# Applicability of PSA Level 2 in the Design of Nuclear Power Plants

**Estelle C. SAUVAGE[a], Gerben DIRKSEN[b], and Thierry COYE de BRUNELLIS[c]**
[a] AREVA-NP SAS, Paris, France
[b] AREVA-NP Gmbh, Erlangen, Germany
[c] AREVA-NP SAS, Lyon, France

**Abstract:**

In the nuclear industry, until recently, the licensing and design of the new Nuclear Power Plants (NPP) were based upon a deterministic approach. The Probabilistic Safety Assessments (PSA) only supported the safety demonstration, mostly by the evaluation of the risks for the population and the environment. The feedbacks in the design of the NPP, when existing, were limited.

Nowadays the use of the PSA becomes more systematic and is extended to the design phase of the new generation of NPP. In this frame the first approach was to develop the concepts of risk based and risk informed decision making to avoid unnecessary burden taking place in the NPP design due to the strong deterministic prescription on low probability events.

Following the development of a new generation of plants, such as the AP1000 or the EPR, which considers the severe accidents in their design, the PSA Level 2 tends to contribute more and more to build the new NPPs. The accident of Fukushima Daishi NPPs even leads to an extended consideration of the severe accident in the design of the nuclear plants and the emergency organization structures.

The interaction between the PSA Level 2 development and the design phase of the NPP became obvious, and part of the safety standards as recommended by the safety authorities and organizations.

This paper assesses how the PSA Level 2 becomes a high visibility topic of the design phase of the NPP. The current safety requirement expectations regarding the use of the PSA Level 2 in the design phase results from this evolution.

Indeed several technical areas can use the insight of a PSA Level 2 to improve the NPP design. It includes the design of hardware and systems (e.g., pipes, valves and tank but also instrumentation and control and civil engineering). It also includes the analysis of human factors, which subject covers the procedures and guidelines, the Human Machine Interface (HMI), the emergency organization, the training and the layout (access to buildings, survivability of the control room…). Two examples of the use of PSA Level 2 for EPR design improvement are provided and reviewed: first the modification of the severe accident spraying system, and second the HMI evaluation for the severe accident.

The use of PSA Level 2 in the design phase depends of the model and the level of detail of the developed probabilistic analysis. Discussions on the areas of improvement regarding the use of the PSA Level 2 in the development of a new NPP are proposed.

**Keywords:** PSA Level 2, NPP Design, Systems, Severe Accident Management.

# 1. INTRODUCTION

The severe accident PSA, so called PSA Level 2, is nowadays an integrated part of the safety demonstration. The initial design phase of the new generation of plants, the verification of safety targets, the conception or modification of the mitigation system and the assessment of the human reliability use both the deterministic and the probabilistic approaches.

For the last generations of NPP the verification of the risk based safety criteria have used the results of the PSA Level 1 and 2 to demonstrate the compliance of the NPP with the national requirements provided by the national safety authorities. The International Atomic Energy Agency (IAEA) safety guides (Ref. [1]) state that the overall results of the PSA Level 2 should be compared with the probabilistic safety criteria with the aim to determine whether the risk criteria or targets have been met or whether additional features for prevention or mitigation of accidents need to be provided. Failure to comply with this requirement, as not acceptable on a safety point of view, obviously leads to systems or procedures/guidelines changes.

Indeed, for future nuclear power plants, rather than defining probabilistic criteria, INSAG (Ref. [2]) has proposed the practical elimination of accident sequences that could lead to large early radioactive release, whereas severe accidents that may induce to late containment failure would be considered in the design process with realistic assumptions and best estimate analysis so that their consequences would necessitate only protective measures limited in area and in time. With this approach the design of severe accident mitigation systems becomes a major goal of the deterministic and probabilistic safety assessments.

As part of the IAEA safety standard (Ref. [1]) the recommendation for the use of the PSA for a risk informed approach is strong. The aim of applying a risk informed approach is to ensure that a balanced approach is taken when making decisions on safety issues by considering probabilistic risk insights with any other relevant factors in an integrated manner. It is stated that in any of the applications of the PSA Level 2 described below, the insights from the PSA should be used as part of the process of risk informed decision making that takes account of all the relevant factors when making decisions on issues related to the prevention and mitigation of severe accidents at the plant:
any mandatory requirements that relate to the PSA application being addressed (which would typically include any legal requirements or regulations that need to be complied with);
the insights from deterministic safety analysis;
any other applicable insights or information (which could include a cost–benefit analysis, remaining lifetime of the plant, inspection findings, operating experience, doses to workers that would arise in making necessary changes to the plant hardware, environmental protection concerns, etc.).

