!!

PLOHS 9x10^{-9}/ry

Non-safety-related air-cooler blowers

Steam Generator

Feedwater

SHTS

PHTS

SHTS

Additional success path

Accident sequence

Core

integrity

AICN/DNC (Successful DBA scenario) OK

AICN/DNC/AFC (Forced air flow cooling by using PRACS-A alone) OK

AICN/DNC/AFC (Passive cooling by using PRACS-A alone) Damage

AICN/DNC/AFC (Forced air flow cooling by using DRACS alone) Damage

AICN/DNC/AFC (Passive cooling by using DRACS alone) Damage

AICN/DNC (Loss of all heat sink) Damage
• RSWG aims to enhance safety through advanced technologies and the early application of a improved safety philosophy
• Full, systematic implementation of defence-in-depth (safety should be built-in, not added-on)
• No new tools but a systematic methodology for a robust demonstration
• ISAM to support safety assessments
Ongoing RSWG activities

• Update Basis of Safety Approach for Gen-IV systems

• RSWG reports (with contributions from SSCs) to date:

  • White Papers on pilot application of ISAM
    • Demonstrate applicability of ISAM as a self-assessment for each of the six Gen-IV systems
    • Provide guidance on improving safety features based on the ISAM approach
  
  • Safety Assessment Reports for six Gen-IV systems
    • Snapshot of high-level safety design attributes, challenges and remaining R&D needs
  
  • Contributions to SFR, LFR, GFR, SCWR and VHTR safety design criteria

Upcoming webinars

20 March 2019  The Allegro Experimental Gas Cooled Fast Reactor Project  Dr. Ladislav Belovsky, UJV Rez, A.s., Czech Republic

15 April 2019  European Sodium Fast Reactor: An Introduction  Dr. Konstantin Mikityuk, PSI, Switzerland

22 May 2019  Formulation of alternative cement matrix for solidification/stabilization of nuclear waste  Mr. Matthieu de Campos, CEA, France