ETSON

EUROPEAN
TECHNICAL SAFETY
ORGANISATIONS
NETWORK

# LESSONS LEARNED ON, FROM AND FOR PROBABILISTIC SAFETY STUDIES

## TECHNICAL REPORT

ETSON/2024-002- NOVEMBER 2024

# CONTENTS

# 1 INTRODUCTION

There are many publications which detail the use and development of probabilistic safety assessment (PSA). The publicly available Nuclear Energy Agency (NEA) Working Group on Risk Assessment (WGRISK) documents "Use and Development of Probabilistic Safety Assessment – An Overview of the situation at the end of 2010" (NEA/CSNI R(2012)11 /NEA 13/ and "Use and Development of Probabilistic Safety Assessment - An Overview of the Situation at the End of 2017" /NEA 20/ are prominent and comprehensive examples. Another set of PSA documents which focus on "extended" PSA are within the EU Advanced Safety Assessment Methodologies: Extended PSA (ASAMPSA_E) Project (www.asampsa.eu) /DEC 17/.

The members of the ETSON PSA Expert Group do not intend to update such guidance documents. They rather feel that their extensive experience in performing and reviewing PSA merits summarizing a set of technical issues which have come up during PSA work, which may be helpful for understanding and improving PSA beyond formal guidelines.

The ETSON expert group on PSA discussed several issues which seem relevant and could be addressed in the document, e.g.:

- Why and how does PSA evolve over time? How do new experiences influence PSA? How to make sure that PSA is as complete as possible? Are there areas which can be considered as "closed"?
- Examples of events and/or issues having been identified and resolved by using PSA results, e.g. "Does the large effort for performing full scope PSA pay off?"
- Did real events not considered in PSA occur? Why have such events not been covered in previous PSA?
- It is too simplistic to suggest that the initiating event frequency or the height of the protective sea defenses were insufficient for a major Tsunami in the Fukushima Dai-Ichi PSA given these are a well-known threat in Japan. The scenario progression of such severe accidents was not fully considered. Is it possible that other existing PSAs underestimate the risk from significant hazards? Or are safety analysts exaggerating some risks unnecessarily? Sites with multiple reactor units and/or multiple sources are not always systematically considered in the present PSA studies. Considering that several nuclear power plan (NPP) sites have more than one reactor unit and sometimes also multiple and different sources of radioactivity (e.g., reactor and spent fuel pool (SFP)), their risk assessment is a relevant open issue, providing experience that can be learned from.
- Aggregation of parts of PSA assessed with different levels of conservatism and of uncertainties is a difficult problem which could lead to an incorrect view on the risk contributions and then to the possibility of inappropriate decisions.

How to take into account the results of simplified conservative PSA developed just to demonstrate that a probabilistic target is met? Apart from probabilistic targets, most PSAs aim at demonstrating a "well-balanced" safety design. For achieving this, a realistic and comprehensive PSA is required.

- Is there (from a PSA point of view) a low frequency limit beyond which no more detailed analysis is justified? Or to be safer, should mitigative and robust provisions be evaluated against any unlikely event?

This example list demonstrates that there are many interesting and sometimes critical questions within the area of PSA practice. The regulations in many countries do not require development of a Level 3 PSA to fully quantify these effects but many do require Level 1 and Level 2 PSA studies which will identify the hazards and provides key information on the routes and scale of potential releases of radioactivity from the facility. This supports improved facility design, monitoring and emergency planning.

Unfortunately, many of the statements in this document are rooted in PSA work which cannot be cited publicly, e.g., when it is based on review work on behalf of regulatory authorities. Therefore, the present document is limited to ETSON's internal use.

The focus of this report is on experiences / lessons learned from a reviewer's point of view. The authors hope that those less experienced in PSA in the technical safety organizations (TSOs) will benefit from the content of this report.

# 2 GENERAL PERSPECTIVES

## 2.1 Deterministic versus Probabilistic Safety Assessment

Historically, PSA were introduced as a complement of the deterministic safety demonstration. Both approaches are nevertheless to be combined and in practice any safety analysis will always include a mixture of probabilistic and deterministic aspects with varying weight for each.

In this report, the term "deterministic approach" means an approach which is based on predetermined bounding assumptions and methods and that produces individual results. An experiment or model can be used to demonstrate process behaviour. That means that the process analysed is fully determined by state variables that have predetermined values. Stated values may be set conservatively to compensate for uncertainties to ensure conservative results.

In this report, the term "probabilistic approach" means an approach considering the variability of process state variables, i.e. stochastic behaviour of the process (aleatory uncertainty) and uncertainty of knowledge (epistemic uncertainty). It produces results with an uncertainty interval. A series of experiments with different initial conditions and/or configurations, or stochastic modelling can be used for demonstrating process behaviour. The probabilistic approaches may explicitly identify the uncertainties and the incompleteness of knowledge.

## 2.2 PSA Achievements

Hazardous events or sequences can be identified by different techniques, e.g. by postulating certain failures or combinations of failures. This is typical for deterministic safety analyses. A practical example is the single failure approach: It needs to be demonstrated that a system experiencing an initiating failure and further consequential failures can still cope with a further single failure that leads to the highest challenge to the safety systems, without determining the probability of such a failure.

The added value provided by PSA is that it widely considers combinations of failures and human errors and determines the probability of hazardous events and sequences. This makes it possible to identify important risk contributors, e.g.:

-the relative risk contribution of different components, systems, human actions or event sequences,

-a safety ranking based on quantitative risk indicators.

Such information, which cannot be obtained without PSA, may be used for:

-efficiently improving the plant safety,

-demonstrating compliance with quantitative safety objectives.

The use of PSA has gradually increased over the last decades and now it is an integral part of the safety assessment process. Some historical outstanding achievements of PSA, which sometimes led to significant plant modification, are:

- Identification of the risk relevance of small loss of coolant accidents (LOCAs) in a time when there was a common belief that the provisions against large LOCAs would envelope small LOCAs as well;
- Identification of the risk relevance of shutdown states;
- Significant improvement of plant safety by optimizing plant design and operation, including assessing potential plant backfits as a reaction to the nuclear accidents at Fukushima.
- Identification of the risk significance of multiple failure situations (including design extension conditions of redundant items important to safety). In some countries, this led to the definition of design extension conditions.

The present relevance of PSA in decision-making is different among countries and organizations. In Section 5 a range of examples for different PSA applications is given.

## 2.3 PSA Challenges

PSA has evolved over time, as NPPs have. The flexibility of PSA is an advantage, as it can evolve to consider plant modifications, new events or new knowledge. A PSA which has been performed decades ago for a specific NPP would look very different today. It is often difficult to track precisely which differences are due to the PSA methodology and modelling advances and which are due to plant modifications. This is of interest because earlier PSA methods had shortcomings and deficiencies which have partly been overcome, but some, e.g. risk aggregation, may still exist, perhaps even unnoticed.

An obvious issue is the availability, quality and relevance of data to be introduced into the PSA model. This is routinely addressed by PSA practitioners; however, data uncertainty remains a significant challenge to PSA. This particularly applies to the assessment of common cause failure (CCF) issues. Their importance for highly redundant NPP safety systems is significant; however, it is a complex and very difficult task to derive CCF probabilities from operating experience or theoretical considerations. The same is true for human reliability analysis. Nevertheless, PSA can be used to identify and to assess the significance of such uncertainties in the safety assessment.

Another complex issue is the question of the completeness of the PSA. Some of the present PSA models are very sophisticated; however, like for any model, their scope is bounded. Moreover, within the scope of the PSA, the degree of analysis completeness may not be homogeneous.

Traditionally, some issues have been out of the PSA scope, e.g. unforeseen operator actions, malevolent acts, multi-unit issues. When compared to the increasing safety of normal operation regimes, these issues may become relatively risk-dominant and thus render the PSA results less relevant. The fact that the risk assessed by PSA did not consider malevolent acts is primarily a deliberate choice and not a methodological deficiency. For this type of hazardous situation, PSA is not intended to evaluate the

risk but to identify sensitive areas or key scenarios.

For the issue of multi-unit and multi-source sites, discussions as well as research and development (R&D) activities for methodological developments are ongoing in many organizations and are subject of international cooperative work (e.g., by IAEA or OECD NEA CSNI WGRISK, see e.g. /IAE 17/, /CNS 14/, /NEA 19/, /ROE 18/, /ROE 19/, /IAE 18/, /IAE 19/, /IAE 24/, /IAE 24a/, /IAE 24b/, /IAE 24c/, /IAE 24d/. Considering that many sites have more radioactive sources than only one reactor unit (e.g., separate SFPs, radioactive storage and waste treatment facilities) this might be a relevant issue with an important impact on PSA results and on PSA applications.

Natural external hazard assessment is an issue which is not unique to NPPs but nevertheless can significantly impact PSA (see /ETS 17/, /NEA 14a/). It is often not possible to accurately predict occurrence frequencies of high impact, low-frequency natural hazards (below ~ 1 E-04 /ry). These large uncertainties contrast with the significantly higher precision which can be obtained for internal event sequences (e.g. in the order of 1 E-07 /ry). Risk aggregation needs to be carefully performed for decision-making.

A further complication is that climate change may increase the frequency of some extreme meteorological events. For new NPPs with design lives equal to or above 60 years, the future period that needs to be considered may be approximately 100 years, including the decommissioning period.

As an example of how this is being addressed, the United Kingdom Meteorological Office periodically produces climate change projections for the United Kingdom under different global emissions scenarios under the UKCP Project, last updated in August 2022. The United Kingdom Regulators (ONR, Environment Agency, and Natural Resources Wales) have issued a Position Statement /ONR 19/ stating that they expect that these projections should be used in external hazard assessments.

There is abundance in PSA guidance aimed at completely covering all issues of high and low safety importance. However, when a PSA is performed under the real-world constraints of budget and resources, many issues must be ignored or addressed in a manner which does not really represent the state of the art. However, it is necessary to ensure that these shortcomings do not impact the PSA results and insights in the frame of the intended goals.

Limitations in PSA scope (e.g. only internal events) may also lead to important limitations in applicability and in acceptance of PSA applications.

It has to be noted that the necessary PSA capability (level of detail, completeness, etc.) depends mainly on its application. The same PSA could be insufficient for a given application and acceptable for another one (a perfect PSA able to treat any application does not exist). For example, the PSA carried out at the beginning of the EPR design in France was very simplistic, including only five internal initiating events families and a Level 1+ PSA (Level 1 including effects on the containment). However, this simplistic PSA was sufficient for identifying the need to incorporate several important safety improvements:

Although the PSA results were not the only basis for making decisions, the preliminary PSA has played a role in several design improvements, for example:

- Implementation of two additional diverse diesel generators (in addition to the four main diesel generators):
- Diversification of the cooling of two low-pressure injection pumps;

- Diversification of a level signal in the main loops;
- Diversification of the ultimate heat sink (a result of Level 1+ PSA).

# 3 PSA AND REAL EVENTS

- It turns out that real events which have been observed might not be represented satisfactorily by the existing PSA models. The models will probably be improved after such deficiencies have been detected, however, it remains uncertain when another real event not modelled properly in PSA will occur.

- This section presents practice and experience relating to real events and PSA. It addresses different aspects: the relationship between real core and fuel damage accidents and PSA results (see Section 3.1), precursor analysis (in Section 3.2), use of PSA to inform decisions during or after the events (see Section 3.3), and PSA changes as a result of the event (cf. Section 3.4).

## 3.1 Core or Fuel Damage Accidents

There is an opinion that the number of real core melt accidents is higher than that expected from PSA and, consequently, that PSA results are not quite correct. Counterarguments may read as follows:

-The Chernobyl nuclear accident occurred in a plant state which was far from normal operation, and which was violating operating instructions. PSA does typically not address such conditions of extreme violation of the rules and extremely low safety culture. There is no indication that PSA for the common operation had given false information. If there is a lesson learned for PSA from the Chernobyl accident, it consists in underestimation of the potential of control room operators and plant management to willingly violate instructions in unplanned plant conditions. Regarding recent PSAs, it can be assumed that such extreme human behaviour is less likely to be repeated, however, the PSA may have the capacity to address such behaviour. The continuous effort to improve the design and strengthen the safety culture of an organisation contributes to reducing the frequency of these types of accidents.

-The nuclear accidents at Fukushima were initiated by a very powerful earthquake and a devastating Tsunami as a "hazard combination". The plants survived the earthquake in a state which is probably consistent with PSA. If a PSA had assumed a Tsunami of the height which really occurred, it would have probably correctly predicted core melt. So, the deficiency of the PSA (a deficiency shared with deterministic safety analysis) consists in the underestimation of the frequency of Tsunamis of this magnitude.

-PSA results are plant-specific and location-specific. Occurrence of core damage in one plant certainly imposes the evaluation of this experience for other plants, but does not imply incompleteness or incorrectness of other plant's PSA.

It could be argued that the PSA community did not clearly communicate enough the limitations of the existing PSAs (e.g., very rough assessment of external hazards), or the PSA users did not (want to) understand the limitations.

## 3.2 Precursor Analysis

PSA-based event analysis (PSAEA) (or precursor analysis), performed either by the licensee or by the TSO, often using existing PSAs, is most helpful in the overall process of operating experience feedback (lessons learned from real events, identification of corrective actions, etc.) and is also often useful to further improve PSA models (missing elements in the PSA model, incorrect modelling, more detailed modelling, etc.).

PSA results are also highly important for the so-called Fukushima "precursor" analysis performed by CNRA; for details see a report by OECD NEA CNRA WGOE /NEA 14/ on "what is the next Fukushima", to which the PSA community (and, in particular, IRSN and GRS) contributed.

### 3.2.1 BELGIUM

Performing precursor analysis is required by Belgian law. Precursor analysis is performed by ENGIE for all operating events that can be modelled with the Level 1 internal events PSA. Some events are also assessed with the Level 2 PSA by the architect-engineer of the utility (Tractebel Engineering). Significant events are also assessed by BEL V. An event is considered as a precursor when the conditional core damage probability (CCDP) is higher than E-06 and is considered as a major precursor if the corresponding CCDP is higher than E-04. PSA is used as an indicator to identify the most important events and to motivate the utility to implement corrective actions accordingly. No prescriptive threshold for the CCDP has been indicated in the Belgian law. As for other PSA applications, PSA is used as a complementary tool and is not the sole input to decision-making.

### 3.2.2 CZECH REPUBLIC

Each year, precursor analysis is carried out by the specialists of the company UJV Řež, with the evaluation being supervised and supported by the Czech regulatory body. Dukovany NPP and Temelin NPP both provide complete lists of operational events with possible safety impacts and detailed information about the events. In several consecutive levels of screening, various events are selected, which are analysed in detail by plant PSAs, including necessary changes made in PSA models, what-if analyses, etc. A comprehensive report is produced every year, which is later analysed by the Czech regulatory body.

### 3.2.3 FRANCE

The probabilistic analysis of operating events (precursor program) is performed by the licensee (EDF) for all events and by IRSN as TSO for the most significant events. An operating event is considered as a precursor if the CCDP due to this event is higher than E-06. Moreover, for the most important events (CCDP higher than E-04), the Safety Authority (ANS) requires EDF to define, in the short-term, corrective measures and to assess the corresponding risk reduction. The results of the precursor program allow a better ranking of priorities.