The pros and cons require a discussion on the PSA uncertainties that need to be identified, understood and studied to gain confidence in the risk informed approach.

In addition as stated in Ref. [1] the PSA Level 2 report should clearly document important findings including:

- plant specific design or operational vulnerabilities identified;
- key operator actions for mitigating severe accidents;
- potential benefits of various engineered safety systems;
- areas for possible improvement in operations or hardware for the plant and the containment in particular.

Successful application of the PSA Level 2 includes the probabilistic evaluation of plant design to identify potential vulnerabilities in the mitigation of severe accidents, and of the development of severe accident management guidelines that can be applied following core damage. EPR based examples are provided here below.

For generation IV NPP the approach is going further. As detailed in Ref. [3], the Advanced Sodium Technological Reactor for Industrial Demonstration (ASTRID), a demonstration plant to be commissioned in the 2020 decade, is going further in the use of PSA at the conceptual design stage to support the design hypothesis. At this stage, the PSA developed by Commissariat à l'Energie Atomique et aux Energies Renouvelables (CEA) and its partners, AREVA NP and Electricité de France (EDF), aims at providing probabilistic insights to assess design choices and to highlight the weaknesses of the design under safety considerations. Currently only a PSA Level 1 is developed, but a PSA Level 2 is under study in particular to assess the design of the severe accident cooling system.

## 2. PROBABILISTIC EVALUATION OF A DESIGN CHANGE

### 2.1. Context of the PSA Level 2 Assessment for Hardware Design Changes

The design changes for the new NPP can benefice from the PSA Level 2 investigations. It can be used to assess the impact of a new systems used in severe accident conditions or the modification of an existing severe accident system. Any change of configuration of an existing system may lead to technical issues that a preliminary impact evaluation on the PSA Level 2 results can identified.

For the standard EPR the connection of the Containment Heat Removal System (CHRS) active flooding line downstream the flooding valve design change was suggested to be evaluated in the frame of the PSA Level 2 study, in order to assess:

- the benefits of this connection modification in term of PSA Level 2 results due the possibility to actuate the active flooding of the spreading area even in case of a failure of the passive flooding,
- the efficiency of measures such as procedures and administrative controls on the Main Control room (MCR) panel to avoid any spurious flooding by an operator error, including for the severe accident scenarios.

In this example the active flooding line connection upstream the passive flooding valves was proposed to be connected downstream of these valves. The impacts on the PSA Level 2 results were assessed.

Currently the suggested risk metrics used to express the frequency results of the PSA Level 2 are expressed in term of Large Release Frequency (LRF) and Large Early Release Frequency (LERF). For the standard EPR a release is large if bigger than 100 TBq of Cesium. A release is early if before or directly concomitant to the vessel rupture. The detailed risk results of the PSA Level 2 are then expressed in term of fraction of initial Cesium, Iodine and Strontium core inventory. But the scope of the study did not include a detailed quantification of the impact of the design modification on the risk results. It was rather limited to the evaluation of the frequency results of the PSA Level 2.

### 2.2. Probabilistic Assessment of the CHRS Design Change

This evaluation started with the review of all scenarios impacted by the modification. The scenarios of concern cover the normal, incidental, accidental, severe accident and maintenance domains. We consider that any scenarios could evolve to a severe accident situation. In such case phenomenological, system availability and source term impacts on the PSA Level 2 were assessed (qualitative assessment).

Following the design modification an In-containment Refueling Water Storage Tank (IRWST) draining into the core catcher was possible, due to a spurious actuation of active flooding line or an operator error to open the active cooling valves instead of the back-flushing valves. It was also considered that an operator can open the active cooling valves instead of back flushing valves in some sequences, or that the operators could miss the opening of the active cooling valves when needed in some other sequences.

A list of impacted systems by the proposed CHRS design change was set up. This list was indeed derived from this list of impacted scenarios, and includes:

- the CHRS,
- the core catcher:

  The risk is an early flooding of the core catcher. From the core catcher point of view, being flooded is against the functional requirements, and will require draining and cleaning and a plant in cold shutdown.
- the IRWST:

  The status of the active flooding valves and the IRWST water level are available in the control room. If during the accident sequence the active cooling valves are in open position, the operation crew will be aware of the situation and instructs to act in consequence.

