Use of PSA at Institute for Radiological Protection and Nuclear Safety for EPR licensing purposes

Gabriel Georgescu*, François Corenwinder and Jean Michel Evrard
Institute for Radiological Protection and Nuclear Safety (IRSN), Fontenay aux Roses, France

Abstract: The “Technical Guidelines for the design and construction of the next generation of NPPs with Pressurized Water Reactors” specify that the safety demonstration has to be achieved in a deterministic way, supplemented by probabilistic methods. Additionally it is specified that a PSA must be conducted, beginning at the design stage, including at least internal events. In general the probabilistic approach should be used in order to demonstrate a significant reduction of the global core melt frequency comparing with the existing NPPs. The accident situations which would lead to large early releases, such as V-LOCA, boron dilutions, high pressure core melting, spent fuel pool melting, etc. should be “practically eliminated”.

For EPR the PSA was used from the beginning of the design, several design improvement being defined. In the frame of the application for commissioning it is expected that EDF will provide an “as-build” full scope PSA for the reactor and for the spent fuel pool. The probabilistic approach will cover the internal events, the internal and external hazards of significant impact.

In parallel, in order to dispose of the appropriate knowledge and tools for the independent verification of the EDF studies, IRSN develops its own limited scope PSA model.

Keywords: EPR, PSA, licensing, new NPP

1. INTRODUCTION

At the Flamanville site, a European Pressurized Water Reactor (EPR) unit (named Flamanville 3) is under construction in France.

The creation authorization was granted by the French Nuclear Safety Authority (ASN) in April 2007. After the first tenders had been awarded and the requisite permits had been granted, site preparatory works began during the summer of 2006. The first pouring of concrete for the nuclear block took place on December, 2007 and the plant construction phase will continue for 54 months, with commissioning planned for 2012.

The Institute for Radiological Protection and Nuclear Safety (IRSN), as the ASN technical support organization, analyses the Flamanville 3 licensing support documentation. This documentation includes several PSA studies submitted by EDF during the licensing processes. In France the PSA is developed and used according to the Basic Safety Rule “Development and utilization of PSA” in reference [2].

2. EPR DESIGN

The EPR is a French and German next-generation 1600 MWe class PWR. It is an evolutionary power reactor based on PWR technology originally developed in the United States. Its design evolved globally from mature and proven technologies, in particular the N4 and Konvoi plants, the most modern nuclear plants in France and Germany. It is designed to ensure the respect of the highest safety standards.

The EPR design takes advantage of over 30 years of operating experience acquired by French and German designers and operators. This approach was implemented by electricity producers and manufacturers in conjunction with both countries’ nuclear safety authorities.
In 2000, following the review of the conceptual design of EPR during the ‘90 years by the French and German nuclear safety authorities (by German experts after 1998), technical guidelines governing the project’s nuclear safety options and defining the requirements for detailed studies were issued. These technical guidelines, formalized in the document “Technical Guidelines for the design and construction of the next generation of NPPs with Pressurized Water Reactors”, become official in France in September 2004 (letter ASN in reference [1] “Safety Options for the EPR Reactor”). The main safety objectives indicated by the ASN by its letter are, compared with the existing reactors, the followings:

- reduction of the number of incidents by a better systems reliability and better consideration of the human factor,
- the core damage risk should be significantly reduced,
- the radioactive releases should be also significantly reduced:
  - no population evacuation in case of accident without core damage,
  - practical elimination of the large early releases,
  - limited protection measures (in time and in space) in case of late releases.

In practice, these safety objectives can be achieved by several features of the EPR design. Some examples are:

- tight double containment,
- built-in severe accident features (as for example the special compartment inside containment to collect the core in case of core melt),
- external anti-aircraft crash shield covering the containment, the spent fuel building and two out of four safety systems buildings,
- four electrical trains including two series of diversified Diesel generators (four main Diesels and two SBO Diesels),
- four 100% trains, physically separated, for the main safety systems and related support systems,
- high quality human-machine interface, based on up to date technology.

3. REQUIREMENTS FOR EPR PSA

3.1 “Technical Guidelines” requirements regarding the design phase PSA

The “Technical Guidelines for the design and construction of the next generation of NPPs with Pressurized Water Reactors”, mentions that the safety demonstration for the nuclear power plants of the next generation has to be achieved in a deterministic way, supplemented by probabilistic methods. A significant reduction of the global core melt frequency must be achieved for the nuclear power plants of the next generation, compared with the existing reactors. Implementation of improvements in the "defence-in-depth" of such plants should lead to the achievement of a global frequency of core melt of less that $10^{-5}$ per plant operating year. It is also mentioned that a probabilistic safety assessment must be conducted, beginning at the design stage, including at least internal events. This probabilistic safety assessment would indicate the frequencies of core melt sequences with a view on the possible consequences of the different types of core melt situations on the containment function.