### 3.2.4 GERMANY

Precursor analyses are performed by GRS on behalf of the Federal Environmental Ministry (BMU). Performing continuously precursor analyses started in 1993 as part of the permanent evaluation of the operating experience of the German NPPs. Events with a probability for hazard states higher than E-06 per year are classified as precursors. This probability does not take into account

accident management (AM) measures. The analyses are limited to Level 1 PSA.

Objectives of the precursor analyses are to quantify the safety significance of operational events and to check their relevance for other NPPs. For safety significant events with generic importance, so-called Information Notices are being issued. The results of the precursor analyses are presented in annual reports.

### 3.2.5 HUNGARY

All safety-related operational events reported by the Paks NPP to the Hungarian Atomic Energy Authority (HAEA) are subject to PSA-based event analysis. These analyses are performed in the frame of a precursor event analysis program that started in 1999. The event analysis framework used by the U.S. NRC in their ASP program has been adapted and further developed for this purpose. A computerized event evaluation system supporting such kind of analyses has been developed. The scope of the event evaluation system covers all units and all plant operational states of each unit. Through calculating CCDP, the event evaluation system provides information to the authority about the risk significance of a given event, the effectiveness of operator interactions and equipment operation aimed at preventing more serious consequences, and, in addition, it supports reporting of safety-related events to international forums. The analysis covers specifically:

- evaluation of licensee event reports, selection of cases that can and should be analysed using the precursor event analysis system,

- risk-based analysis and evaluation of selected events resulting in the determination of CCDPs characterizing the event importance,

- documenting analyses and their results.

PSA-based analysis of past events is performed by NUBIKI experts for the HAEA, and a summary report of the analysis process and analysis findings is produced on an annual basis.

### 3.2.6 SWITZERLAND

The Swiss guideline ENSI-A06 /ENS 15/ formalizes the requirements for PSA applications, including precursor analysis. The guideline includes the procedure for the probabilistic analysis of the operating experience and reportable events, in particular for the calculation of the relevant risk measures, e.g. the incremental CCDP associated to the event, ICCDPEvent. The procedure includes technical aspects such as rules for treating components' unavailability and operator actions as well as documentation requirements.

The safety significance of reportable events is expressed in terms of the IAEA INES scale:

-1 > $ICCDP_{Event.}$ ≥ 1 E-02: INES 3,

-1 E-02 > $ICCDP_{Event.}$ ≥ 1 E-04: INES 2,

-1 E-04 > $ICCDP_{Event.}$ ≥ 1 E-06: INES 1,

- 1 E-06 > $ICCDP_{Event.}$ ≥ 1 E-08: INES 0.

### 3.2.7 UKRAINE

Starting in 2009, a quantitative assessment of the Ukrainian NPPs´ operational events using probabilistic assessment is carried out by SSTC NRS. Assessment of operational events is performed in Level 1 PSA models of the VVER-1000/320 for initiating events at the nominal power level as well as at a reduced power level and in shutdown states developed specifically to address objectives of the Ukrainian regulatory body. Using the precursor analysis allows the creation of a set of current engineering and deterministic methodologies for assessing operational events. The results of the precursor analysis are presented in the R&D reports named "Prompt and Detailed Analysis of

Operational Events at Ukrainian NPPs" which are developed twice a year.

## 3.3 Post-Events Analysis Using PSA

In addition to the precursor program, which is a post-event analysis with PSA insights, PSA can be also used during the management of the actual events or to assess technical or operational changes to overcome shortcomings made evident by the event occurrence. This type of evaluation allows risk-informed decision-making (e.g. identification of the safer plant state during an event) and/or the identification of plant improvements (a posteriori). Some relevant experience is reported in the following paragraphs.

### 3.3.1 CZECH REPUBLIC

Whereas the precursor analysis project described in paragraph 3.2.2 represents a systematic effort of the Czech regulatory body, the Czech NPPs have also employed PSA models on an ad-hoc basis in response to potentially safety important events where the plant had been shut down for long periods (in some cases for many months). In most cases, the events analysed within PSA were found not to represent any significant risk. An example of such an event was the loss of service water piping buried in the ground outside plant buildings, where several months and significant resources were spent on the replacement of the piping. This led to events connected with equipment failures (thus, with randomly occurring changes of plant equipment configuration) being analysed directly with offline risk monitors installed at Czech NPPs. A good example of such an activity was a large project for the special control of the quality of welds on the piping of safety important systems carried out for all four units (beyond the scope of regular planned piping control) and connected with many changes of plant equipment configuration.

Plant PSA models designed for the analysis of such cases involve the use of events which do not represent equipment configuration changes, rather it is a kind of finding, which may question the results of previous analytical efforts and the assumptions adopted. It can be found on the basis of the thermal hydraulic analysis, for example, that the time window for some prescribed operator action is significantly shorter than expected before. A real example from plant operation was the case when the new thermal hydraulic analyses provided evidence that some heat exchangers may not have capacity for sufficient heat removal from the frontline safety systems. Here, the PSA model was used to model and quantify the consequences of the scenario when heat removal was unsatisfactory.

### 3.3.2 FRANCE

In addition to the precursor program, which is a post events analysis with PSA insights, PSA can be also used during the management of some real events.

**LE BLAYAIS – 1999 – FLOODING**

The PSA was used by the IRSN crisis team to better understand the accident sequence development and to propose adequate mitigation measures to reach and maintain a safe reactor state.

**CRUAS – 2009 – LOSS OF HEAT SINK**

In the 1990s, based on PSA results, a beyond design emergency operating procedure has been added on French pressurized water reactors (PWRs) to manage loss of heat sink initiating events. The procedure uses the thermal inertia of the refueling water storage tank (RWST) water as an emergency heat sink for temporarily cooling the component cooling water system (CCWS), throughout a CCWS/CCS (containment cooling system) heat exchanger).

This procedure was applied for the first time in France during a loss of heat sink event that occurred in the NPP Cruas; Unit 4 in December 2009 (heat sink clogging by biological materials on the river). The procedure proved to be effective to avoid an aggravation of the situation.

### 3.3.3 GERMANY

In selected cases PSA is used in Germany for the assessment of technical changes or changes in the operation of the system and for the safety related classification of findings from events important to safety. A few examples are provided.

- Example 1: Small leakage of a 110 kV oil cable between offsite power transformer and switchgear of a NPP with no need for instant repair

In case of such an event there are two possible strategies for recovery:

- Strategy 1: No replacement of the defect cable piece with the risk of a need for repair during power operation;

- Strategy 2: Replacement of the defect cable piece during the next outage with some additional risk-increasing circumstances (no automatic activation of offsite power via the 110 kV connection possible).

For these two strategies the time dependent risk has been evaluated by modelling and quantifying both alternatives in a PSA model. The result of the comparison showed a better risk profile for strategy 2.

- Example 2: Sealing leakage of an intermediate cooling pump of the residual heat removal (RHR) system with an increased risk of later pump failure later

Again, two alternative strategies are possible for corrective actions:

- Strategy 1: Conduct immediately a precautionary repair measure for the intermediate cooling water pump with a defined unavailability of four days, with the result that it could then be assumed that the previous level of reliability for the intermediate cooling water pump can be recovered.

- Strategy 2: No precautionary repair measure for the intermediate cooling water pump, with the result that an increased failure probability up to a total failure of the intermediate cooling water pump at a corresponding request cannot be excluded.

Assuming a more significant degradation in the level of reliability of the intercooling water pump to a potential total failure on a request to the next periodic testing, the evaluation via PSA modelling showed that strategy 1 (immediate implementation of the repair measure) is favorable with regard to nuclear safety.

### 3.3.4 HUNGARY

As described in paragraph 3.2.5, a full scope precursor analysis program ensures PSA based evaluation of safety related events experienced at the Paks NPP. These analyses result in quantitative risk importance measures and yield qualitative insights into the risk significance of past events. As an example of the results, Figure 3.1 shows the distribution of risk importance (RI) of past events for years 1999 to 2017 as assessed by PSA-based event analyses.

Risk importance is defined as follows in Figure 3.1:

$$RI = \begin{cases} \text{CCDP" for initiators} \\ \text{CCDP-NCDP" for unavailability} \end{cases}$$

Where:
CCDP is the conditional core damage probability considering the occurrence of an event,

NCDP is the nominal core damage probability calculated by the nominal PSA model for the duration of an unavailability type event without assuming the occurrence of the event being analyzed.

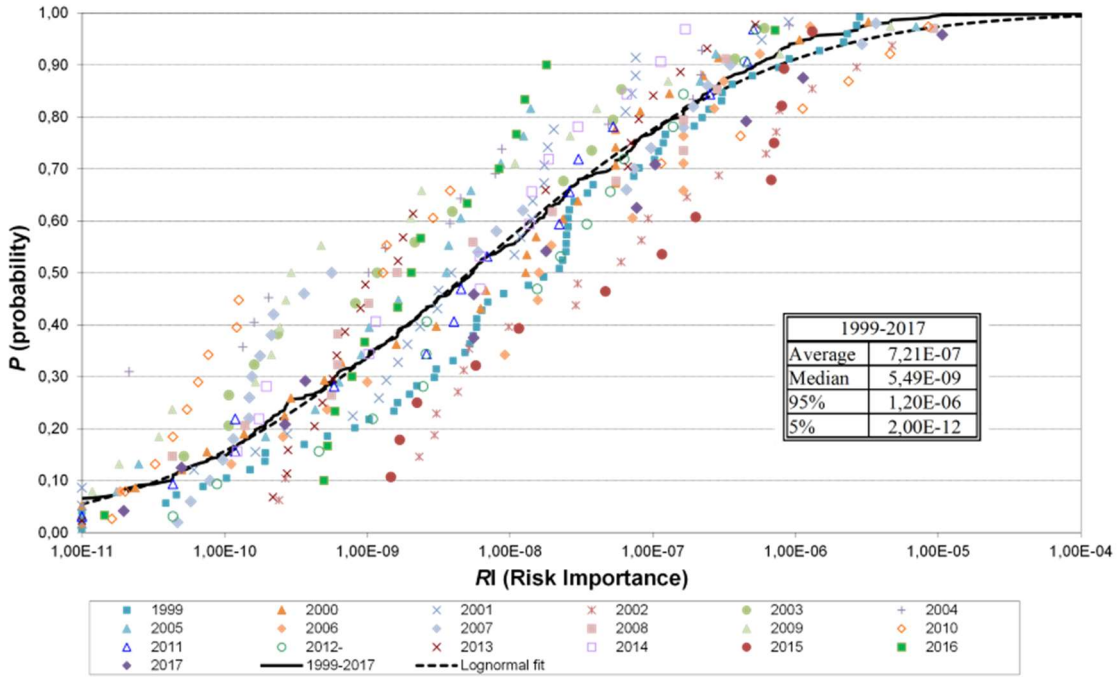


*Figure 3.1 Probability distribution of the event importance for the Paks NPP (1999 – 2017)*

The PSA based analysis of past events performed by NUBIKI for the HAEA is retrospective in nature so that the past events are analysed after collecting event reports for a pre-defined period of time, typically a quarter of a year. However, the responsible members of HAEA may decide to order prompt analysis if seen necessary due to the assumed safety significance of an event. These prompt analyses can help the authority to communicate risk information with the licensee in relation to an event using support from PSA. Some recent examples of such prompt analyses are as follows:

- Unplanned unavailability of 1 out of 3 diesel generators at Unit 4 due to repair in its oil lubrication system;

- Unplanned reactor scram at Unit 3 during online maintenance;

- Unavailability of a motor-operated valve for more than 24 hours in the fire suppression sprinkler system of an electrical room at Unit 4.

- In addition to the use of PSA based event analysis by the HAEA, the application of quasi-online risk monitoring has been in place at the Paks NPP since 2016. This enables keeping track of the operational events on a daily basis, evaluating them from risk point of view, and also reporting the evaluation results to the decision-makers, if seen necessary. Lately, risk monitor has been applied amongst others to reduce outage risk by evaluating and comparing different outage scenarios from risk point of view. The risk of the planned maintenance schedule is evaluated 90 days and 60 days prior to an outage, and modifications are proposed in an attempt to optimize the sequence of the different maintenance tasks. The actual maintenance schedule is also evaluated with the risk monitor after the maintenance activities have been

completed. This analysis helps to reduce the risk significantly during plant outages.

## 3.4 Past Events Informing PSA

Data and knowledge underlying the PSA (type of initiating events, initiating events frequencies, reliability data, HRA, etc.) are typically based as much as possible on operating experience. The occurrence of some events may highlight aspects which then may lead to the evolution of PSA, for example, new initiating events, new SSC failure modes, specific plant behaviour, enhanced human error modelling, new human errors, etc. Some examples are presented in the following paragraphs.

### 3.4.1 BELGIUM

In 2013, the Tihange NPP, Unit 3 experienced an event of loss of the normal compressed air system. The real event showed the consequential loss of the normal feedwater system although this dependency between the normal compressed air system and the normal feedwater system had not been identified during the development of the PSA model. This event was assessed by PSA event analysis as a major precursor. The PSA model was modified to incorporate this dependency.

### 3.4.2 CZECH REPUBLIC

In Czech NPPs, the plant operational history is systematically analysed and recorded by the utilities. Every five years, a complete up-date of PSA parameters is carried out by UJV Řež as support organization on the basis of recorded information about component failures and initiating events or precursors of them. Each individual safety important event is discussed between PSA data specialists and plant engineers to make a decision on whether it is a real "full" event, a precursor of an event, or an event which does not represent a real component failure modelled within the PSA. A very important and sometimes non-trivial part of the analysis is linking the event analysed to an adequate component failure mode.

For the important standby safety frontline systems, most of the events are related to component failures during tests, whereas the failures recorded for operated systems represent real operational events. There are also a few events recorded which may not fit some system boundaries and may contribute to initiating event frequencies. The CCF potential is searched for in the analysis of the events recorded from time to time and taken into consideration when CCFs are quantified within PSA. Events from all plant operational regimes are recorded and used in PSA based on the same rules and methodology.

A typical area of events recorded (both during tests and in operation) are failures of control valves on the feedwater piping lines to steam generators. Plant specific statistics are sufficient to quantify corresponding PSA basic events i.e. just based on plant specific data. In many other cases, plant specific data (numbers of failures) are not comprehensive enough and Bayesian approach combining plant specific and generic data is used for quantification of PSA parameters.

### 3.4.3 FRANCE

Generally speaking, operating experience, including real events having occurred in the past, are the basis for assessing PSA data (reliability data, initiating event frequencies, CCF parameters, etc.). However, some events had an important impact on PSA, resulting in taking into account new initiating events or to better evaluate the frequency of previously hypothetical initiating events considered in PSA such as:

- Loss of heat sink events:
In 2009, the Cruas NPP experienced a total loss of heat sink of one reactor unit and

partial loss of other units. The "total loss of heat sink" initiating event frequency, which was previously evaluated by expert judgement (about E-05 /ry), was then revaluated to take into account this event (E-04 /ry). This revaluation had an important impact on all French NPP PSA results and insights.