Note that the containment isolation function as modeled in the standard EPR RS model is not jeopardized by any spurious opening of the active cooling valves. These valves are part of the containment isolation valves, but the CHRS is included in a bunkered room and is in a closed loop. If the operator would spuriously open the active cooling valve the opening will not lead to releases from the plant.

## 2.3. Scenario of Concern Detailed Analysis

The IRWST draining into the core catcher due to a spurious actuation of active flooding line or an operator error to opens the active cooling valves instead of the back-flushing valves leads to the presence of water in the spreading area during power operation which required a mandatory shutdown. It also lowers the IRWST inventory available for accident mitigation. The impact on PSA Level 2 considered was an unavailability of the IRWST water that could evolved to core damage in a few sequences.

For the scenarios with an operator error to open active cooling valves instead of back flushing valves in incident or accidental situations, with containment spray and switch to back-flushing required, no impact on PSA Level 2 was found due to the low probability of occurrence of these sequences at power. In shutdown states the increase of the Core Damage Frequency (CDF) could be up to a factor 10.

Finally in severe accident situations a spurious actuation of the active cooling valves may be of concern, leading to an early presence of water in the core catcher. In case of spurious actuation of the active cooling valves before the vessel failure and the corium arrival in the core catcher, the presence of water in core catcher leads to an unavailability to perform its quenching function. The interaction between the water and the corium can lead to several modes of containment failure considered in the PSA Level 2.

To assess the combined frequency of all sequences leading to melt stabilization success, which sequences may be jeopardized by a spurious actuation of active cooling valves, a quantification of the standard EPR PSA Level 2 model was performed. All the severe accident sequences concerned by the analysis include a vessel failure and an early flooded core catcher by spurious actuation of the active flooding valves prior corium arrival.

Note that the quantification of the model is performed by using the software tool RiskSpectrum (RS) PSA Professional developed by Lloyd's Register. Point estimated quantifications were used in the frame of this study for the assessment of containment failure split into different Release Categories (RC).

For these sequences three severe accident phenomena are of concern: first a Fuel Coolant Interaction (FCI) leading to a steam explosion that can jeopardize the containment, second is an incomplete melt transfer leading to Molten Core Concrete Interaction (MCCI) in the transfer channel, third a containment over-pressurization due to the contact of the hot material with the water. The containment failure probability for these sequences was assessed. It was found that the risk of FCI, MCCI and containment pressurization was low enough to be considered as practically eliminated.

Another severe accident scenario of concern includes the failure of both passive flooding valves and the operator missing to open the active cooling valves for cooling the corium in the spreading area with water. In such case the failure of the core catcher system is possible if not garanted, and conservatively considered as equivalent to a failure of the containment. For all states (at power and shutdown) these sequences had very low probability of occurrence.

### 2.4. Technical Review Committee Conclusion

The impact of the proposed CHRS design change on the probabilistic results is limited for at power, and significantly increases the risk in shutdown by increasing the CDF. The modification was chosen not to be implemented in the standard EPR based on these results.

## 3. PROBABILISTIC EVALUATION OF HUMAN ACTIONS

### 3.1. Severe Accident Management Issues in Probabilistic Modeling

With the development of the Severe Accident Management Guidelines (SAMG) the question of the modeling of the human actions in the PSA Level 2 and of the potential feedbacks of the PSA Level 2 results in the SAMG become obvious.

In particular as the severe accident systems are integrated in the design of the new plants, modeling their failure modes become part of the safety demonstration. The human failure of the actions to start or verify the correct actuation of these systems contributes also to the PSA Level 2 results. In addition being in severe accident conditions implies that several equipments or components are failed or unavailable, and maybe repaired. The recovery of failed equipments, when part of the SAMG, should be part of the PSA Level 2.

As stated in Ref. [1] when design improvements are being considered with regard to severe accident management measures, a range of options are often available. The PSA Level 2 may be used to provide an input into the comparison of these options. For example, the PSA Level 2 could provide a basis for determining whether severe accident management measures and guidelines fully address the fourth level of defense in depth as defined in Ref. [4].