The probabilistic safety assessment has to be performed with the following objectives at the design stage:

- supporting the choice of design options, including redundancy and diversity in the safety systems,
- well-balanced safety concept and evaluation of deviations from present safety practices,
- appreciation of the improved safety level compared to existing plants.

Concerning the general methodology, the probabilistic safety assessment can be carried out in two or more steps:
• a simplified assessment at the conceptual stage, and,
• more complete studies during the engineering phases, when more precise information on the design becomes available.

The simplified assessment, including at least internal events, has to present a preliminary evaluation of the core damage frequency and the corresponding sequences; furthermore, the designer has to distinguish between the different types of core melt sequences according to their consequences related to containment behaviour.

Moreover, at the conceptual stage, different design alternatives have to be analysed, and sensitivity studies have to be performed. However, the application of a probabilistic safety assessment at an early stage of the design has to be handled cautiously because the final results will be dependent on the real choice of components, system techniques and operational procedures. Nevertheless it is underlined that, even for the first assessment at the conceptual stage, the designer has to consider a list as complete as possible of initiating events. It is also stressed that the treatment of common cause failures is essential for the assessment of some design options. Another special concern is the treatment of human interventions, including diagnosis and maintenance. The use of qualified data is also essential.

The “Technical Guidelines” precise also that, in the frame of the deterministic safety demonstration of the EPR reactor, in addition to reference transients, incidents and accidents, multiple failures conditions have to be considered. The results of the probabilistic safety studies done at the design stage will have to be used to check and adjust the preliminary list of multiple failures conditions and to check the appropriateness of the foreseen additional measures.

3.2 IRSN requirements for EPR PSA

IRSN considers that, generally, for the EPR reactor all the initiators, including the external and internal hazards, have to be studied by using probabilistic methods, as far as possible. The PSA, even simplified, allows to appreciate the plant global safety level and to highlight the weak points which are not or partially treated by the classical deterministic methods.

Regarding the internal events Level 1 PSA, the fulfilment of methodological aspects included in the “Technical Guidelines” as well as in the Basic Safety Rule “Development and utilization of PSA” in reference [2] is sufficient to allow a quality internal events PSA for the licensing process. Nevertheless, regarding the treatment of internal and external hazards, these documents are not enough prescriptive, and consequently some specific requirements were developed by IRSN.

IRSN considers that the development of the hazards PSAs for the EPR Reactor can be realized in two steps:

- Simplified hazard PSAs in the frame of the application for commissioning; this step intends to provide a first evaluation of the achievement of the probabilistic goals for the internal and external hazards, in a simplified manner. Both, the hazards and the corresponding load cases used at the design stage and the hazards and load cases beyond design basis have to be considered. For some hazards, a qualitative approach can be used, when it can be surely demonstrated that the risk is residual.

- Complete hazard PSAs after an initial plant operation period; IRSN considers that, for the Final Safety Analysis Report, the objective should be to develop a complete hazard PSAs, when the hazards can be characterized. At least, the simplified studies previously developed should by updated and completed after the plant commissioning, in order to take into account the “as-built” NPP, in terms of final design, installed equipment, fire compartments, seismic supports, accident procedures, etc. Some aspects related to the initial operation period can also have an impact on the PSA.
IRSN considers that, the scope of the simplified hazard PSAs have to include at least the following hazards, their potential combination as well as the induced loss of heat sink and loss of offsite power:

- fire,
- internal flooding,
- earthquake,
- external flooding (all the hazards included in this category, as rainfall, storm, ground water, etc.),
- internal explosion,
- extreme wind leading to the pumping station plugging and to the loss of external power,
- extreme cold.

Regarding the Level 2 PSA, the availability of a full scope Level 2 PSA (which would include the internal and external hazards) is deemed necessary in the frame of application for commissioning. The Level 2 PSA update to take into account the “as-built” NPP will be done for the Final Safety Analysis Report.

The mentioned PSAs should consider the safety of the reactor core as well as of the spent fuel pool.

4. PSA DEVELOPMENTS FOR EPR

During the different phases of the EPR reactor design several PSA were developed by the EPR designer (AREVA) and then by EDF. In parallel, in order to dispose of the appropriate knowledge and tools for the independent verification of the EDF studies, IRSN develops its own limited scope level 1 PSA model. The different assessments are here shortly presented.