- Loss of 6,6 kV busbars by a CCF event:
In 1990, one Cruas NPP unit experienced a total failure of one 6.6 kV safety busbar, the second one being also affected by the same cause (potential CCF). Following this event new initiator "6.6 kV safety busbar CCF" was included in all PSAs. PSA results and insights showed the necessity to study safety improvements to cope with such situation, given that all safety systems are unavailable in case of this event. Consequently, several design and operational modifications were performed to prevent seal LOCA, to ensure cooling by steam generators and to ensure minimum instrumentation and control (I&C).
- Two events of small breaks at the reactor heat removal system occurred (Gravelines NPP in 1995 and Civaux NPP in 1998):
The LOCA frequency during shutdown states, previously evaluated by expert judgement (no operating experience available) was re-evaluated to consider these events. PSA results and insights showed the necessity to study safety improvements to cope with such a situation. Consequently, design and operational modifications were performed to ensure improved inventory management in shutdown states (automatic primary make-up).

### 3.4.4 GERMANY

Operating experience is one cornerstone of PSA to be considered properly. In the following, two examples for operational events are provided which have been analyzed within the low power and shutdown (LP&SD) PSAs performed by GRS:

- Actuation of emergency core cooling (ECC) signals during level lowering for mid-loop-operation or during mid-loop operation:
Several events have occurred at German PWR type NPPs. The inadvertent actuation of these signals led to the interruption of the residual heat removal, flooding of the reactor cooling system (RCS) with the RHR-pumps, feeding with the extra borating system and pressure increase in the RCS. This initiating event yields the highest contribution (5.1 E-06 /ry, 76 %) to the overall probability for hazard states in the LP&SD PSA.

- Drop of an ultrasonic testing device (400 kg) into the gap between reactor pressure vessel (RPV) and the biological shield of a boiling water reactor (BWR) plant. The device fell 6.7 m and hit a nozzle (DN50) at the RPV. Calculations showed that a rupture of the nozzle would have been possible in case of a slight pre-impairment of the tube. Thus, tube ruptures at the RPV above and underneath the core are investigated in the LP&SD PSA.

### 3.4.5 HUNGARY

A Living PSA program has been introduced in the Paks NPP in accordance with the recommendations of the national regulatory PSA guide. PSA models, input data, results and documentation are updated annually in this program, as necessary. The updates include internal reviews of the analysis methods and assumptions at least for those parts of the analysis that were modified. Maintaining the Living PSA program seems essential to continuously improve PSA quality and strengthen the basis for PSA applications. One of the most important drivers of the annual update is the consideration of operating experience. Examples on feedback from operating experience to plant PSA are:

- Update of component reliability data and initiating event frequencies (less frequently than annual updates);

- Lessons learned from PSA based analysis of operational events;

- Experience with the use of the plant risk monitor;
- Operational events triggering further in-depth risk analyses:
- Rigorous search for and risk quantification of interfacing system LOCA scenarios;
- Icing at the water intake facility;
- Low Danube river water level;
- Blockage of air intake systems to the demineralised water storage tanks (e.g., by birds or snow);
- Potential nitrogen ingress into primary circuit due to leakage through isolation valves of core flooding hydro-accumulators.

# 4 Lessons Learned from the PSA Review Process

The experience of TSO when performing the review of PSA led to the identification of the lessons learned shared in this section. The role of a TSO in that context is specific and the TSO is often confronted with particular challenges (e.g. due to a lack of resources to develop its own PSA, due to bias in its vision of the operational reality, etc.). The TSO therefore has to develop its own way of working in order to motivate progress in PSA and the use of this tool (in its own company and at the utility side also).

## 4.1 General Experience from PSA Reviews

Excellent knowledge of the technical systems, operational practices and procedures, including recent developments and operating experience is an obvious prerequisite for a meaningful review. Close interaction with non-PSA experts, e.g., with plant inspectors, developers of procedures, training instructors, thermal hydraulics specialists, systems design specialists (including I&C), internal and external hazards specialists, etc. is essential.

### 4.1.1 BELGIUM

In PSA development and review there is still some subjectivity, e.g., in event tree development, human reliability analysis (HRA), or with respect to external hazards. For better credibility of the PSA results, the independent reviews are highly important. Moreover, reviews in parallel with the process of performing a PSA (in this document called simultaneous review) seem to be more efficient than a review process after the PSA has been completed (follow-on review). In case of a simultaneous review, a formal interaction process should be implemented between PSA developers and PSA reviewers.

In Belgium, the review of PSA by the TSO is mostly performed simultaneously to the PSA development. This allows the regular incorporation / consideration of the BEL V comments (formulated on the first deliverables received from the utility and its architect engineer, which develops the PSA). Interactions with BEL V plant experts within the context of PSA review are necessary to have a better insight into the operational practices and to have access to the plant documentation (operational documents). Collaboration with non-PSA experts is also desirable (especially within the context of the review of Fire, Flooding and Seismic PSA, for which the opinion of specialists in the different hazards is of significant use).

The development of a PSA model by reviewers, independent from the analysts performing a PSA is obviously an appealing approach. However, the development of full scope PSA by reviewers requires significant resources and can be affected by budget

constraints. Limited developments, focused on areas of interest, can provide valuable help to the review process.

### 4.1.2 CZECH REPUBLIC

The review process is organized in close cooperation between the PSA team and plant experts. A Living PSA project is ongoing since 1998, covering new activities and each year focussed on addressing all plant changes, as well as methodological and data development. Detailed independent review of all updates of PSA documentation is carried out by plant specialists. In addition, IAEA PSA review missions are organized occasionally (the last one was organized for the Dukovany NPP in June 2016).

### 4.1.3 FRANCE

It is noted that in France the situation is specific: the reference PSAs are developed by the licensees (according to the French Basic Safety Rule). IRSN, the TSO of the French Safety Authority (ASN) develops its own studies (sometimes with a limited scope), which are very useful for the review of the licensee´s proposals and moreover to identify additional safety issues.

EDF as the licensee presents Level 1 and 2 PSA results mainly to demonstrate that the NPP´s safety objectives are met. IRSN performs the reviews of these studies, mainly during the Periodic Safety Reviews (PSR) or, for new reactors, during the different licensing steps. During the PSA review, IRSN also uses its in-house developed PSA for comparing the PSA results and insights as well as a tool for performing sensitivity studies. The PSA approaches, methods and assumptions may differ between the PSA conducted by IRSN and EDF; however, there is a progressive convergence of views on different issues. As an example, for severe accident management, several severe accident provisions have been justified by Level 2 PSA (material hatch access reinforcement, instrumentation, containment isolation electrical supply, base mat reinforcement, water access to cavity, reactor coolant system (RCS) safety valves´ modification, etc.) resulting from EDF or IRSN conclusions.

### 4.1.4 GERMANY

In Germany, performing PSAs in the frame of PSRs is mandatory by the Atomic Energy Act considering the German PSA Guideline and its supplements /FAK 05/, /FAK 05a/, and /FAK 16/. The specific German situation is that the local state ("Länder") authorities are responsible for the supervision of the safety and security of German NPPs. PSA reviews are conducted by German technical expert organisations (e.g., the TÜV) on behalf of the respective local state authorities.

However, on behalf of the Federal German authority, the Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection (BMUV), GRS has performed comprehensive comparative evaluations of recent PSAs for all those German PWR and BWR type NPPs which were still in commercial operation in order to provide generic findings and review aspects.

Generic aspects found for Level 1 PSA mainly concern the safety assessment of the SFP, the consistent use of emergency measures, in particular for low power and shutdown phases, the spectrum of initiating events for low power and shutdown plant operational states (particularly leakage incidents) as well as the neglect of initiating events.

With respect to (single and combined) hazards, the generic aspects mainly concern the need for enhancing PSA models in order to assess the risk resulting from internal and external hazards respectively.

For Level 2 PSA, the most relevant generic aspects are related to missing discussions of combustion-caused damage to venting

systems and failures of the venting filter, to realism versus conservatism of the analyses, and to considerations concerning a general metrics in order to better characterize Level 2 PSA results.

Moreover, focused PSA studies have been conducted either additionally to the full PSA mandatory as part of PSRs or on a case by case basis beyond the scope of the PSR in order to address specific issues. Predominantly these issues are related to plant modifications or changes in the plant operation, or to the assessment of events relevant to nuclear safety having occurred during operation. A methodology for determining the effect of a given issue on the PSA results by means of a screening process allowing to identify the affected areas of the PSA has been derived and provided in a Technical Supplement /FAK 18/ to the German PSA Guide Both, time independent considerations, e.g. for plant modifications, as well as time-dependent considerations typically concerning temporary measures, are addressed in that document. The proposed methodology is demonstrated by some examples.

### 4.1.5 HUNGARY

According to the regulatory requirements for PSRs to be performed by the licensees every 10 years, a PSA review within PSR is mandatory in Hungary. The review is conducted by the licensee, and the adequacy of the review and its findings are evaluated by the regulatory authority (HAEA) as part of reviewing the licensee submissions for PSR. The latest PSA review within PSR was performed in 2017 for the Paks NPP. In conclusion, improvements were found necessary and thus prescribed by the HAEA to extend and improve the Paks PSA for external hazards, to model and to quantify the effects of post-Fukushima plant modifications in PSA and make advancement in the applications of PSA at the plant to support risk-informed decision-making.

It is also required by the regulatory authority to maintain the PSA of a plant up to date. This requirement is fulfilled by operating a Living PSA program for the Paks NPP. The PSA models, results and documentation are updated annually by the licensee. This update assumes an internal review of the plant PSA every year. The updated PSA (PSA models and documentation) is submitted to the HAEA for information every year. In addition, the summary report of the PSA is part of the Final Safety Analysis Report of the plant, which is also annually updated.

Over and above PSRs and Living PSA, the HAEA sometime performs independent regulatory reviews of PSAs. These reviews are usually made by an expert team composed of internal experts of HAEA and hired external subject matter experts. The purpose of these reviews is to assess PSA quality and credibility of PSA results and conclude on the applicability of the PSA in risk-informed decision-making. The Level 1 PSA of Paks for full power operation and, separately, for low power and shutdown modes has been subject to such reviews. The Level 2 PSA for the Paks NPP has been reviewed by a team of international experts from the European nuclear safety authorities and their TSOs.

### 4.1.6 SWITZERLAND

PSA reviews are conducted in the context of the PSR process, as well as for resolution of specific issues, e.g. follow-up on PSR issues and for evaluation of PSA and plant changes as prescribed by the Swiss Guideline addressing PSA applications /ENS 15/.

The three Swiss operating NPPs feature full scope, detailed, Level 1 and Level 2 PSAs, addressing full, low power and shutdown modes and all initiating events, as required by the Swiss Guideline ENSI-A05 /ENS 19/. Accordingly, the PSA review itself entails a detailed assessment of all PSA aspects, combining knowledge of PSA methodologies as well as of plant design and operational details.

The software implementation of the PSA is included in the licensee submission, and it is in the scope of the review. Access to the software implementation often eases the understanding of implementation details that may not be sufficiently clear from the PSA documentation.

PSA reviews are generally conducted after the PSAs are released, i.e. not during the PSA development. In a few cases, typically those involving use of novel methodologies, a preliminary review of the proposed methodology is performed before its implementation in the PSA.

#### 4.1.7 UKRAINE

The PSA development process should be based on a unified industry-wide methodology. The PSA methodologies developed and used for Ukrainian NPPs differ in various aspects, for example, in the assumptions for accident sequence analysis, pre-plant operational state grouping process (different number of plant operational states), or fire compartments identification (for low power and shutdown Fire PSA). Moreover, different PSA codes (RiskSpectrum® and SAPHIRE®) are used by different NPPs in Ukraine, which makes the review process more difficult.

#### 4.1.8 UNITED KINGDOM

Full scope PSAs performed to modern standards are needed to ensure the real risk has been properly quantified and to be useful as a design tool; experience after updating some PSAs for NPPs in the United Kingdom was that the modern PSAs revealed gaps that had been previously missed using a simpler approach.

This concurs with the United Kingdom regulator's experience from the recent Generic Design Assessment (GDA). ONR has recently issued some guidance for future GDAs of new NPPs which includes their lessons learned from the three previous GDAs in the main technical areas including PSA. ONR states in its Technical Guidance for the GDA /ONR 19a/: "Partial scope PSAs do not provide the full picture of the risk and distort the risk profile and importance of SSCs. Any decisions made with a partial scope PSA (such as design modifications) may not be optimal."

In the United Kingdom, the regulatory expectation for new NPPs is that a full scope Level 1 to 3 PSA that assesses the risk to both public and workers be produced. The assessment of the Level 3 PSA requires an understanding of both PSA principles and those of radiological protection and the differing approaches usually applied in these areas – best-estimate and conservative respectively – need to be reconciled.

## 4.2 Reviewing Level 1 and Level 2 PSA

In most countries developing PSA, Level 1 and 2 PSA are required in the licensing process: However, in the past, only Level 1 PSA has been conducted for many operating NPPs. Developing Level 2 PSA requires more resources than developing Level 1 PSA (due to less accessible data, different computational codes, etc.). This has led over time to more applications of Level 1 PSA for design improvements. Moreover, the Safety Reference Levels (SRLs) by the Western European Nuclear Regulators Association (WENRA) emphasize the importance of preventing nuclear accidents. This somehow gives priority to the use of Level 1 PSA for improvements of the design and of operational practices, leading to more recommendations from Level 1 PSA results than from Level 2 PSA for upgrading design and operational practices.

The usual degree of resolution for system failures is sufficient for Level 1 PSA, but correctly processing such sequences in Level 2 PSA is not easy. This may, for example, affect considerations regarding reparability of systems or considering available

resources for severe accidents´ mitigation (the problem of modelling (in)sufficient resources is significantly more related to Level 2 scenarios).

In Level 1 PSA, the core damage frequency (CDF) is a well-known and universally accepted risk metric. (It should however be noted that discussions are ongoing, e.g. on risk metrics to be defined for multiple units or for SFP accidents and how to interpret the CDF in these cases). In the frame of Level 2 PSA, no unique risk metric has been agreed and widely accepted. Instead, the release category frequencies are mostly used as Level 2 PSA results – often with not always satisfactorily specified attributes such as "large" or "large early" releases. Source terms with different lists of contributing isotopes and different metrics (e.g., fractions of core inventory, or radioactivity) are also used. It seems that the endorsement of a universal risk metric (e.g. "total risk" [...] defined as the release frequencies times [1/a] the release consequences [Bq or mSv]) could promote the application of Level 2 PSA. Such an approach has been recommended in the ASAMPSA_E project documents (see http://asampsa.eu/, /DEC 17/ and others). Some PSAs in Germany have come up with such a figure applying it in case of assessing plant modifications.

One way of addressing this issue is to perform a Level 3 PSA; this can derive a value for the individual risk (e.g., the total risk of fatality from early and late effects of exposure) to a member of the public or a worker. This would combine the risks from multiple sources and from early and late releases into a single value for comparison to a target. However, the value of the risk determined will depend on many assumptions and, for a fair comparison, the assessment should be performed on the same basis as that is assumed in the target. Such assumptions include:

- Selection of the individual for whom the risk is calculated (ICRP-101 /ICR 06/);

- Assessing the dose of the representative person for the purpose of radiation Protection of the public (ICRP Publication 101a, Ann. ICRP 36 (a) /ICR 06/) provides guidance on selection of the representative person which is not the most exposed individual but about the 95th percentile);

- Whether implementation of countermeasures (evacuation, sheltering, stable iodine tables, food bans, etc.) can be credited or not;

- Exposure pathways to include and integration time for the dose from deposited activity.

Severe accidents at NPPs have the potential to affect many more than one individual and may lead to other consequences such as economic losses from contamination of land and property. There are also non-radiological consequences on people evacuated such as disruption, stress etc. These impacts may need to be captured by other targets.