Modeling the use of SAMG in a PSA Level 2 faces several issues:

- The SAMG actions are based on guidance as opposed to step-by-step procedures. No verbatim compliance to the SAMG is required. So, depending on the SAMG structure of material, the analysis process of the situation may not be obvious.
- The present Human Reliability Analysis (HRA) techniques used in the PSA Level 1 may not be applicable. Some methods like ASEP mainly remain on time-based HEP calculation for post-fault error, focusing more on decision/diagnosis (very sensitive to time) and less on actions.
- the SAMG are under the responsibility of different actors of the emergency crisis organization. This emergency organization structure adds some complexity and sources of error. The final human or error could result from an overall organization failure,
- The SAMG allows multiple choices to the emergency crisis organization when an evaluation of the situation is performed, including the possibility to decide that no action should be performed following the evaluation.
- The SAMG actions are difficult to define on an accident time line and some are directly dependent on the modeling of system and component recoveries or reparation.

In addition modeling of human errors in a PSA Level 2 may introduce possible new containment challenges that may have unique consequence considerations. For example in the Station Blackout Sequences (SBO) the start of the containment heat removal systems de-inert the containment and allow earlier containment failures due to hydrogen burns. If human recovery actions in severe accident lead to earlier releases in the vicinity of the plant the off-site emergency planning actions may be ineffective in the population protection. This aspect of the HRA was studied at the function event level in the RS model of the PSA Level 2.

### 3.2. HRA Methodology for EPR

One of the major obstacles to be overcome in the development of a method to consider SAMG in the PSA Level 2 is the modeling of the human reliability associated with SAMG. For the standard and Chinese EPR a new methodology for the HRA model in the PSA Level 2 was developed. The objective was the selection of an appropriated process and quantification method of the human error in severe accident conditions. The state-of-the-art of the EPR SAMG, so called Operating Strategies for Severe Accident (OSSA), were used as an input.

Due to the specificity of the organization and of the nature of the tasks performed under severe accident conditions (multiple actors, complex chain of command, complex diagnosis, use of different procedures…), the Standardized Plant Analysis Risk-Human Reliability Analysis (SPAR-H) methodology was chosen. It provided simplified assessment of the failure mode, action vs. diagnosis failures. Furthermore SPAR-H leads to a simplified but conservative Human Error Probability (HEP) assessment via the Performance Shaping Factor (PSF) rating.

Besides the HRA process developed follow the good practices prescribed in the NUREG-1792 Ref. [5].

The methodology models the dedicated organization set up to face the severity of the accident. The needed organization relies on interacting local and national teams with different levels of knowledge and responsibilities. The chain of command involves multiple actors using different procedures or dedicated guidelines to cope with an evolving situation.

The methodology assessed the role of the emergency organization in the decision process, and if a Technical Support Center (TSC) evaluation was required. If these human actions correspond to human actions realized on the mitigation path or performed when a challenge exists the TSC evaluation was judged obvious.

### 3.3. Actions and Tasks Analysis for the OSSA

Actions, in MCR and performed locally, necessary for the operation of systems/functions credited in the PSA Level 2 were screened and classified in four categories depending when they were performed during the accident (at the OSSA entrance, as immediate actions, as intermediate actions or in the long term).

Then the actions were divided in tasks. A task modeling so called Hierarchical Task Analysis (HTA) and a Task Analysis (TA) allowed identifying the needed data and cues necessary to perform the actions and the required controls to actuate systems/functions. The involved required HMI could be identified. As a feedback to the HMI design the missing or inadequate interfaces can be identified during the process. Note that a TimeLine Analysis (TLA) supported the evaluation of the time available for the operators to perform the actions for the reference scenarios.

The RS software was used to develop action by action Fault Tree (FT) including all tasks, and to calculate the intermediate and final HEP; the lower level of HEP being calculated with SPAR-H. Some values were given to the defined human recovery tasks in the fault trees. Human recovery is used in severe accident as a safety mean or level of defense to enhance the human operator tasks reliability. The recovery could consist in a recovery of an operator by another one or by a member of the emergency organization. When an action HEP was high, consideration can be given to the recovery of one or several tasks linked to the action. Finally the FT models the organization reliability and not only individual human error.

According to the SPAR-H methodology dependencies between human failures were also modeled. It was chosen to value the recovery tasks trough the fault trees and not trough the work process PSF. This modeling puts the emphasis on the work organization retained in order to enhance the whole organization reliability/resilience.