4.1 PSA during EPR design stages

For EPR the PSA was used form the beginning of the design by AREVA. During the design stages the PSA was essentially a limited scope Level 1 PSA which developed with the design, the probabilistic models being up-dated several times in order to consider the latest design features. This allowed identifying several design improvements, like: SBO Diesels, diversification of ultimate heat sink, diversification of support systems of the safety systems, etc.. Additionally, a simplified level 1+ PSA was developed in order to investigate the containment and the built-in severe accident features.

The reliability of the systems needed to ensure the safety of the spent fuel pool was also investigated; this allowed identifying the need for a third cooling train with diversified power supply and heat sink. In parallel, methodological developments were done for the Level 2 PSA, Fire PSA as well as for the PSA application for the assessment of the multiple failure situations.

4.2 PSA for Flamanville 3 creation request

In the frame of the Flamanville 3 application for NPP creation, the licensee (EDF) provided several PSAs and PSA’s applications.

Level 1, internal events PSA related to the reactor core

The study considers all reactor states, from the full power to the core unloaded with at least one fuel element in the reactor core, only the internal initiating events being considered (however, the loss of ultimate heat sink and the loss of external power supply, which are external initiating events are here included).

The main results of the internal events PSA are presented in the table 1 (extracted for the Public Preliminary Safety Analysis Report of Flamanville 3 NPP in reference [3]).

The analysis of the PSA allowed identifying several design issues which need to be clarified during the final design stage. These aspects are related mainly to the diversity of systems and components,
new design features (like the Partial Cooldown function), the possible inadvertent automatic signals, the ATWS capability (importance of the moderator coefficient), etc.

Table 1 EPR PSA Level 1 results

<table>
<thead>
<tr>
<th>Category</th>
<th>Sub-category</th>
<th>Core damage frequency (reactor x year)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Power</td>
</tr>
<tr>
<td>LOCA</td>
<td></td>
<td>1.37 (10^{-7})</td>
</tr>
<tr>
<td>VLOCA</td>
<td></td>
<td>3.72 (10^{-7})</td>
</tr>
<tr>
<td>Secondary break</td>
<td>Secondary break</td>
<td>1.89 (10^{-8})</td>
</tr>
<tr>
<td></td>
<td>Secondary break + SGTR</td>
<td>6.21 (10^{-9})</td>
</tr>
<tr>
<td>SGTR</td>
<td>SGTR</td>
<td>1.41 (10^{-9})</td>
</tr>
<tr>
<td>Secondary transients</td>
<td>Total loss of feedwater</td>
<td>1.10 (10^{-7})</td>
</tr>
<tr>
<td>LOOP</td>
<td>Total loss of offsite power (2h)</td>
<td>1.68 (10^{-9})</td>
</tr>
<tr>
<td></td>
<td>Total loss of offsite power (24h)</td>
<td>2.95 (10^{-8})</td>
</tr>
<tr>
<td></td>
<td>CCF of LH busbars</td>
<td>5.12 (10^{-9})</td>
</tr>
<tr>
<td>Primary transients</td>
<td>Homogenous dilution</td>
<td>2.83 (10^{-9})</td>
</tr>
<tr>
<td></td>
<td>Total loss of RHR</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Uncontrolled level drop</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Total loss of CVCS</td>
<td>9.81 (10^{-9})</td>
</tr>
<tr>
<td>Loss of cooling</td>
<td>Loss of cooling chain</td>
<td>3.86 (10^{-8})</td>
</tr>
<tr>
<td></td>
<td>Loss of ultimate heat sink</td>
<td>4.31 (10^{-8})</td>
</tr>
<tr>
<td>ATWS</td>
<td></td>
<td>1.24 (10^{-7})</td>
</tr>
<tr>
<td>Heterogeneous</td>
<td></td>
<td>5.20 (10^{-9})</td>
</tr>
<tr>
<td>dilution</td>
<td></td>
<td>TOTAL</td>
</tr>
</tbody>
</table>

Probabilistic assessments to support the “practical elimination” of large early releases

Two standalone probabilistic assessments treating the containment by-pass scenarios and the heterogeneous boron dilutions were presented by EDF. The studies confirmed the possibility to achieve extremely low frequency of occurrence of such situations and provided the information to specify detailed design characteristics (like, for example, components reliability and diversification).