For example, the United Kingdom's regulator ONR uses five numerical targets against which the PSA results are compared; these are described in ONR's Safety Assessment Principles (SAPs) and outlined below.

- Target 7 for individual risk for a member of the public;

- Target 9 is a societal risk target – it is a frequency target for the total frequency of all events leading to more than 100 total fatalities.

- Target 8 is a semi-probabilistic target – it is set in terms of a series of targets for the total frequency for events leading to an off-site dose in a series of dose bands. The dose is for someone directly downwind and so the probability of the wind being in the given direction is not considered.

- Targets 5 and 6 are for workers and are similar to Targets 7 and 8 above.

A simplified approach avoiding the need for a full Level 3 PSA – i.e. something between a Level 2 and Level 3 PSA – but still addressing the problem with Level 2 PSA targets discussed above might be to just have a semi-probabilistic target (actually a series of targets) similar to Target 8 above.

### 4.2.1 BELGIUM

For PSA applications, Level 1 PSA offers more opportunities (applications based on CDF, importance measures, etc., using one single tool/code) than Level 2 PSA (applications are based on release frequencies, etc., often using another tool/code and a Level 1 / Level 2 interface which is not fully automatic). The licensee is therefore often not willing to invest as much effort in Level 2 PSA as in Level 1 PSA.

### 4.2.2 CZECH REPUBLIC

The trend in the Czech Republic is the development of one common integrated plant site Level 1/2 PSA model covering all plant operational states (POSs) and all types of risk sources (both reactor core and spent fuel pool versus all internal events, internal and external hazards). The development of this model is supported both by thermal hydraulic analyses for Level 1 PSA and by severe accident scenarios analyses for Level 2 PSA.

In the Czech Republic, specific guidelines have been developed by adopting IAEA documents such as SSG-3 /IAE 10/ and /IAE 24a/ for Level 1 PSA, or SSG-4 /IAE 10a/ for Level 2 PSA), which are being used to address the scope and quality of PSA in general. There are also inputs from the methodology developed for PSRs, where PSA forms a standalone area.

### 4.2.3 FRANCE

In France the review of Level 1 and Level 2 PSA is performed by applying similar approaches with a similar level of detail. In fact, the review of the PSA by the licensee (EDF) is performed mainly during the PSR and integrates the Level 1 and Level 2 PSA, even it is performed by two different teams. The importance of different aspects is always assessed by taking into account the importance for both core damage and releases. Similarly, the development of the IRSN in-house Level 1 and Level 2 PSA is performed by close cooperation between the Level 1 and Level 2 PSA teams.

For the internal events Level 1 PSA, IRSN performs its review mainly based on the French PSA Safety Rule /RFS 02/. Additionally, international guidelines (IAEA, EPRI, etc.), are used. In order to gain experience and benefit from the review, internal review guidelines for specific PSA (internal events, hazards such as fire, flooding seismic) are also developed and updated periodically. For Level 2 PSA, guidance or state of the art are often general and not dedicated to a NPP; some efforts have been made (see ASAMPSA 2 project /RAI 13/) to develop technical guidance. Nevertheless, it appears that independent studies are needed to build an argued opinion on Level 2 PSA.

### 4.2.4 GERMANY

According to the German Atomic Energy Act, PSA is mandatory to be performed for operating NPPs at least in the frame of the PSR. The high level "Safety Requirements for Nuclear Power Plants" /BMU 15/ require in Chapter 5 to conduct as supplement to deterministic safety assessments in the frame of the safety demonstration. This is clearly stated: "Deterministic methods as well as the probabilistic safety analysis shall be applied to demonstrate that the technical safety requirements are fulfilled." In addition, the "Interpretations of the Safety Requirements" /BMU 15a/ provide the information that the PSA scope and objectives are given in the German PSA Guide and its Technical Supplements on PSA methods and data /FAK 05/, /FAK 05a/ and

/FAK 2016/ and in line with international requirements from WENRA and IAEA.

For the most recent PSAs conducted for German NPPs, the cope of PSA to be conducted in the frame of PSRs covers Level 1 PSA for power operation as well as low-power and shutdown modes (covering the spent fuel pool) for plant internal events as well as for single and combined internal and external hazards identified relevant to the site and plant investigated. As a result of insights from the reactor accidents of Fukushima, PSA for single and combined hazards have been significantly extended and enhanced in Germany. The scope of Level 2 PSA is limited to plant internal events for power operation. Traditionally, such a PSA has been performed for each single NPP unit. However, multi-unit aspects have been addressed in the more recent PSAs, which also cover a broad spectrum of single and combined external and internal hazards in line with /IAE 24/ and /IAE 24a/.

According to the guidance provided in the above-mentioned documents, the main objectives of PSA are:

- "*to demonstrate that the NPP design of items important to safety is balanced*,
- *to assess the effect of modifications of structures, systems, and components (SSC) important to safety, measures taken, or the plant operating mode on the results of the analyses, in order to ensure that the risk is not increased by such modifications.*"

The PSA needs to be reviewed by the regulatory body in charge of the "Land" (a federal state inside Germany), supported by experts from the TSO(s) to check that the objectives are met and that potential deficiencies in the plant and its operation have been addressed.

Based on the PSA review results and recommendations, plant modifications may be necessary either before the next PSA is conducted in the frame of the PSR or earlier depending on the relevance of the identified deficiencies for meeting the safety goals.

Moreover, PSA is a possible means to supplement deterministic safety assessment in case of observations and findings either from safety assessments or from events with relevance for nuclear safety observed from the operating experience and applicable to the plant under investigation. Explicit guidance on the approaches for probabilistic analyses apart from the PSR is provided in the Technical Supplement on "PSA Applications Outside Periodic Safety Reviews" /FAK 18/. Such analyses, often not representing a full scope PSA but comparative analyses specifically performed to support the licensee as well as the regulator in the decision-making which plant modification may be preferrable, have been conducted, mainly on a voluntary basis, and are agreed on between the NPP licensee and the regulatory body and its TSO in charge on a bilateral basis. The review results have, to some extent, been used for risk-informed and/or performance-based modifications in the plant design and/or changes in the plant operation. The resulting requests by the licensees require a re-assessment and comparison of the PSA results for the requested modifications/changes to the original PSA results, which again need to be reviewed for a risk-informed and/or performance-based decision-making.

German PSAs apply the pertinent German PSA Guideline with the supporting technical documents on PSA methods and data /FAK 05/, /FAK 05a/, /FAK 16/, which recommend some methods and data as applicable but do not prescribe to use only these. Nevertheless, there is a significant variety of approaches in the PSA performed for different plants. In general, the quality is adequate, but there may be single deficiencies in the approach (e.g., hydrogen risk in venting systems, melt-through of containment bottom penetrations).

### 4.2.5 HUNGARY

The major findings from PSA reviews and recent modifications to the Hungarian nuclear safety requirements, triggered mostly by experience from the Fukushima nuclear accidents and the WENRA safety reference levels /WEN 14/, substantiate the need to further extend the scope of PSA and to improve PSA quality. Improvements are seen to be essential in the following two major areas in particular:

- assessment of external events, and
- site-level risk assessment (multi-source PSA including multi-unit aspects).

Ongoing PSA developments for the Hungarian NPPs (operating plants and planned newbuilds) can be considered as an attempt to close existing gaps in these risk assessment areas.

Another key issue addressed in PSA reviews is the use of PSA in support of risk-informed applications. It appears that, over and above the quality of PSA, the structure and flexibility of the PSA model and the associated level of modelling detail are very important factors that shape the scope and limitations of PSA applications. These factors are seen even more important when it comes to applications of Level 2 PSA as the Level 2 analyses often follow modelling approaches that are different from that of a Level 1 PSAs, and integration of the associated models into a common model useful for PSA applications may well be challenging. Improvements to the regulatory framework to further substantiate and strengthen risk-informed decision-making and risk-informed safety management are also considered important in Hungary.

### 4.2.6 SWITZERLAND

The three Swiss operating NPPs feature full scope, detailed Level 1 and Level 2 PSAs, addressing full, low power and shutdown modes, and all initiating events, as required by the Swiss Guideline ENSI-A05 /ENS 19/. The ENSI-A05 Guideline includes specific requirements addressing Level 1 and Level 2 PSA and provides the basis for the review, although the review should not be limited to assessing the fulfilment of requirements.

Besides analysing if the requirements of ENSI-A05 /ENS 19/ (e.g. in terms of adequacy of the adopted methodologies) are met, an important lesson learned from review experience is the need to focus on the resulting accident sequences. Verification of the adequacy of the different PSA elements (e.g. initiating event analysis, data, human reliability analysis) is an important task of the review; however, the review should also address the resulting "overall picture". In this perspective, it is useful to review selected minimal cut sets, or groups of minimal cut sets, and analyse the adequacy of the underlying accident representation in light of the plant system response and procedural guidance.

A good practice is to focus detailed review to risk significant elements (e.g. failure events, components, operator actions, etc.) as well as accident sequences. Focusing on risk significance ensures that eventual review issues have an impact on the PSA results and, ultimately, that the review process has a recognizable role in ensuring plant safety. A detailed review should address the modelling methodology, its application, assumptions, data as well as the complete accident sequences where the elements are incorporated. Both Fussell-Vesely (FV) and risk achievement worth (RAW) importance measures shall be used in the prioritization of the review. The review focus should not be driven by the importance from both measures together, but from one at a time because of the different risk information by the measure. Spot checks on low significance PSA elements and sequences are also recommended, especially addressing unexpected low risk contributions or changes in the risk contributions (PSA elements that decrease

their significance across different PSA updates).

### 4.2.7 UKRAINE

The trend in the Ukraine is to develop integrated models for a Level 1 / Level 2 PSA for the full scope of initiating events covering all POSs for the reactor core as well as for the SFP. These integrated models (with the exception of the one for seismic hazards) have been developed for each unit and are used for the safety analysis of Ukrainian NPPs. With the necessary adjustments these models can be further used in risk-informed applications (the pilot project is under development for the Zaporizhzhia NPP).

As a part of the plants´ safety assessment documentation, the results of Level 1 and Level 2 PSA are subject to obligatory regulatory review performed by SSTC NRS that serves as TSO of the regulatory authority. In the frame of the review all PSA technical components are analysed starting from the data collection and finishing with the final model quantification. The results of the quantification are compared to the limits established in the regulations for CDF and large radioactive release frequency (LRF) to confirm their compliance with the regulatory requirements. The review also includes the evaluation of deterministic analyses results supporting the PSA success criteria and the definition of accident sequences end states.

For an updated PSA documentation, the review focuses on the analysis of the correct consideration of plant modifications, new statistical data on initiating event frequencies, equipment reliability, changes in emergency operating procedures and accident management guides.

It shall be noted that according to the Ukrainian regulatory requirements, the assessment of plant safety related modifications shall include the analysis of modification effects on the CDF as well as on the LRF. Even though the regulations do not specifically require quantifying changes in CDF and LRF values caused by the proposed modifications, in the most cases, the operating organisation supplements qualitative assessment of modification effects on the CDF and LRF with quantitative estimates using Level 1 / Level 2 PSA models. In particular, Level 2 PSA is widely used for the assessment of modifications related to severe accident management and mitigation, such as the installation of provisions for:

- hydrogen control (recombiners),

- prevention of containment failure due to excessive pressure (containment venting),

- prevention of an early containment bypass.

With the exception of the Seismic PSA, which is currently under development, the probabilistic assessments for the Ukrainian NPPs cover the full scope of events (plant internal initiators, internal and external hazards) for all POSs and follow the general requirements to PSA scope and content specified in the Ukrainian regulations /RD-95/, KND 306.302-96 /KND 96/, NP 306.2.1412008 /NP 07/, NP 306.2.162 2010 /NP 10/. More detailed guidance for various PSA tasks (e.g., data collection, IE identification and grouping, etc.) is provided in procedures developed by the utility to ensure correct methodology application by PSA developers at different units of the plants. In addition to that the regulatory review of PSA is generally not limited to the verification of PSA compliance to the regulatory requirements but also encourages the application of the IAEA Guides SSG-3 /IAE 10/ and SSG-4 /IAE 10a/ as well as promotes the incorporation of advances in the PSA methodology. This particularly involves the extension of PSA to account for event combinations and consideration of recommendations provided by the ASAMPSA_E project documents (e.g., /DEC 17/).

### 4.2.8 UNITED KINGDOM

Regulatory expectation for new NPPs is for a full scope (all sources of activity, all plant states, and all initiating events) Level 1 to 3 PSA with results compared with numerical targets for individual and societal risk amongst others.

Recent work to extend this to Small Modular Reactors (SMRs) and Advanced Modular Reactors (AMRs) has identified similar PSA requirements for these units.

## 4.3 Assessing PSA Quality

In principle, the TSO must check whether the PSA to be reviewed conforms to the applicable regulations (e.g., adequacy, transparency). However, there are several difficulties.

There is a large number of documents and extensive experience related to regulations, rules, best practices. The TSO will of course be required to apply the local (national) guidance set by the authorities, but, in addition, it shall also consider the "state of the art" (which is difficult to define and which may be advanced since the issue of the local guidance), or consider also other relevant guidance (e.g., IAEA SSG-3 /IAE 10/, its recently published revision /IAE 24a/ and SSG-4 /IAE 10a/ and its actual revision /IAE 24b/ as well as ASME-RA-2009 /ASM 09/ and several NUREG documents). Those sources of guidance may not be always consistent, and consequently the TSO may tend to utilize a combination of the most demanding requirements. Indeed, a high level of expertise from the reviewing team is a necessary condition for the selection of the applicable documents and the best guarantee of the review quality.

In general, the TSO will have limited resources (manpower, budget, time, access to codes, etc.) which does not allow a detailed examination of whole aspects of the full PSA. It is important to define, before the review, the goals and requirements regarding review and to allocate adequate resources. However, there is no convincing way to demonstrate that a limited review process is adequate and does not miss significant issues. Significant expertise is necessary both to perform a limited review and to judge its adequacy.

Risk significance information can be used to prioritize the review effort, e.g. focusing detailed review on modelling of risk significant systems and components, and operator actions. However, experience is required to assess the adequacy of the assumptions and models underlying the low significance of the other events.

Some issues can be identified where guidance for reviewing (and to some extent also for performing) PSA is missing:

- PSA for external hazards is not always covered by sufficient guidance (Level 1, Level 2, PSA generation and review). However, at least for some external hazards such as seismic hazards, external flooding, extreme wind hazards (including tornado, hurricane, etc.), etc. guidance is available and can be found in IAEA guidance documents such as /IAE 18a/, /IAE 24/ /IAE 24a/, /IAE 24c/ and /IAE 24d/, national guidelines and their supplements, e.g. /FAK 16/, and in various reports from the ASAMPSA_E project (details see /DEC 17/) such as:

- Guidance document on practices to model and implement earthquake hazards in extended PSA, Volume 1 and Volume 2 (final version),

- D50.16 Report 2 – Guidance document on practices to model and implement flooding hazards in extended PSA (final version),

- D50.17 Report 3 – Guidance document on practices to model and implement extreme

weather hazards in extended PSA (final version),

- D50.18 Report 4 – Guidance document on practices to model and implement lightning hazards in extended PSA (final version),

- D50.19 Report 5 – Guidance document on practices to model and implement biological hazards in extended PSA (final version), and

- D50.20 Report 6 – Guidance document on practices to model and implement mans-made hazards and aircraft crash in extended PSA (final version).

