European project SARGEN_IV: safety approach and assessment of GEN IV reactors

L. Ammirabile on behalf of the SARGEN_IV Consortium
JRC-IET Institute for Energy and Transport
Petten - The Netherlands

http://ie.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/
The SARGEN_IV project: objectives and structure

Safety approach and assessment

1. Scope
2. Safety objectives
3. Principles
4. Safety assessment
   a) Deterministic safety assessment
   b) Probabilistic safety assessment
   c) Fukushima accident insights
5. Conclusions
SARGEN_IV brings together the main European stakeholders to propose a European framework for the safety assessment for the future innovative reactors:

Objectives:

1. Identification and categorization of the critical safety features associated with four concepts (SFR, LFR, GFR, FASTEF)
2. Review of the available safety methodologies followed by a proposal for harmonization of the safety assessment practices for innovative reactors
3. Pilot application of the proposed methodology
4. Development of an European roadmap for the fast reactors safety R&D
<table>
<thead>
<tr>
<th>WP No.</th>
<th>Work Package Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SARGEN_IV management</td>
</tr>
<tr>
<td>2</td>
<td>Identification of critical safety features for technical terms of reference</td>
</tr>
<tr>
<td>3</td>
<td>Review of safety methodologies for innovative reactors</td>
</tr>
<tr>
<td>4</td>
<td>Pilot application of the European methodology in WP3</td>
</tr>
<tr>
<td>5</td>
<td>Development of a European roadmap for fast reactor safety R&amp;D</td>
</tr>
<tr>
<td>6</td>
<td>Dissemination and Communication</td>
</tr>
</tbody>
</table>
Proposal for an harmonization of the safety assessment practices
With consistency with most of approaches, the framework of assessment to perform should include:

- **The entire plant**: reactor and fresh/spent fuel storage, waste management..., including situations that affect different parts of the plant,
- **All plant states and conditions**,
- Maintenance and in-service inspections,
- All plant **life time**:
  - From commissioning to decommissioning: design should include **decommissioning provisions**,
  - Ageing,
- Protection of workers, environment including public,
- Technical and human/organisational aspects, natural phenomena,
- Safety and security/safeguard aspects.
Chemical effects could be a **challenging issue** with regards of the current expected designs of GEN IV reactors

WENRA → **non-radiological impact should be also reduced**, but this goal is not mentioned as a safety objective

→ It is proposed to take into account chemical risks **with a graded approach** on 3 aspects:

- Establishment of PIE and/or Screening of hazards
  - NOTA: particular attention to corrosion or any interaction between different materials. Both deterministic and probabilistic approach,

- The potential impact on the public, environment and workers should be assessed: compared to radiological impact, a different approach could be developed:
  - Definition of **objectives**,  
  - **Barriers** approach, definition of **fundamental functions** (confinement for instance),

- Design choices that are made according to chemical risks analysis should be **consistent** with safety design choices.
Safety objectives are ambitious with the general aim to reduce potential radiological consequences and impact on public, workers and environment as well as to reduce the occurrence/frequency of failures, incidental and accidental situations.

Some safety objectives:

- Ensuring effective management for safety from the design stage (mostly organizational and human factors)
- Effectiveness of the independence between all levels of defence-in-depth,
- Plant design should take into account provisions to avoid or to delay cliff-edge effects in case of extreme situations that ENSREG stress test deal with,
- Safety and security measures are designed and implemented in an integrated manner.
- Limited potential chemical impact on the public
• Radiological consequences of abnormal events do not exceed radiological consequences of normal operation,
• No off-site radiological impact or only minor radiological impact for accidents without severe core damage
• Reducing potential radioactive releases to the environment from accidents with severe core damage, also in the long term, by following the qualitative criteria below:
  ▪ accidents with severe core damage which would lead to early or large releases have to be practically eliminated,
  ▪ for the other ones:
    • Ensuring that there should be no need for offsite measures in case of severe core damage accident,
    • In case of no fully achievement, it should be justified by designer and design provisions have to be taken so that only limited protective measures in area and time are needed for the public (no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in food consumption) and that sufficient time is available to implement these measures,
Defense-In-Depth (DiD) remains a fundamental principle.

An overall reinforcement of DiD is expected for GEN-IV NPP, including

**Independency**: Enhancing the effectiveness of the independence between all levels of DiD is a safety objective

**Hazards**: A special attention is paid to hazards that could potentially **impair several levels of defense**

DiD is structured in **levels**. Thus, the strategy of DiD is **twofold**:

- To **prevent escalation from one level to an upper one**, so to define provisions against challenging of levels of DiD,
- To **consider that a level could fail**, despite its prevention provisions.
IAEA SSR-2/1: A “relevant aspect of the implementation of DiD for a NPP is”:

- 
  provision in the design of a series of physical barriers,
- 
  combination of safety features that contribute to the effectiveness of them.

The design shall prevent, as far as is practicable:

- 
  challenges to the integrity of physical barriers,
- 
  failure of one or more barriers,
- 
  failure of a barrier as a consequence of the failure of another barrier.”