Spent fuel pool PSA

For the spent fuel pool, a standalone probabilistic assessment was developed, treating the loss of cooling situations but also the loss of inventory situations. Some design optimisations, mainly related to the reduction of frequency of loss of water inventory situation by inadvertent siphoning were defined.

Level 1+ PSA

In order to estimate the efficiency of the containment systems and of the built-in severe accident features, a simplified version of the Level 2 PSA (Level 1+ which consists in a prolongation of the Level 1 PSA with the containment systems) was presented by EDF. This study allowed to identify some design optimisation related to the design of support systems needed for the mitigation of severe accidents, as for example the power supply of the primary circuit last depressurisation valves and of the severe accident dedicated I&C.

Multiple failure situations

An application to the assessment of deterministic multiple failure situations, called Risk Reduction Categories (RRC-A), considered in the design of the EPR reactor was presented by EDF. The RRC-A list was firstly defined by the “Technical Guidelines” and it should be adjusted taking into account the results of PSA.
Initial assessment of internal and external hazards

For several internal and external hazards, simplified probabilistic quantitative or qualitative assessments were presented by EDF. These hazards are: internal fire, internal explosion, internal flooding, leak or rupture of components, internal missiles, heavy load drop, earthquake, airplane crash, industrial and transport hazards, extreme climatic hazards (heat wave, extreme cold, cold/snow and wind, frazil formation and freezing), external flooding, lighting and electromagnetic interference and heat sink plugging by marine detritus arrival. As presented here above, IRSN considers that these assessments have to be supplemented by more complete PSA before the Flamanville 3 NPP commissioning.

Two standalone probabilistic studies were also presented for the assessment of the long term loss of offsite power (8 days) and of the loss of ultimate heat sink (4 days) in all reactor states. These studies allowed defining the Emergency Feedwater System (EFWS) supply system requirements as well as the Diesels generators operational requirements.

4.3 Expected licensee’s PSAs for FLA3 EPR commissioning

The Internal Events Level 1 PSA for reactor core will be updated in order to take into account the final plant design. The PSA will be completed with detailed modeling of the support systems and PSA support studies will be performed in order to reduce the uncertainties related to the plant behavior.

The Internal Events Level 1 PSA for the spent fuel pool will be also updated, in order to dispose of an integrated model for both loss of cooling and water drainage accident scenarios induced by the internal initiating events and the internal and external hazards.

It is also expected to dispose of complete hazard PSAs. The licensee will provide the following PSAs:

- Internal Hazards PSA: Fire PSA, Internal Explosion and Internal Flooding,
- External Hazards PSA: Earthquake, Extreme winds, Extreme cold.

Limited assessment will be provided for the external flooding (only the pumping station) and heavy loads drop (limited to handling devices reliability assessment).

A complete Level 2 PSA will be provided by the licensee in order to demonstrate the fulfillment of general safety requirements for the EPR reactor.

The probabilistic studies performed to support the conclusion of the practical elimination of the containments by-pass and of the heterogeneous boron dilutions will be also updated in order to take into account the final design.

The list of multiple failure conditions (RRC-A) and the corresponding design features will be assessed by using the updated PSAs.

4.4 PSAs for EPR developed by IRSN

In parallel, in order to dispose of the appropriate knowledge and tools for an independent verification of the EDF studies, IRSN develops its own limited scope level 1 PSA model. The experience in development and using of PSA at IRSN is rather extensive taking into account the past and actual developments (internal events PSA for the 900 MWe and 1300 MWe plants, fire PSA, seismic PSA, internal flooding PSA, HRA research activities, reliability data and CCF research activities, etc.).

The EPR PSA model, which first version is already available, deals with the internal initiating events supplemented by the “loss of offsite power” and “loss of heat sink” initiating events. Simplified modeling of the external and internal hazards is foreseen in the next future. As the objective of this PSA is to support the licensee PSA verification and early plant design checking, special attention will be paid to the model flexibility and facilities to perform sensitivity studies (house events, groups, attributes, etc.).
5. INSIGHTS

The availability of the probabilistic tools as a complement to the deterministic methods allows today to consider the risk information and the risk importance ranking from the design stage of new plants. Deterministic methods continue to be very effective to ensure safe plant design, however the probabilistic methods is increasingly being used to develop risk optimized design. The use of PSA is nevertheless raising new challenges for the development, utilisation and interpretation of the PSA models.

Firstly, the PSA should be able to support the identification of design weakness and the determination of appropriated alternative solutions, allowing the assessment of risk benefit of different design options. In this context, the PSA should allow the easy understanding of the contribution of components and systems to accident sequences. PSA should allow the identification of important systems interdependencies and of the important common mode failures (CCF). Moreover the PSA should be able to identify the accident scenarios sensitive to human actions.