- More detailed guidance is still needed for Level 2 PSA regarding the consideration of single and combined external and internal hazards (see also /IAE 24c/ and /IAE 24d/), so far mainly addressing containment and other structural elements failure. Advanced guidance for Hazards PSA should also cover Level 2 specifics.

A lot of detailed and widely recognized international guidance is available regarding the consideration of plant internal fire and flooding as single, and partly also as combined hazards according to /IAE 21/ within PSA for all POSs (see /NRC 05/, /EPR 09/, /IAE 24a/, /IAE 24c/, /IAE 24d/). On a national level there is more guidance available applied to some extent not only in the country where it was developed (cf. e.g. /FAK 05/, /FAK 05a/ and /FAK 16/).

- The expectation for PSA to be conducted for new NPPs, e.g. in the United Kingdom and France, is that all sources of initiating events are considered including internal and external single and combined hazards. Performing PSA for external hazards in the recent GDA has proved challenging for a number of reasons:

- Input from different disciplines outside the PSA area is required and needs to be coordinated to ensure the input data supplied are sufficient and fit for purpose. These include amongst others:

- external hazards to define the hazard curves for each hazard. Other than for seismic hazards – which is relatively advanced in this respect – defining design basis events for 1,000 and 10,000 return frequencies is challenging enough and is even more so for the longer return periods required for PSA,

- civil engineering and structural integrity to determine the behaviour of building and SSC under hazard loadings.

These difficulties have resulted to date in simplifications which tend to be overly conservative and distort the risk profile.

- As previously indicated, for the Level 1 internal events PSA in France, a safety rule, indicating acceptable methods for and applications of PSA, was published by the French safety authority /RFS 02/. IRSN as TSO performs its review mainly based on this safety rule. However, there are no specific formal guidelines regarding the PSA for internal or external hazards or for Level 2 PSA. These PSA are developed by EDF by using its own methodologies which are generally based on available international practices. IRSN also develops its own studies which constitute a valuable tool for reviewing the EDF PSA. IRSN PSA methods can be sometimes different from the methods used by EDF. The technical discussion may also highlight the importance of some methodological aspects and contribute to continuously improve the representativity of PSAs.

- As already briefly mentioned before, another emerging issue in PSA are event combinations of consequential, correlated or coincidental hazards, in line with the specifications provided in the IAEA Specific Safety Guide SSG-64. The most recently published IAEA Guide on Level 1 PSA, SSG-3, Rev. 1 /IAE 24a/

covers this aspect on a high level. More detailed guidance is available in /IAE 24c/, already available and recognized advanced practices can be found in /IAE 24d/.

- Multi-unit und site-level considerations in PSA have been increasingly addressed internationally in the recent past, based on internationally recognized practices. These activities resulted in an exchange of experiences from OECD/NEA/CSNI WGRISK member countries with PSA for multiple reactor units and other radioactive sources co-located at the same nuclear site /NEA 19/, followed by further international activities resulting in IAEA standards, such as /IAE 23/ and /IAE 24d/ as well as several publications (e.g., /IAE 18/, /HAG 21/ and /ROE 23/).

- Knowledge based human actions. These refer to actions not explicitly covered by the procedural guidance, but for which the PSA team may have arguments that their inclusion in the PSA will result in a realistic representation of the accident scenarios. These actions represent exceptional cases that require justification, because PSA typically addresses actions explicitly mentioned by the procedural guidance. Justification may refer to coverage of the action in the training program, but the verification of the justification during review is not straightforward because it involves assessing the differences between the training experiences and the PSA scenarios.

- Data quality: One important issue to be mentioned is the need to assess the quality of the input data of the PSA for assessing the global quality of the PSA. This issue becomes increasingly important within the context of the review of Fire, Flooding and Seismic PSA, which require a huge amount of data to be collected and processed (e.g., cable routings and orientation, pipe length, fragility curves, etc.). Conservative choices should be evaluated, and it should be checked that the final PSA does reflect the actual safety level of the nuclear installations. Performing audits during and after the elaboration of the databases could be a good method to review this aspect of the PSA.

## 4.4 Some Problematic Issues Encountered in PSA

There are a number of issues that can be encountered when performing PSA:

- PSA does not (yet) allow taking into account the effect of safety culture (this shortcoming is also true for deterministic assessments). Purely based on the design and operational procedures, a CDF can appear to be correct; however, if the safety culture during plant operation is inadequate, the "real" CDF may be (or become) much higher.

- The quality of the PSA also depends on the safety culture of the PSA producer. Despite the existence of internal procedures, quality issues can appear, and they may have an important impact on the PSA and its results (for example, if the issue impacts the data collection process). As a TSO, regular audits throughout the PSA development are useful in order to check the correct progress of the PSA project.

- Comparing quantitative results of PSAs from different "origin", even for similar plants, can be misleading.

- Even small differences in plant design or operation may affect the PSA results.

- Different PSA producers may obtain different quantitative results for an individual plant according to differences in their PSA model. For the TSO

reviewing the PSAs this is highly important for their assessment.

- PSAs often show the same order of magnitude for CDF, maybe because a certain CDF/FDF is acceptable to the reviewers, and more effort is not applied. It is also likely that because PSA tend to be pessimistic that when a result is above a tolerated range pessimism is reduced to arrive at the desired level. This may be an acceptable approach; however, it casts doubts whether PSA is applicable for identifying the real safety issues (instead of simply demonstrating compliance with a target) "risk profile".

- According to available PSA Guidelines (e.g., IAEA SSG-3 /IAE 24a/), assumptions made for PSA should be "best estimate" in order to avoid a skewed risk profile caused by pessimism. If this is not possible the influence of the pessimism applied on PSA results (importance, sensitivity measures) should be evaluated.

### 4.4.1 FRANCE

Some lessons learned from PSA used for decision-making in France are:

- In the decision-making process the PSA should be used as a guideline. The respect of deterministic criteria must prevail, and maintenance/operating aspects have to be considered (restoration feasibility in a reactor state, time needed to repair, etc.).

- The impact of the reference PSA model simplifications on its consistency with the given application has to be assessed. If needed, specific assessments should be developed.

- If the SSC analysed is also involved in hazards mitigation or has a containment function, the safety impact on these specific functions needs to be specifically assessed.

- If a SSC fails to operate or is found failed during tests the similar redundant SSC may be more likely to fail to a CCF well. When the safety impact of this failure is estimated, the conditional failure probability of the redundant SSC has to be taken into account appropriately.

- If the inoperable SSC is common to several units (e.g., site back-up diesel generator, etc.), all these units are simultaneously affected. CDF increase to be compared to the guideline criterion should take into account all these contributions.

- Uncertainties coming from inherent simplifications or assumptions of PSA have to be taken into account, for example:

- For SSC modelled in the reference PSA and not required to be operable by the Tec Specs, the probability of their unavailability has to be carefully estimated.

- For reactor states where different operating practices can be employed, the time spent in an operating configuration has to be carefully estimated, as the PSA model is developed for a hypothetical reactor, spending an average time in each configuration.

Over the last years, there was a high interest in Level 2 PSA in parallel with the reinforcement of the severe accident management strategies. This is an important part of the PSR; this is driven by the objective to bring the safety level of operated PWRs closer to the Gen III one safety level.

The PSAs for hazards are also used for decision-making. For example, the internal fire and internal explosion PSA have been used by EDF to identify the most important protection means against these risks in order to focus the inspection and maintenance. The adequacy of methods and of the PSA models (assumptions, support studies,

simplifications, etc.) must be specifically assessed for these applications.

### 4.4.2 GERMANY

For operating NPPs in Germany, Level 1 PSA principally deals with design basis issues, while Level 2 PSA addresses beyond design basis issues. Regulators were more focused on design issues than on beyond design. Therefore, the German interest in Level 2 PSA was in the past less pronounced than in Level 1 PSA. This has changed; Level 2 PSA for all POSs is now required and detailed guidance provided in /FAK 16/.

### 4.4.3 HUNGARY

In 2022 the Hungarian Atomic Energy Authority (HAEA) issued the construction license for two 1200 MWe Russian-designed PWR units at the Paks site. According to the Hungarian Nuclear Safety Code, an assessment should be performed independently of the vendor for safety analysis including deterministic analysis as well as PSA. Even in the previous pre-construction license design phase, the PSA performed by the vendor was supposed to be a full scope study, reflecting the relevant information and limitations of plant design of course. The independent PSA should have not necessarily been a full scope analysis at that stage as the major purpose of that assessment in this pre-licensing phase was to provide some support to an independent review of the vendor's PSA as opposed to developing a complete, stand-alone risk assessment study in full details.

However, a full scope independent PSA should also be developed until the operating license application is submitted. After the completion of both assessments (by the vendor and by independent analysts), the results should be compared. If significant differences are found (including the risk estimates as well as the dominant event sequences or minimal cut sets), the reasons thereof should be revealed and evaluated. Depending on the findings there may be a need to compare some analysis tasks, including event tree and fault tree analysis, input data assessment, HRA, dependent failure analysis in more depth. Either the acceptability of both assessments should be substantiated, or a consensus should be reached followed by the modification of at least one of the PSAs, as necessary. This comparison is expected to be challenging due to the different modelling approaches used by the different PSA teams, which may also give rise to numerous and serious discussions.

### 4.4.4 SLOVAK REPUBLIC

The experience (more related to the old generation of reactors) shows that there must be a close cooperation between deterministic and the probabilistic experts' team to interpret the results of deterministic analyses in the same way. (Example: deterministic codes for melt core and concrete interaction (MCCI) assume flat top surfaces – this may not be real) (Example: deterministic analysis needs a lot of specific assumptions for each single scenario – but these may not be the same scenarios which are real or relevant from PSA point of view).

PSA experience should be added to the deterministic analyses realistic aspects by more exact consideration of functional limitation and interdependency of the systems, unit configuration and operator actions.

There is a lack of analyses particularly for shutdown states in several countries, but it can be expected to be solved in the next decade. Any POS forms very specific conditions differing each from the others, e.g., the situation before refueling and after refueling.

All deterministic analyses supporting PSA should use some valid data source (common database preferred) and the same approach to set the boundary conditions (e.g., conservative, best estimate). A realistic

approach should be used. However, the scope of deterministic analyses is often limited by available resources to cope with increasing requirements from PSA side so that there is still room for expert judgement to interpret the results of envelope deterministic cases for the purpose of modelling specific conditions appearing in the event trees.

### 4.4.5 UKRAINE

Preparation of the plant to long-term operation generally involves implementation of a large number of various plant modifications, extensive maintenance, equipment repair or replacement activities requires considerably longer time than it is needed for typical plant shutdown for repairing or outage. If accounted in PSA, these extended shutdowns distort relative contribution of individual plant operation states to the total CDF and LRF, increasing the risk from shutdown and decreasing the risk from other POSs, and lead to unrealistic PSA results when the plant returns back to usual power operation and shut-down intervals. On the other hand, it does not seem correct to completely ignore that such long shutdown periods may be required.

Strictly established quantitative probabilistic criteria may become an issue for an extension of PSA scope since more and more events groups are added to the integral PSA model which certainly leads to CDF/FDF/LRF increase and may result in exceeding the regulatory limits.

Improvements in understanding of severe accidents progression and consequences, implementation of provisions to cope with these accidents at VVER type plants of older design, and correspondent evolution of Level 2 PSA models raise new questions that need to be considered by PSA analysts, for example:

- Potential failure of containment function due to vacuum in case of late containment spray actuation following use of containment filtered venting system;

- Hydrogen propagation from the containment to adjacent rooms following consumption of containment oxygen by hydrogen recombiners.

### 4.4.6 UNITED KINGDOM

In the United Kingdom there is the requirement for the risks to workers and public to be reduced to a level "as low as reasonably practicable" (ALARP); this principle applies whatever the level of risk is, and it is not sufficient to just meet the targets. This is similar to the ALARA principle but more far-reaching and is legally enforced. PSA is expected to be used to support the ALARP demonstration and it is therefore essential that the PSA results reflect the real safety of the plant.

Assessing risks to workers is difficult for a number of reasons including:

- Exposure can result even if no releases occur;

- Different categories of workers may need to be considered, for example: those directly involved in responding to the accident, maintenance workers, control room workers, other workers on site;

- For atmospheric releases, dispersion models able to deal with building effects and determine short-range dispersion are needed to calculate dose to workers on site.

# 5 LESSONS LEARNED FROM CASE STUDIES

In the following, the experience of the ETSON TSOs with PSA applications is provided by means of specific case studies

## 5.1 Belgium

*Question/Issue*

How to organize PSA review in order to ensure PSA quality for an extended use of PSA and PSA applications by the utility?

Initially, in Belgium the PSA was mainly used by the utility to demonstrate plant safety ("acceptability" of CDF, LERF, well-balanced risk contributions, etc.) and to identify and solve potential weaknesses in design or operational practices. This was often done in the framework of a PSR, during and after the development/update of the PSA. It has led to several safety improvements, either during the development of the PSA model (called "early feedback") or after the analysis of the PSA results /GRY 12/.

Nowadays, the Belgian utilities use PSA more and more for several PSA applications (e.g., precursor analysis in support of event/incident analysis (operating experience feedback, OEF), safety demonstrations of plant modifications, modifications to Technical Specifications (Tec Specs), plant configuration control, etc. /IAE 01/). This is done either on the initiative of the utility itself (in the framework of its Strategy for PSA-based applications) or because it is requested by the Belgian regulations (e.g., since the transposition of the WENRA Safety Reference Levels from 2008 /WEN 08/ into the Belgian legislation in 2011).

A PSA review by the TSO has to follow this evolution in the use of PSA. How can such a review be organized? What is the most efficient way to perform a PSA review in the Belgian context and should it be done in different ways or at several levels?

*Approach/Procedure*

The review of PSA and PSA applications have been organized at several levels:

- For the initial PSA development as well as for PSA updates/upgrades, the following combinations of review approaches are or have been used:

- a review of the PSA by Bel V, the Belgian TSO: simultaneous review during the elaboration of the scope, the methodologies and the PSA models, follow-on review when the PSA results and documentation are completed,

- a comparison with PSAs of similar (foreign) plants among TSOs, and

- a peer review against the ASME/ANS standard RA-Sa-2009 /ANS 09/, focusing on the demonstration of the technical adequacy of the PSA for risk-informed activities / PSA applications.

- For PSA applications: Bel V keeps an oversight of the PSA applications performed by the utility (procedures for PSA applications, annual meeting, annual report) and reviews results of specific PSA applications on a case-by-case basis (e.g., precursor analysis, plant modifications, etc.).

This case study focuses on insights and lessons learned from the review of the PSA (development, update, upgrade) and its evolution due to the different PSA applications.

*Results / Lessons Learned*

- Utility Initiatives: Development, Update/Upgrade and Use of PSA

After the first development (by the utility) of plant-specific PSA models for plant internal events, the utility has developed two strategy documents:

- "Strategy for PSA models development, updates and upgrades" and

- "Strategy for PSA-based applications".

A PSA update is covering the changes in plant design and operation ("implemented modifications"), plant-specific data based on the Belgian operating experience feedback (e.g., initiating event frequencies, POSs´ durations, planned testing and maintenance (T&M) and unplanned (i.e. inadvertent) unavailability of components, modified system configurations, e.g. as required by Technical Specifications (Tec Specs) or normal operating procedures), in order to assure a correct and realistic modelling of the plant under consideration.