Barriers principle:

- 
  There should be identified barriers between radiological material and the environment, whose integrity should be maintained as far as reasonably practicable,
- 
  the barriers number and effectiveness should be justified, notably to ensure the achievement of safety objectives at each level of DiD,
- 
  failure of one barrier should not jeopardize the integrity of another one.
IAEA SSR-2/1:
- Control of reactivity,
- Removal of heat from the reactor and from the fuel store,
- Confinement of radioactive material,

This list should be improved if necessary by taking into account some specificities (chemical confinement?)

**Diversification**: Fulfillment of fundamental safety functions should be sought by diverse means.

**Inherent** characteristics:
- Expected according to Finnish approach for EPR or French approach for GEN III reactors, mentioned by IAEA SSR-2/1 and GIF

Inherent approach reinforces the fulfilment of FSF by delaying the need of some safety features or limiting their number. Such an approach is notably fully consistent with:
- The objective of reducing the potential for escalation to accident situations by enhancing plant capability to control abnormal events,
- The insights of Fukushima NPP accident, which underlines the importance of a sufficient grace period.
According to the objectives, each situation with severe core damage which could lead to large or early releases should be identified and be practically eliminated:

- **Primarily**, it should be demonstrated that, due to the basic design, the situation is **physically impossible**,
- **Otherwise**, provisions should be taken to ensure that or the conditions can be considered with a high degree of confidence to be **extremely unlikely to arise**.

Practical elimination should be:

- **Primarily based on deterministic** arguments and confirmed by a probabilistic assessment. The relative weight of the previous elements has to be adapted to each situation. The demonstration should rely on the **implementation of several successive and diversified provisions**
- **Applied to a limited number of situations**.
ALARA/ALARP principle

Built-in rather than added-on

Complementary and integrated approach that combines both deterministic and probabilistic.
IAEA NS-G-1.2 – Safety Assessment

“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:

- Verification of the compliance of the system with the principles, the requirements, the guidelines defined by the regulator as well as with the safety goals and objectives developed by the designer;

- Verification of the conformity of the safety architecture of the system with the quantitative safety objectives, translated into physical parameters or “decoupling criteria”.
Set principles, requirements, guidelines
  Safety goals, objectives
  Regulatory and safety approach

(b) Identify design options and decoupling criteria

(c) Ensure design compliance with principles, requirements, guidelines
   Yes
   No

(d) Identify the challenges to the safety functions and their mechanisms (PIE)
   Yes
   No

(e) Establish the System Provisions

(f) Design of System Provisions

(h) New design options necessary
   Yes
   No

QSR-INPRO

OPT [MLD]

LICENSING PHASE

DPA    PSA

Check conformity of the safety architecture
1. Exhaustive
2. Progressive
3. Tolerant
4. Forgiving
5. Balanced

[All DiD levels fulfilled]

Joint Research Centre
SSR-2/1 requirement: “The design for the nuclear power plant shall apply a systematic approach to identifying a comprehensive set of postulated initiating events ...”

The entire scope of assessment should be considered to identify the PIE

In SARGEN_IV WP2 critical safety features were identified and categorized:

**Common phenomena:**
- Materials (fuel, coolant, structure, absorber)
- Aspects specific to fast reactors
- Aspects specific to design solutions envisaged for ESNII concepts, and

**Possible impact on the fulfillment of fundamental safety functions:**
- Control of reactivity
- Removal of heat
- Confinement of radioactive materials
Need of PIE classification consistent with the DiD in order to perform deterministic safety assessment:

- According to the estimated frequencies of the groups of initiating events they cover
- Complement this approach with engineering judgement, insights of PSA or operating experience.

Specific rules and acceptance criteria are affected to each PIE class.

**Design Basis Conditions 1 (DBC 1):** normal situations including different transients necessary to operate the plant.

**Design Basis Conditions 2 (DBC 2):** could occur several times in plant life time.

**Design Basis Conditions 3 (DBC 3):** Events not expected to occur during plant life time. Return to power with inspection, rectification and checking.

**Design Basis Conditions 4 (DBC 4):** Events not expected to occur during plant life time. Plant restart is not expected

**Design Extension Conditions 1 (DEC 1):** Events not expected to occur during plant life time, correspond to complex sequences not considered in DBC.

**Design Extension Conditions 2 (DEC 2) – Severe Core Damage:** Events relevant to DEC 2 are those with severe core damage that are not practically eliminated.
Some rules and acceptance criteria:

- The combination with a single aggravating failure is considered,
- The combination with a loss of off site power (LOOP) at the most penalizing time is considered,
- Operator actions in acceptable environment and with a sufficient grace period,
- Unavailability due to this maintenance should be considered (if foreseen),
- Classified Equipment
- Conservative/Realistic calculations
- Radiological consequences
- The integrity of barriers
- Fuel damage
- Loss of safety equipment

Acceptance criteria common to all DBC and DEC:

- A postulating initiating event should **not propagate to a more serious one**:
  - Another PIE with more serious consequences,
  - Another PIE of a higher category
- If a PIE triggers an emergency shutdown, the core should remain subcritical during the entire scenario.
A hazard can be defined as an **event** with the potential to cause **adverse conditions or damage** to equipment necessary for safety, challenging the fulfilment of fundamental safety functions.