Note that the consideration of recovery is more difficult with the current static PSA Level 2 model. In the development of the generation IV NPP the use of PSA Level 2 dynamic models intends to develop time/state dependant models. Currently the Research and development (R&D) programs on the Petri nets or on Monte Carlos tries coupled to a RS models allows developing PSA Level 2 models that cover the equipment recovery and the component maintenance.

### 3.4. Improvement of the PSA Model and OSSA following the Human Reliability Analysis

The study emphasized the impact of the dependency between actions. As an example the action to connect the severe accident batteries had not a high HEP, but by the combination of the dependencies between actions it lead to impossibility to isolate the containment, and to major impact on the LRF/LERF.

Recovery was also a requirement for some actions. The OSSA entrance initially modeled with no recovery from any member of the safety organization had a strong contribution to the early release frequencies. Monitoring of the OSSA entry condition by several operators, safety engineer or any other member of the safety organization decreased the delayed entry into the severe accident guideline and the lack of initial response to the severe accident situation.

## 4. CONCLUSION

It is a strong IAEA recommendation for the PSA Level 2 to be used to provide inputs into design evaluation throughout the lifetime of a NPP or during the design process for a new plant.

Currently the use of the PSA Level 2 in the design of the EPR showed some interesting feedbacks of the probabilistic safety into the design, both for the hardware aspects and the severe accident management. It emphasized the major benefits of the emergency organization in the severe accident management.

The studies can cover with a good confidence in the frequency and the source term results the impact of the modified design. However a further step is the knowledge of the uncertainty and their propagation in the PSA Level 2 can improve the PSA Level 2 and the conclusions.

Following the Fukhusima Daiichi Nuclear Power Plant (NPP) accident in Japan resulted from the combination of two correlated extreme external events (earthquake and tsunami). The consequences went beyond what was initially considered in the design of the NPP. The concept of extended PSA is reviewed. It may give in the future a new dimension for the use of PSA Level 1 and 2 in the concept and design phase of NPP.

In the future PSA Level 2 taking into consideration the reparation of the failed or malfunctioning system will change the approaches and results.

## REFERENCES

[1] "Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants", IAEA Safety Standards, Specific Safety Guide n° SSG-4, 2010

[2] "Basic Safety Principles for Nuclear Power Plants", 75-INSAG-3 Rev. 1, International Nuclear Safety Advisory Group INSAG-12, IAEA, 1999

[3] Use of simplified PSA Studies to support the ASTRID design process", ICAPP 2014, USA, April 6-9th, 2014

[4] "Safety of Nuclear Power Plants Design", IAEA Safety Standards, Series No. NS-R-1, IAEA, 2000

[5] "Good Practices for Implementing Human Reliability Analysis", NUREG-1792, 2005

[6] "Severe Accident management Plan (SAMP) for Nuclear Power Plants", IAEA Safety Guide NS-G-2.15, Draft 2014

[7] "The SPAR-H Human Reliability Analysis Method", NUREG/CR-6883, 2005

## ACRONYMS

| | |
|---|---|
| ASTRID | Advanced Sodium Technological Reactor for Industrial Demonstration |
| CDF | Core Damage Frequency |
| CEA | Commissariat à l'Energie Atomique et aux Energies Renouvelables |
| CHRS | Containment Heat Removal System |
| EDF | Electricité de France |
| FCI | Fuel Coolant interaction |
| FT | Fault Tree |
| HEP | Human Error Probability |
| HMI | Human Machine Interface |
| HRA | Human Reliability Analysis |
| HTA | Hierarchical Task Analysis |
| IAEA | International Atomic Energy Agency |
| IRWST | In-containment Refueling Water Storage Tank |
| LERF | Large Early Release Frequency |
| LRF | Large Release Frequency |
| MCCI | Molten corium concrete interaction |
| MCR | Main Control Room |
| NPP | Nuclear Power Plant |
| OSSA | Operating Strategies for Severe Accidents |
| PSA | Probabilistic Safety Assessment |
| PSF | Performance Shaping Factor |
| R&D | Research and Development |
| RC | Release Category |
| RS | RiskSpectrum |
| SAMG | Severe Accident Management Guideline |
| SAMP | Severe Accident Management Program |
| SBO | Station BlackOut |
| SPAR-H | Standardized Plant Analysis Risk-Human Reliability Analysis |
| TA | Task Analysis |
| TLA | TimeLine Analysis |
| TSC | Technical Support Center |