Secondly, the PSA should be able to support the optimisation of the design, by taking into account the information provided by the risk assessment, in order to determine the good balance between the safety and the availability and between the prevention and mitigation measures. The using of cost-benefits methods can also be supported by the PSA.

The scope of the PSA should by at least a simplified Level 2 PSA. The PSA should determine the frequency of different plant damage states and it should identify all important physical and functional dependencies that affect containment or confinement systems. The accident sequences induced by the most relevant internal and external hazards should be also considered.

Some of the most important PSA aspects, revealed by the IRSN PSA developments and by the IRSN verification of the licensee/constructor PSAs during the different phases of the EPR design, beginning at the very early design stage, are hereafter shortly presented.

Reliability data: some of the components will be of the same type as in the existing NPPs, some of them are largely used in the industry, but some others are new, evolutionary components for which the operating experience is very limited or does not exist (usually this is the case with some electrical and I&C components). The identification of most appropriated reliability data in a design PSA is not a trivial activity and it has to be done having in mind that the study insights are sometimes highly dependent on the data. The assumption that the new components have the same reliability as the existing ones can be a reasonable initial assumption. Sensitivity studies should be performed at least for the dominant contributor’s reliability data.

Common cause failures: the treatment of common cause failures needs a special attention for new designs, the insufficient diversity of redundant systems having to be identified and improved if it is found as a dominant risk contributor. The CCF groups and parameters should be carefully assigned in order to avoid the distortion of the results, preferring a rather conservative treatment when the information is not sufficient.

Hazard area events: in order to allow the assessment of the impact of the internal and external hazards on the plant safety, it is important that the design phase PSA incorporates useful information (like equipment location, fire compartments, etc.), even using simplified assumptions. A thoughtful verification should be done regarding the possible common mode failures of redundant trains, systems or functions.

Systems interdependencies: the systems interdependencies represent a crucial point of the design of the new plants. The PSA is one of the most powerful tools to study the impact of different design solutions. Even if the complete design is not finalised, the interdependencies between the safety systems, i.e. functional dependencies or induced by the support systems (power supply, cooling,
ventilation, I&C, etc.) should be modeled as detailed as possible, and conservative assumptions should be used if the information is not available. The omission of the dependency modelling, even the detailed design of support systems is not known, should be avoided.

New design features: this aspect should be carefully investigated, a thoughtful study of the potential new initiating events, failure modes, event sequences and dependencies that may be introduced by new design features should be performed. The effects of the inadvertent actuation of the new automatic actions should be carefully analysed.

Preventive maintenance: the foreseen preventive maintenance should be taken into account in the design PSA. The unavailabilities due to the maintenance but also the system configurations for maintenance are particularly important.

Technical Specifications and Surveillance requirements: the surveillance requirements and the technical specifications are generally not available during the design phase. The aspects should be modelled as accurate as possible since the PSA can be further used to define “risk-optimized” Technical Specifications and surveillance requirements.

I&C failures (including software “failures”): the advanced NPP design includes digital, software based instrumentation, control and protection systems. Advanced, computerised, operator interface is now generally foreseen. It has to be recognized that the today PSA methods have limited capability to estimate the reliability and risk contributions from such kind of systems. The EPR design PSA incorporates this information by using the “compact model”, which allows to identify the dependencies induced by I&C systems and to identify the dominant I&C contributors. The IRSN considers that the approach is acceptable for a design PSA.

HRA: since the procedures (operating, emergency, maintenance, etc.) are in general not available a rough HRA model (pre-accidental and post-accidental) is in general used in the PSA. IRSN considers that, for a design PSA, a “screening” HRA model can be used, but with a careful consideration of the dependencies (between the pre-accidental actions, between the post-accidental actions and between the operator actions and the automatic actions).

In practice the above presented aspects are treated in an iterative manner, several PSA versions being developed, following the design completion.

6. CONCLUSION

The use of the PSA from the early design for the EPR reactor shows that the PSA is a very valuable tool to obtain an optimised and balanced design by taking into account the information provided by the risk assessment. On the other hand, the development and the use of PSA should take into account some specific methodological aspects of a design phase PSA. The decision making process should consider the fact that PSA for a new plant design may contain substantial uncertainties. Extensive sensitivity studies should be performed and the uncertainties should be known and taken into account.

Acknowledgements

Many thanks to Mrs. JM Lanore for the reading of this paper.

References