- **Internal hazards**: events originated in the plant that could affect a part of the plant not involved in this event.
- **External hazards**: natural or man-induced events originated outside the plant. For multiple unit plant sites, hazards could be originated by another unit.

Safety process of hazards evaluation could be divided in **three main steps**:

- **Identification of hazards** and screening of those that are relevant to the design or the site. (chemical hazard)
- **Determination of hazards parameters**, 
  - should be characterised in terms of their severity and/or magnitude and duration.
- **Analysis**
  - Hazards assessment as **PIE**: PIE -> category -> acceptance criteria
  - Deterministic approach: Hazard -> loading to design systems
  - PSA
**Classification** of SSC also required by IAEA SSR-2/1

The method for classification: based primarily on deterministic methodologies complemented by probabilistic methods, with account taken of factors such as:

- The function(s) to be performed by the item. Thus the role with regards to fundamental safety functions, barriers, PIE (including hazards) and practical elimination should be considered,
- The consequences of failure to perform the function(s). Thus, an item considered in practical elimination of a situation should be classified at the highest level. Moreover, supporting SSC should be considered in classification,
- The frequency at which the item will be called upon to perform a safety function,
- The time following a PIE at which, or the period for which, the item will be called upon to perform.

The design should be such as to ensure that any interference between items important to safety should be prevented (example: any failure of items important to safety in a system in a lower class will not propagate to a system in a higher safety class).
DSA/PSA combined approach will provide assurance:

- the nuclear power plant as designed is capable of meeting acceptable limits for accident conditions
- provide assurance that a robust defence in depth has been implemented.

- **exhaustive**: the identification of the risks should look for exhaustiveness.

- **progressive**: to avoid “short” sequences for which, downstream from the initiator, the failure of a particular provision entails a major increase, in terms of consequences, without any possibility of restoring safe conditions at an intermediate stage.

- **tolerant**: no small deviation of the physical parameters from an initial situation, outside the expected ranges, can lead to a more serious situation (i.e. rejection of “cliff edge effects”).

- **forgiving**: which guarantee the availability of a sufficient grace period and the possibility of repair during accidental situations.

- **balanced**: no sequence participates in an excessive and unbalanced manner to the global frequency of the damaged plant states.
DSA/PSA should provide:

confirmation that operational limits and conditions are in compliance with the assumptions and intent of the design for normal operation of the plant (Level 1 DiD);

analysis and evaluation of event sequences that result from PIEs, comparison of the results of the analysis with radiological acceptance criteria and design limits and confirmation of the design basis (Level 2 to 4(5) DiD);

demonstration that the management of anticipated operational occurrences and design basis accidents and severe plant conditions is possible by automatic response of safety systems in combination with prescribed actions of the operator (progressive and forgiving DiD).

to demonstrate that a balanced design has been achieved (balanced DiD);

to provide confidence that ‘cliff edge effects’ will be prevented (tolerant DiD);

the required reliability of SSCs, tests, inspections, surveillance and maintenance requirement to assure that the acceptance criteria for each level of DiD and the safety goal are met.

establish the conservative assumptions that shall be adopted where there may be insufficient data to allow best estimate methods to be used to assure that the acceptance criteria for each level of defence in depth and the safety goal are met.
Based on ENSREG specifications (May 2011) and conclusions (April 2012)

**Proposal → Performance of a complementary assessment:**
- Based on deterministic approach, irrespective of the probability of the loss of line of defence,
- Consider a sequential loss of the lines of defence and a long duration of events,
- Take into account the entire affected plant (reactor, fuel storage),

The objective is to identify weak points and cliff-edge effects, for each of the following extreme situations.

**Extreme situations to be considered:**
- Extreme earthquake, flooding (consequential or linked event should be considered (fire, load drop for earthquake, bad weather conditions for flooding…)),
- Total loss of power sources, total loss of ultimate heat sink, combination of both,
- Severe accident, notably in case of the two previous situations.

**Identification of:**
- Weak points, cliff-edge effects. A particular attention should be paid to confinement failure risk,
- Provisions to cope with them, notably to improve the grace period before cliff-edge effects.

These provisions should be considered as hardened equipments.
• SARGEN_IV has elaborated a proposal for the harmonization of safety assessment practices for GEN IV NPP.

• An overall reinforcement of DiD is expected for GEN_IV NPP, including improved independence between all levels of DiD.

• An inherent approach should reinforce the fulfillment of fundamental safety functions e.g. the consequences for some situations should be reduced and the grace periods should be extended. For the same reason, the use of passive systems can be envisaged.

• The need of complementary and integrated deterministic and probabilistic approaches is reiterated.

• Methodologies: Some of them are not yet applied.

• Assessment of hazards would be a challenging aspect of next generation of NPP safety assessment and should be improved, which is confirmed by the first insights of Fukushima Daiichi TEPCO reactors accidents.

• Provisions to cope with extreme events notably to improve the grace period before cliff-edge effects and thus allowing back-up measures to be implemented have to be defined and should be considered as hardened equipments.
THANK YOU