A PSA upgrade is intended to revise/increase the scope of the PSA (e.g., additional initiating events or POSs, systems not modelled before, etc.) and to introduce improved or revised methodologies (models, assumptions, generic data, etc.), in order to assure an up-to-date state-of-the-art of the PSA.

A PSA upgrade is normally done every ten years (coupled to the PSR framework), whereas a PSA update is performed on a more regular basis (at least every five years, or in between if needed e.g. due to important plant system modifications).

All potential PSA-based applications have been prioritized (high/medium/low) by the licensee and the high-priority applications which are nowadays applied by the utility are the following ones:

- "NPP upgrade" (i.e. design improvements) following a PSA upgrade or a PSA application;

- Assessment of the adequacy of plant modifications, modifications of Technical Specifications and procedure modifications (cf. WENRA Safety Reference Levels O3.2 and O3.4 /WEN 08/, /WEN 21/), in support of the deterministic approach (on a regular basis, but also in view of long-term operation / plant lifetime extension);

- PSA-based event analysis (PSAEA) or "precursor analysis" (cf. WENRA Reference Level O3.4 /WEN 08/, /WEN 21/);

- Support to operational decision-making (e.g., risk matrix, RIF (Risk Increase Factor) monitoring).

For these PSA based applications, the utility has developed dedicated procedures. Reporting on the PSA based applications is done on a case-by-case basis (specific documents) and through an overview in an annual report.

- PSA Review by the TSO: Organizational Aspects

In Belgium, the TSO review of the PSA developed by the utility is based on a two-tier approach:

- The first tier is a simultaneous review during PSA development (focusing on methodologies, plant specific modelling for PSA Level 1 (sequence analysis / event tree

(ET) and thermal hydraulic support analysis, system analysis / fault tree (FT), HRA, appropriate generic or plant-specific data taking account of operating experience feedback, CCFs, etc.) and Level 2 PSA (interface, APET (Accident Progression Event Tree) development and quantification, etc.);

- The second tier is the follow-on review when PSA results are obtained, and all documentation is finalized, resulting in an Evaluation Report with TSO recommendations related to further improvements of the PSA model and to the interpretation of PSA results and its translation into safety improvements (modifications in design, operation, accident management, etc.) derived from these PSA results. The TSO recommendations related to further improvements of the PSA model are intended to be used during a next PSA upgrade/update. For the safety improvements derived from these PSA results (modifications in design, operation, accident management, etc.), an action plan is established and implementation at the plant is followed in a dedicated process of the plant oversight/inspections.

■ PSA Comparison (among TSOs)

After the first development of plant-specific PSA models (by the utility) and PSA reviews (by the TSO), a detailed comparison with Level 1 PSA results of similar (foreign) plants (France, South Africa) /COR 06/ showed to be most useful to define the scope of the first major PSA upgrade/update which was completed in 2011 /GRY 12/. The PSA comparison led to some of the following improvements in the internal events PSA:

- Additional or refined initiating events: loss of all 6.6 kV emergency buses, loss of offsite power (LOOP) with different recovery times (short vs long duration), very small LOCA, secondary line breaks (SLB) of different sizes, heterogeneous dilution in shutdown states, etc.;

- More detailed plant operational states for low power and shutdown states;

- Revised event trees: more transparent modelling/functional hypotheses (e.g., steam generator tube rupture (SGTR), coupled event trees for induced LOCA/SLB sequences, etc.);

- Updates of the primary pump seal LOCA model for all NPP units;

- Systematic analysis of compressed air systems for all NPP units;

- Systematic analysis of ventilation systems and modelling in PSA if needed.

■ Peer Review against PSA Standards

After the first major PSA upgrade/update in 2011, a peer review of one PSA (i.e., for a representative NPP unit) against the ASME/ANS "Standard(s) for PRA for NPP Applications" /ANS 09/ was performed by an external, independent peer review team, on behalf of the utility in the frame of a PSR based on the IAEA Safety Standard NS-G-2.10 /IAE 03/ and the Specific Safety Guide SSG-25 /IAE 13/). The results of the peer review (i.e. strengths and weaknesses of the PSA, findings and recommendations) and the use of its recommendations by the utility were also reviewed by the TSO and confronted with the simultaneous/follow-on review of the plant-specific PSA by the TSO. Examples of such mutually corroborated recommendations and finally agreed PSA improvements are:

- Use of realistic data for the unavailability of systems and/or components due to tests or planned maintenance for all POSs (instead of generic data based on theoretical frequencies and test durations);

- Removing asymmetries in the PSA models (e.g., modelling of initiating events, system configurations with running and standby components, unavailability data for redundant components);

- Verification of the identification of all potential initiating events (including, e.g., initiating events based on plant operating experience, or human induced initiating events);

- Identification and modelling of additional dependencies (diesel ventilation systems, normal feedwater as backup system, CCFs of breakers and auxiliary feedwater (AFW) pumps);

- Development of full fault tree for the containment isolation system;

- Identification and quantification of miscalibration errors (type A human errors), including CCFs;

- Implementation of a new HRA methodology for Level 1 PSA (type C actions) and a compatible HRA methodology for Level 2 PSA, to allow modelling of HRA dependencies between Level 1 and Level 2 PSA;

- Modelling of fission product retention in the nuclear auxiliary building;

- More detailed source term modelling and verification (release groups, check source terms of APET branches by means of specific MELCOR calculations).

■ PSA Review by the TSO – Technical Aspects

As mentioned above, some high-level recommendations (mostly related to scope and methodological aspects) were identified by both peer review and TSO review. Nevertheless, the more detailed technical review performed by the TSO (i.e., a review for all NPP units, using the TSO's PSA experience and knowledge of the Belgian nuclear facilities) also led to the identification of several other needs for improvement of the PSA models. Several improvements could already be implemented during the simultaneous review.

Examples of further improvements identified by the TSO for Level 1 PSA are:

- Improvements of supporting studies (e.g. a sufficiently extended set of thermal hydraulics studies to justify success criteria (used in event trees) or recovery times (needed for quantification of type C human errors));

- Re-examination of apparently optimistic HRA results (human error probability (HEP) values), e.g., due to crediting several dependent recoveries (in type C human errors) and not applying a dedicated methodology for errors of commission (EOC);

- Re-assessment of the introduction of mission times other than 24 h, for specific accident sequences and/or systems, in particular if it cannot be demonstrated that a safe end state (or at least stable plant conditions) is reached after 24 h;

- Adequate use of the available databases or references for reliability data (e.g., T-Book data /TUD 15/) or initiating event frequencies (e.g., LOCA frequencies according to NUREG-1829 /NRC 16/);

- Differentiation between POSs (e.g., differences in availability of automatic safety signals) in the modelling of accident sequences;

- Elaboration of CCF-type pre-accidental human errors related to changes of plant operating state (e.g., based on operating experience feedback).

Examples of further improvements identified by the TSO for Level 2 PSA are:

- Development of a sufficiently extended set of MELCOR supporting calculations for representative accident scenarios during the APET quantification process;

- Use of less conservative assumptions compatible with operational practices and/or Technical Specification requirements

(e.g. availability of ventilation systems considered in Level 2 PSA for buildings adjacent to the reactor building);

- Consideration of hydrogen release and combustion outside containment (e.g., in the annular space or nuclear auxiliary building) which may lead to loss of equipment used in severe accident management;

- Evaluation of structural containment failure due to excessive water weight when containment and reactor cavity are flooded using alternative water sources (severe accident management (SAM) measure);

- Improvement of the expert judgement technique (e.g., improvements of expert elicitation and aggregation of results);

- More extensive analysis of Level 2 PSA results in order to identify risk reduction options and/or plant-specific accident management strategies or measures.

- PSA Review by the TSO – Further Developments (Internal and External Hazards PSA)

For internal hazards (fire, flooding), discussions with other TSOs (GRS, IRSN) on their PSA methodologies and results have led to some improvements during the elaboration of those PSAs, e.g., an increased focus on flooding caused by stand-by systems and a more suitable justification of the means of flood detection credited in flooding PSA, a better modelling of the fire detection and suppression phase when credited in Fire PSA scenarios.

The TSO review also identified numerous conservative assumptions in the initial Fire PSA models (e.g. due to an underestimation of the resources required for the plant walkdowns and the cable routing process by the utility), leading to unrealistic PSA results (e.g. extremely high CDF contributions).

In the context of the development of Flooding PSA models, the simultaneous review by the TSO led to the identification of the need for more realistic data to assess the pipe lengths and the need for the consideration of operating experience feedback (i.e. flooding events that occurred at the Belgian plants).

At a later stage, External Hazards PSA (for seismic and external flooding events) have also been reviewed, highlighting once again the need and the challenge of introducing realistic data to obtain usable models for PSA applications and to be able to identify concrete improvement measures on the plant site.

- Insights / Lessons Learned

A review accompanying the development/update/upgrade process of a PSA (simultaneous review) seems to be much more efficient than a review process conducted only after the PSA has been completed (follow-on review). However, in case of such a simultaneous review, a formal interaction process (and a good mutual understanding of each role) is needed between PSA developers and PSA reviewers in order to adequately improve the PSA model during the development/update/upgrade process. Moreover, for a simultaneous review to be effective, a high quality of the available PSA documentation (and related presentations and discussions) is needed during the whole PSA elaboration process, while access to the PSA model itself (e.g. the RiskSpectrum® model for Level 1 PSA) is a significant additional strength, at least if such access is enabled in a sufficient early stage. Finally, access to the whole PSA model of the utility is desirable at the latest when the PSA results are provided.

The use of international guidance (e.g., ASME/ANS, NUREG, IAEA) or national guidance is still to be complemented by a more detailed technical review by individuals with good knowledge of plant-specifics (design and operation) in addition to

knowledge of PSA techniques/methodologies.

- Indeed, while the peer review against ASME/ANS standards (or any other international guidance document) allows a comprehensive review of the scope, methods, attributes and documentation of a PSA, it must still be complemented by an in-depth technical review of the PSA and its adequacy for the plant under consideration, even if the latter may be more time consuming.

- On the other hand, the complementary nature of the (peer) review by individuals with experience in the use of PSA Standards (e.g., the ANS/ASME standard RA-Sa-2009 /ANS 09/) and the more detailed technical review by experts with good knowledge of the plant specifics (i.e. the deterministic plant design as well as the recent plant operational aspects) is most beneficial for getting a global review focusing on all relevant aspects of the PSA model and on their relevancy/capability for (potential) PSA applications after PSA development.

The ASME/ANS standard RA-Sa-2009 /ANS 09/, which was endorsed by U.S. NRC (see Regulatory Guide 1.200 /NRC 09/), provides a set of well-defined requirements and criteria against which the strengths and weaknesses of the PSA are judged, so that decision-makers can judge the degree of reliance that can be placed on the PSA results of interest, and so that the applicability of the PSA for various types of PSA applications can be determined. The standard also requires a peer review process that identifies and assesses where the technical requirements of the standard are not met, and hence where further improvements of the PSA are needed.

However, before performing a peer review against the requirements of the standard, i.e. the so-called high-level requirements (HLRs), and the more detailed supporting requirements (SRs)) that are developed for the different PSA quality levels (so-called PRA Capability Categories(CCs) I, II and III), it is important to identify, as much as possible, the PSA applications for which the PSA will be used, in order to determine, during the peer review, the appropriate Capability Category to be reached for each requirement. If this is done on beforehand, the reviewers can focus on those findings and recommendations that are most relevant for a next PSA upgrade/update, in view of the intended PSA applications. On the other hand, aiming at a global Capability Category (e.g., at least CC II) for most requirements of the standard after such a peer review, or using historical lessons learned regarding some selection criteria (e.g., based on the expected impact on PSA results or on intended PSA applications), leads to a less adequate selection process of the appropriate findings and recommendations for PSA improvement.

At the time of this report, there is still a lack of a published ASME/ANS standard for low power and shutdown states and for Level 2 PSA (although the peer review team hired by the licensee had knowledge of the draft standard as they had participated in its development). Hence it was difficult to confirm/support some of peer review results, in particular for PSA Level 2 (several recommendations of the peer review team did not corroborate, and in some cases contradicted, insights from the TSO review).

The lack of a sufficiently broad range of supporting studies (e.g. thermal hydraulic studies for various accident sequences in all POSs) appeared to be a recurrent issue for Level 1 PSA when conducting HRA or for the validation of some success criteria. In the quantification of APET branches (basic events) in Level 2 PSA, a similar lack of a sufficiently extended set of supporting studies (e.g., MELCOR calculations for representative severe accident scenarios) was found. These issues could not be identified solely by the peer review based on the ASME standards, since the use of these supporting studies during PSA development needed a more detailed technical review.

PSA-based event analysis (PSAEA, or precursor analysis), performed either by the licensee or by the TSO, is most useful in the overall process of operating experience feedback (lessons learned from real events, identification of corrective actions, etc.), but is also often useful to further improve PSA models through identification of missing elements in the PSA model (e.g., missing initiating events, accident scenarios or human actions), incorrect modelling, needs for more detailed modelling (e.g., I&C systems), etc.

For instance, in 2013, a real event (loss of the normal compressed air system) in a Belgian unit highlighted a dependency between the loss of the normal compressed air system and the (induced) loss of normal feedwater, which was not correctly modelled in the PSA (i.e. the recovery of normal feedwater was erroneously considered as possible operator action). The importance of this dependency could be demonstrated by the PSA-based event analysis (implying some adaptations in the PSA model itself).

Limitations in the PSA scope (e.g., considering only plant internal events) or degree of detail (e.g. accident sequences that are not developed in further detail since it is considered that a safe end state is reached, systems that are not modelled or modelled in a simplified way because their safety importance is judged to be minor) can also lead to important limitations in applicability of PSA models for specific risk assessments and/or PSA applications (e.g. risk-informed Technical Specifications).

An example is a risk analysis in case of LOOP with success of house load operation, for which it was questioned if house load operation could be considered as a safe end state and/or for how long. Since potential accident sequences during house load operation were not developed, the risk evaluation remained indecisive.

For PSA applications, Level 1 PSA usually offers more opportunities (applications based on CDF, importance measures, etc., using the same PSA code, e.g. RiskSpectrum®) than Level 2 PSA (applications based on release frequencies, etc., often using another tool/code and also a Level 1 / Level 2 PSA interface which is not fully automatic). More-over, in Level 1 PSA, the modelling of accident sequences, systems and human actions is more elaborate, whereas Level 2 PSA is often hampered by a less detailed modelling of possible mitigating strategies, measures, equipment or manual actions, leading to a more difficult identification of possible plant improvements and risk reduction options. Hence, the licensee is not investing as much in Level 2 PSA as in Level 1 PSA.

## 5.2 Czech Republic

*Question/Issue*

The project of long-term operation justification of the Dukovany NPP beyond the planned 30 years operational lifetime is ongoing. The Czech regulatory body developed a list of conditions that the utility has to fulfil to prolong the plant operational lifetime. A number of these conditions have been connected to postulated emergency scenarios, where the utility was asked to adopt some measures for increasing safety or for justification that such measures are not necessary because of an extremely low emergency potential of the scenarios of concern. The supporting analyses were expected to be deterministic by nature, but in some specific cases, a probabilistic approach was also used in support of getting evidence about an extremely low risk contribution of the scenario.

A specific example given in this section concerns the scenario "*Unintentional closing of valves located on (all) main steam lines followed by failure of steam generator relief valves to open*", where the potential negative effect would be critical – not only "just" a loss of safety functions but destroying of

secondary circuit piping due to the effects of over-pressurization. This is a typical example of a *"very low probability and very high consequences" scenario*.

The goal of the analysis was to provide a conservative estimation of the occurrence probability for such a scenario by means of the Dukovany NPP PSA model with the aim of proving that this probability is extremely low. A sufficiently credible result of this work could justify avoiding much more expensive thermal hydraulic analyses in support of the conclusion that the safety impact of this scenario is negligible.

*Approach/Procedure*

- General Approach

The most current version of the Dukovany NPP PSA model was used for some specific points of the analysis (valid to the last day of the last year). The criterion was postulated that the scenario under concern would be found as negligible regarding safety impact, if the conservatively estimated value of annual frequency of scenario occurrence would be lower than 1 E-07 /ry. This approach was compatible with the screening criteria recommended in the official guide written and released by Czech regulatory body, which uses the ideas originally presented in the ASME/ANS RA-Sa-2009 standard /ANS 09/.

Unintentional closing of all steam line valves can be treated as initiating event in the PSA model of the Dukovany NPP. A more exact definition of such event is: closing of fast acting valves RAxxS03 or main steam valves RAxxS04 or combinations of these at all steam lines which are linked with the steam generators used for residual heat removal at the given time point (the configuration of steam generators used for cooling differs for the individual plant operation states).

Failure to open steam generator relief valves (for the given configuration of operated steam generators) could be treated as an element of plant response to the initiating event. The success criterion of plant response is defined as a success of opening of at least one steam generator relief valve.

The Dukovany NPP is a six-loop NPP with six steam generators. It can be supposed that at least three steam generators are available for cooling over all operational states. The only exception is plant operation Regime 6 where as many as four loops can be maintained. However, the supporting thermal hydraulic analyses provided evidence that the secondary circuit cannot be critically over-pressurised in this plant operation regime.

Other assumptions made were connected to the failures of steam generator relief valves to function in frame of this scenario, keeping the scenario as fully unintentional, i.e. no direct planned maintenance and test actions regarding steam generator relief valves were considered as causes. A direct effect of control room operator action was also neglected because the possibility of unavailability of all relief valves at the same time point due to human failure was estimated as extremely improbable. The (seemingly more probable) intentional "failure" potential belongs to the area of security analysis, which is out of the scope of the current Dukovany NPP PSA.

The basic approach used was to split the analysis into several parts as follows:

- Derivation of a simple ultra-conservative frequency estimation for the scenario based on conservative assumptions;

- Evaluation of the criterion regarding the occurrence frequency derived for the scenario;

- Provided that the ultra-conservative estimation had not met the criterion, derivation of a less simple and less conservative frequency estimation;

- Evaluation of the criterion using a less conservative estimate.

■ Ultra-conservative Estimation

This estimation provided the following numerical values:

- Initiating event frequency: < E-02 /ry;

- Conditional probability of failure of plant response (contemporary failure of opening of nine steam generator relief valves on demand): < 5 E-06 /ry;

- Frequency of the scenario: < 5 E-08 /ry.

The initiating event frequency value represents a roundup of direct statistical experience of no event for 115 years of operational history. The conservative assumption of one event provides the value of 8.7 E-03 /ry.

The probability of contemporary failure to open of all steam generator relief valves (SGRVs) (a roundup of the value 4.51 E-06) was derived based on the plant specific failure rate for independent failures of one SGRV to open derived based on plant specific data covering the operation of four units during the time period 2009 to 2013 – ( ˙ = 1.11 E-06 /h, TI = 8760 h, q = ˙TI/2) and generic alpha factors for the group of eight components published by U.S. NRC in the update of NUREG/CR-5497 released in 2016 /NRC 16a/ (SGRV CCF to open on demand).

The final value of estimated frequency of the scenario is a product of two values presented above. The value is connected to the following sources of conservatism:

- The unintentional closing of main steam valves is a not expected event so that the real frequency is much lower than 1 E-02 /ry;

- The CCF probability for the CCF group of eight components was used, but in reality, nine components are available and have to fail to follow the definition of the scenario (no generic data for the group of nine SGRVs are available);

- The failure probability of one SGRV to fail open derived based on plant specific data included all possible failure modes, including the failures initiated by I&C, when the valve can still be opened, this part of failure potential can be significant;

- The operational configuration with just three steam generators available is not quite common in the operational regimes relevant for the scenario; at least four, but better six steam generators are available for most of the time so that as many as 18 SGRVs have to be lost to fulfil the scenario definition corresponding to a much lower CCF probability.

■ Less Conservative Estimation

This estimation was based on the following numerical values:

- Initiating event frequency based on more thorough analysis: < 4 E-03 /ry;

- Conditional probability of failure of plant response (contemporary failure of opening of nine steam generator relief valves on demand): < 3 E-07;

- Frequency of the scenario: < 1.2 E-09 /ry (as product of the initiating event frequency and the conditional probability of plant response failure).

The value of the initiating event frequency was derived by analysis of all possible spurious signals, which could cause closing of steam lines valves (human failure was excluded as the cause at the beginning of the analysis, as described above). Two basic categories of signals were analysed:

- Steam line break signals;

- Main steam collector rupture signals.

A CCF of at least three I&C paths leading to generation of three spurious signals (for all three steam line valves under concern in the case, plant configuration is limited to three steam generators) is necessary to happen for the first case. It was proven by more detailed analysis that the probability of such CCF is much lower than 1 E-03 /ry.

The frequency of generation of spurious signal "main steam collector break" was proven to be lower than 1 E-03 /ry based on operational data; since there are three such signals of different kind, which could be generated, the total frequency of this alternative is 3 E-03 /ry.

The upper bound estimation for generation of spurious signal causing closing of all three steam lines operated or the main steam collector, the operated steam lines are linked with, is:

1 E-03 /ry + 3 E-03 /ry = 4 E-03 /ry.

The probability p of contemporary failure to open of all SGRVs (3 E-07) was derived in similar way as in case of ultraconservative estimate described above. Once again, this probability was a product of probability of independent failure of one SGRV and generic alpha factor for the group of eight components (SGRVs). The intensity and other parameters ($\lambda$ = 7.55 E-08 /h, TI = 8760 h, p = $\lambda$ TI/2) were derived on the base of plant specific data, where one event of that kind was identified as recorded in plant history covering 84 reactor years of operation of 16 SGRVs – event 70/2/2000 from the year 2000 (time period 1995 to 2016 covered by the analysis). Alpha factor generic values were used the same as in the case of ultraconservative estimation.

The final value of upper bound estimation of frequency of the scenario is a product of two values presented above. The value of 1.2 E-09 /ry is connected to the following sources of conservatism:

- The frequencies of occurrence of multiple spurious signals are significantly over-rated.

- The CCF probability for the CCF group of eight components was used; in reality, nine components are available and have to fail to follow the definition of the scenario (no generic data for the group of nine SGRVs are available) (the same source of conservatism as in the case of ultra-conservative estimation).

- The operational configuration with just three steam generators available is not quite common in the operational regimes relevant for the scenario as a whole, at least four, but better six steam generators are available for most of the time so that as many as 18 SGRVs have to be lost to fulfil the scenario definition corresponding to a much lower CCF probability (the same source of conservatism as in the case of ultra-conservative estimation).

■ Conclusions

An example of a real probabilistic analysis was given, using the PSA plant model and plant operational data analysis in support. Although the approach used was fairly simple and the analysis was not time consuming, the conclusions made regarding risk potential of the emergency scenario under concern were important, because they justified avoiding much more resource and time consuming supporting thermal hydraulic analyses. Although the level of conservativeness of the analysis was relatively high; there was still significant margin in meeting the pre-defined criteria justifying the conclusion about negligible potential of the risk scenario analysed.

## 5.3 Finland

*Question/Issue*

Level 2 PSA differs from Level 1 because physical phenomena have an important role in severe accident progression, whereas

Level 1 PSA mainly focuses on failures of safety functions. In addition, recoveries of some safety functions are typically modelled in Level 2 PSA. Timings of events are more important in Level 2 PSA. For example, if a reactor core is reflooded during a critical time window, significant amounts of hydrogen are produced possibly leading to a hydrogen explosion. Traditional fault tree-based modelling does not suit very well for modelling this type of time dependency and phenomena. In addition, the set of possible accident conditions is so large that it cannot properly be captured in a binary model.

*Approach/Procedure*

VTT has developed a simulation-based Level 2 module to their FinPSA software. The basis for the development was the DOS-based SPSA software developed by the Radiation and Nuclear Safety Authority (STUK) of Finland. The Level 2 module combines event trees with script-based modelling. The model includes a script file for each event tree header. In the script files, functions are defined to calculate probabilities of event tree branches as well as source terms for accident sequences. The script files offer lots of flexibility for modelling, and it is possible to include timings of events explicitly in the model with uncertainty distributions. All dynamic dependencies related to severe accident phenomena can be modelled in the scripts. The model is also not restricted to binary logic. A branching point can include more than two branches, continuous variables can be used, and various different conditions and accident timing scenarios can be incorporated in the scripts.

Uncertainty distributions can be defined for all variables of the model, and the model is solved by Monte Carlo simulations. The result is a set of simulation results for each accident sequence. Then, for raw simulation data, statistical analyses are performed to calculate mean results and uncertainty distributions. The tool also includes a risk integrator that combines simulation results from multiple containment event trees.

The Level 2 PSA model can be integrated tightly to the Level 1 PSA model built using traditional PSA approach with event trees and linked fault trees. The Level 2 PSA tool can read Level 1 accident sequence and minimal cut set results. Level 1 PSA information can be utilised in Level 2 PSA modelling, e.g. to calculate core cooling recovery probability. Contributions of the most important Level 1 sequences, basic events and initiating events can also be reflected in the Level 2 PSA results.

*Results*

The capabilities of the Level 2 FinPSA have been demonstrated in simplified case studies for a generic boiling water reactor plant /TYR 18/. The tool enables several different modelling techniques /TYR 19/. Probabilistic calculations can be performed in a static or dynamic manner. Dynamic approaches can be more realistic, but handling of epistemic and aleatory uncertainties in a dynamic model has been identified as an issue that re-quires more development. The tool also supports integrated deterministic and probabilistic safety analysis (IDPSA), it is possible to include physical equations representing the plant behaviour in the model to a given extent. The tool has also been used in the Level 2 PSA for the Olkiluoto NPP units.

## 5.4 France

### 5.4.1 PSA USE IN THE FRAME OF PERIODIC SAFETY REVIEWS

*Question/Issue*

One of the most important uses of PSA in France is the PSR.

*Approach/Procedure*

During the first step of the PSR, the reference PSA is updated by the licensee (EDF), incorporating the most recent operating experience, the updated plants

state (design modifications and operation) and new knowledge obtained from the most recent studies.

The scope of the PSA is not fixed, and it is likely that it will be enlarged at each PSR.

The assessment of the overall CDF is an element which can be used to estimate the change in safety level compared with the assessment made after the previous PSR. This assessment is supplemented by an analysis of the principal contributions to the CDF. This analysis results either in an acceptance of the status or design, or operation changes may be studied. In the event that changes are studied, PSA can be used to assess the advantages and drawbacks of the various solutions considered.

Following the PSR, a new version of the reference PSA is provided, considering the changes decided on the completion of the review process. This version of the PSA is used for different PSA applications before the next PSR.

*Results*

Some examples of important safety aspects highlighted by the past PSA studies in France are:

- LOCA mitigation: The flow injected by the low-pressure injection system (LPIS) could be too small for the pumps; the importance of using of the low flow by-pass line for the LPIS pumps was highlighted and adapted measures were implemented.

- Heterogeneous dilutions: The risk of a reactivity accident in case of a dilution while the main pumps are restarted after a loss of offsite power; plant modifications to decrease the risk;

- Loss of reactor heat removal during mid-loop operation: Mainly, an automatic primary circuit make-up system was implemented.

- Plant modifications in order to reduce the frequency of ATWS (anticipated transient without scram) situations (diversification of the reactor scram function);

- CCF of redundant 6.6 kV safety busbars; plant modifications to allow the mitigation of such situation (improvement of the steam generator (SG) feedwater and of reactor coolant pump (RCP) seals injection functions).

- Improvement of the ventilation system;

- The need for plant modifications in order to reduce the risk of core damage with containment bypass in case of primary pumps thermal barrier rupture was identified.

- An important internal flooding scenario was identified which may need plant or operational improvements.

- The Fire PSA for the 1300 MWe plants demonstrated the need for some improvements.

- Many improvements regarding the SFP design and operation (particularly to reduce the risk of accidental loos of inventory).

### 5.4.2 COMPLEMENTARY DOMAIN DEFINITION (MULTIPLE FAILURE SITUATIONS)

*Question/Issue*

The safety of PWRs of the French nuclear power program essentially relies on a classical deterministic design based on the concept of defense-in-depth. Later (after WASH 1400) the regulators requested EDF to evaluate the frequency and consequences of the loss of redundant safety systems (loss of the reactor safety shutdown system (ATWS), loss of ultimate heat sink (LUHS), total loss of steam generator feedwater, total loss of electrical supplies). The results of these probabilistic evaluations indicated that the risk of core

damage could be higher, and that the deterministic demonstration was not complete, with several high risks being not covered by the design.

*Approach/Procedure*

For assessing the efficiency of the design of the complementary measures, a more formal framework was defined with a list of "multiple failure situations" leading to implementation of safety improvements, and precise rules were stated for the demonstration of the acceptability of these situations. Even if PSA is used to identify the list of "multiple failure situations" and associated mitigations, the rules for their acceptability analysis became a part of the deterministic safety demonstration.

*Results*

Examples of complementary domain features are:

- additional systems to avoid seals LOCA,

- feed and bleed procedure,

- additional site power supply,

- auxiliary feedwater tank supply,

- containment venting, etc.

### 5.4.3 TECHNICAL SPECIFICATIONS

*Question/Issue*

The Technical Specifications (short: Tec Specs) of the operating reactors were initially developed based on the design basis accidents (DBAs) analysis of the safety report, following a deterministic approach or using expert judgment. PSA insights were subsequently used to improve the Tec Specs on specific aspects (Tec Specs permanent changes) or to assess the Tec Specs temporary changes.

*Approach/Procedure*

Since 2002, the regulatory framework for applying PSA in the decision-making process has been established by the "French PSA basic safety rule" /RFS 02/. The main areas of using risk information in the Tec Specs are to:

- Identify risk significant SSCs to be included in the Tec Specs and define the required actions and estimate completion time;

- Justify a TS temporary change.

Furthermore, internal events PSAs can be used as a complement of the safety analysis, to derogate to Tec Specs, for example in the case of maintenance operations for which the duration could be longer than that initially expected.

*Results*

Currently PSA are uses for Tec Specs definition and for Tec Specs exceptions assessment by EDF and IRSN.

### 5.4.4 TREATMENT OF NONCONFORMING CONDITIONS (NCS)

*Question/Issue*

Many non-conforming conditions (NCs) are noted. For a part of them, permanent corrective measures need time to be implemented. Consequently, a particular reactor unit could be simultaneously affected by two or more NCs. PSA can be used to assess the impact of a NC in order to decide the priorities of corrective measures.

Approach/Procedure

PSA is used to analyse the cumulative effect of NCs by EDF, even if no probabilistic criteria is used:

- to better estimate the NCs´ safety impact when SSCs reliability is affected,

- to take into account the compensatory measures´ effectiveness,

- to better address the support systems NCs,

- to deal with a large number of NCs and accident scenarios and carry out more exhaustive assessments,

- to give an overall picture of the unit level safety, and

- to prioritize actions based on importance analyses or comparing different situations.

*Results*

First assessments are already available and have demonstrated the effectiveness of the approach.

### 5.4.5 PSA USES FOR NEW REACTORS (EPR) IN FRANCE

*Question/Issue*

According to the French Technical Guidelines for new reactors /ASN 04/, the safety demonstration for NPPs of the next generation has to be achieved in a deterministic way, supplemented by probabilistic methods.

*Approach/Procedure*

Specific procedures or approaches were defined for several PSA applications at the design stage.

*Results*

During the design of the EPR reactor, the PSA was used both by EDF and IRSN, as a complement of other traditional deterministic methods for several purposes. Some of them are listed in the following:

- Definition of risk reduction categories (RRC-A);

- Systems design assessment;

- Contribution to the verification of the "practical elimination" for particular situations that could lead to large or early releases;

- Safety classification.

## 5.5 Germany

### 5.5.1 POTENTIAL INTERNAL FLOODING DUE TO BREAK OF A FIRE EXTINGUISHING PIPELINE

*Question/Issue*

The fire water supply of a NPP electrical building is achieved by, amongst other means, a fire water main from the building basement routed via the staircase to the different building levels supplying the different fire extinguishing systems. The fire water line was under permanent pressure, with a valve for isolating the line installed in the basement (in open position). In case of a leakage in the pipeline the valve had to be manually closed.

Investigations as part of the PSR indicated that it could not be excluded that a leakage would be recognized and located only when the basement was already flooded making the closing of the valve impossible. It turned out that implementing a further isolation of the pipeline outside the building would be extremely time and effort consuming, since the fire water network had to be split up for isolating the electrical building isolated from the whole network. In conclusion there was the risk that in case of increasing water level the staircase would be flooded with consequential flooding of the electrical cabinet on a higher building level via gaps under doors.

*Approach/Procedure*

In a first step, the damage state probability of such a scenario was estimated:

- The leakage frequency of the fire water pipeline was determined depending on the pipe length considering assumptions on the material quality. It was conservatively assumed that the leak size is the same as in case of a complete line break.

- In case of a fire water system pressure drop the operation of the fire water pumps is required and these pumps start feeding water into the system. It was assumed that the leakage is not detected at first and therefore the pumps continuously run over the whole time period of the flooding event. Due to this assumption the leakage rate was calculated based on the pump capacity of the fire water pumps.

- The water gauge over time in the rooms inside the electrical building was estimated by numerical simulation based on different scenarios (e.g., a basement door being pressed open by the water ingress or a door remaining closed during the whole flooding process).

- The gap size under the doors was measured for realistic simulation of water spreading.

- The simulation aimed at estimating the point in time up to which feeding into the leakage needs to be stopped latest to prevent flooding of switchgears and breaker cabinets. In this context, it had to be considered that a flooding of such cabinets can occur in different rooms and on different elevations, if the water feeding is stopped when the cabinet location is still dry. Even after leakage isolation water from a higher elevation in the staircase intrudes into the switchgears.

- The consequences of a flooding of the entire electrical cabinets belonging to a switchgear were assumed not to be assessable. Therefore, a hazard state was assumed to occur as soon as the water level in the switchgear rooms was high enough to flood the breaker cabinet floor (cabinets installed on a higher elevation).

A main objective of the study was the probabilistic assessment of personnel actions: Diagnosis of the leakage, localization of the leakage and leakage isolation. During leak-age diagnosis the additional difficulty occurred that the fire water system of the NPP site affected supplies two NPP units. Investigating the causes after a pressure decrease and localization of the leakage requires to consider not only one unit but both ones. The assessment was based on the written administrative procedures. The flooding of the isolation valve located in the basement occurred so early that the possibility of isolating the leakage by this valve was not credited.

The result of the assessment was that the above-mentioned scenario provides a non-negligible contribution to the damage frequency, mainly according to the fact that the estimated grace periods for a timely isolation of the leakage were too short for directly neglecting the probability of a successful leakage diagnosis, localisation and isolation. The damage frequency resulting from a leakage of the fire water pipeline in the electrical building was estimated to be the same as the occurrence frequency of such a leakage (no countermeasures possible).

For reducing the risk resulting from this scenario it was suggested to replace the manually operated open valve in the basement of the electrical building by a motor operated closed one, which automatically opens in case of a fire in the electrical building for ensuring the fire water supply. For prevention of pressure surges (water hammer) in the fire water pipeline in case of opening the valve, which may endanger the integrity of the fire water pipeline, the pipeline in front of the valve should be connected to the one behind valve by a bypass pipeline with small diameter and orifice to ensure that the pressure is maintained.

*Results*

The scenario was re-assessed with respect to the frequency of damage states considering the intended changes. The following aspects had to be considered in the assessment:

- The damage frequency resulting from a leakage occurring between building entrance and the closed valve is the same as the occurrence frequency of this leakage (so-called "critical leakage"), since this length can still be isolated only by the long duration isolation possibility outside the building. However, the occurrence frequency of a critical leakage is much lower than without the modification. The reason is that only a short part of the pipeline will be affected.

- The damage frequency resulting from a leakage occurring behind the closed valve is only insignificantly lower than without the modification: The pressure remains the same resulting in the frequency per length of the pipeline remaining the same. The short part of the pipeline between building entrance and valve is no longer considered. However, the exhaust rate is significantly lower because of the exhaust only via the bypass line with orifice resulting in significantly lower time periods for flooding. The success of countermeasures, such as isolation outside the building, could therefore be assessed to by probable. This was done by explicit modelling in the frame of providing a new event sequence for the flooding event.

- From a fire protection viewpoint, the situation is worse, since in case of fire a motor operated valve needs to be opened to ensure the fire water supply in the electrical building. The valve can also fail, while in the unchanged configuration the fire water supply was ensured by the permanently open manually operated valve. The in-creased safety with respect to flooding had to be balanced against the loss of fire protection. The overall risk was lower in case of the modification.

Because of the significant reduction of the overall plant risk the proposed modification could be implemented as intended.

*Summary*

Type: first, occasional assessment, then review of the intended modification

Screening process of the relevant questions: in a first step, the questions 1, 3, 4, 5, 7, 8, 11 and 12 of the questions provided in /FAK 18/ were answered with yes.

Identification of potential consequences: In a second step, a variety of questions were identified to be relevant, i.e.:

| No. | Question | Identification of Those Areas Affected by the Safety Related Question | Consideration of the Area affected within PSA | |
|---|---|---|---|---|
| | | | Explicitly and Quantitatively | Only Qualitatively |
| 1.1 | Does the question result in new initiating events (PIEs)? | The scenario "flooding of electrical building by break of a fire water pipeline had not yet been considered | no | No (before occasional assessment) |
| 1.3 | Is a re-assessment of the frequencies of the groups of PIEs necessary according to the question? | The suggested modification results in a decrease of the occurrence frequency of critical leakages | no | yes (after occasional assessment) |
| 3.2 | Is it necessary due to the question to implement new branch points or system functions for considering aspects not yet considered in the event sequence diagrams | Actions of the personnel, leakage diagnosis, localisation and isolation | no | yes (after occasional assessment) |
| 5.1 | Is it possible to connect the question distinctly to the definition of one or more basic events or is it necessary to define new basic events? | Fire water supply in the electrical building (closed motor operated valve instead of open manually operated valve) | yes | |
| 7.3 | Will time periods for actions by the personnel be changed by the question? | Extending grace periods for leakage diagnosis, localisation and isolation by modification | no | yes (after occasional assessment) |
| 8.1 | Does the question affect the qualitative screening analysis? | New event identified | no | no |
| 8.6 | Does the question affect time considerations for the flooding analyses? | Extended grace periods by modification | no | yes (after occasional assessment) |
| 9.4 | Does the question affect the status or the availability of fire protection means, e.g., for fire detection and extinguishing? | Fire water supply in the electrical building (closed motor operated valve instead of manually operated valve) | yes | |

*Table 5.1 Questions for identifying areas affected by a safety related question and their consideration within PSA*

Conclusion:

First the theoretical possibility of the scenario was identified. This resulted in the necessity to quantify its contribution to risk for assessing if a corrective action / safety improvement was necessary. This assessment was performed with simplified assumptions (actions of the personnel for leakage diagnosis, localization and isolation not explicitly modelled, but in general assessed as not successful because of the short grace period avail-able, leakage occurrence frequency was set on the same value as the damage frequency resulting from this scenario). The simplified assumptions were justified to represent a screening step for investigating if this scenario can result in damage.

This could be justified resulting in an analysis of the modification (corrective action). In the frame of this analysis some of the simplified assumptions were replaced by explicit modelling (developing an event sequence diagram, where the action of the personnel for leakage diagnosis, localization and isolation were modelled). The assessment of

the effects of the modification on the fire induced risk was performed by adapting the failure probability of the fire water supply in the electrical building in the Fire PSA.

For the overall assessment of the modification before their implementation in the affected NPP a comparison of the situation with and without this modification was carried out for some aspects. The complete modelling of the modification in the plant PSA model was performed after the implementation of the modification in the frame of the PSR.

### 5.5.2 RISK SIGNIFICANCE OF UNEXPECTED DETAIL AT THE REACTOR PRESSURE VESSEL BOTTOM IN LEVEL 2 PSA

*Background*

The TMI accident resulted in an almost complete core melt and in significant relocation of core material into the lower RPV plenum. Although there were some RPV bottom penetrations for instrumentation devices in that specific design and although analyses indicated high material temperatures near to failure conditions, the RPV bottom remained intact. If it had failed, the accident progression and the consequences could have been much more severe.

GRS has performed several PSAs, one of them for a German BWR. The issue of RPV bottom failure has been one of the issues which were analysed in detail. It turned out that a design feature which was hardly known, and which could not easily be detected in the plant documentation very much influences the RPV bottom failure issue.

*Technical Description of the Issue*

It is well known that the RPV bottom of a BWR contains a lot of penetrations, e.g. control rod penetrations, instrumentation penetrations and openings for internal circulation pumps. Accordingly, relevant effort has been dedicated in the PSA for determining the resilience and the failure mode of such penetrations under core melt impact. It turned out that those penetrations are not significantly weaker than the plain RPV bottom material. Accordingly, failure conditions and associated event progressions have been incorporated in the PSA.

During a late stage of the PSA the relevant plant drawings have been revisited. Almost by chance a miniscule detail in a RPV bottom drawing became visible (see Figure 5.1, detail "E"): There was another unique sort of penetration. It had no use at all, no tube or instrument was attached to it, and therefore it had gone unnoticed. This additional penetration is located in the center of the RPV bottom at the lowermost position. It has a diameter of 0.085 m. It is assumed that in the original design probably a draining line was intended at this location which later was found unnecessary or inappropriate. Because it had already been manufactured into the RPV bottom, it was then closed with a cap-type structure (see Figure 5.1). It is invisible by manual inspection because it is hid-den above the many components below the RPV bottom.

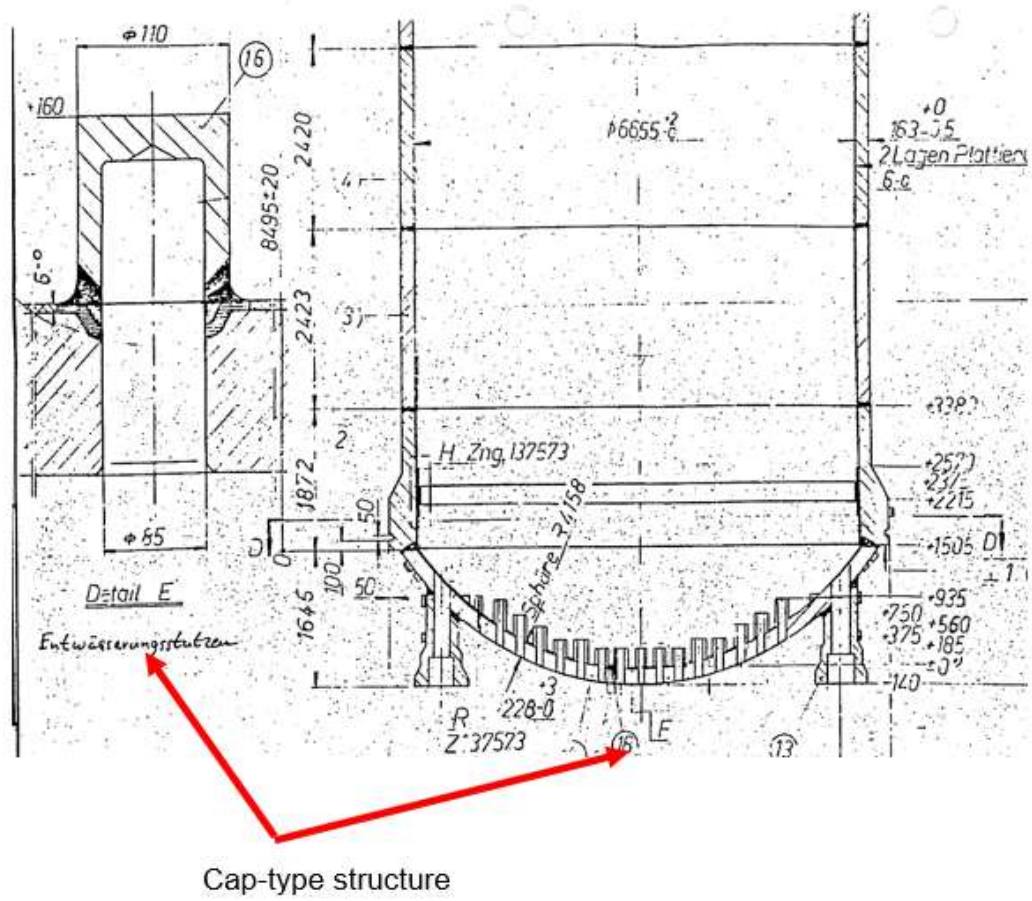


*Figure 5.2 RPV bottom drawing – transverse section*

Once this additional penetration had been detected, it was simple to estimate its effect on the PSA: This penetration will certainly fail soon after contacting core melt. The RPV bottom failure would be faster than anticipated, but it would also be limited to a rather small diameter compared to the probably bigger failure size without this penetration. It is even more significant that this penetration can by no means be cooled if the RPV vessel is flooded from the outside. Steam would be generated inside it and force any water out of the penetration, leaving it uncoolable. Any considerations for accident management measures to flood the containment to prevent or delay melt-through are obsolete.

The effect of this penetration on the integral PSA results is beneficial, not adverse as might be expected: The small failure area of the penetration diameter poses less risk than the probably larger failure area without that penetration.

*Lessons Learned*

The following are lessons learned:

- Details in the design of components or structures which are affected by core melt impact can be decisive for event progression.
- Plant documentation review and plant inspection must look for such important de-tails.
- The overall effect on risk of specific designs may not be obvious.

## 5.6 Hungary

### 5.6.1 SAFETY ENHANCEMENT PROPOSALS BASED ON THE UPGRADE OF THE LOW POWER AND SHUTDOWN PSA MODEL

*Background*

Level 1 PSA models for low power and shutdown (LP&SD) conditions are available for the Paks NPP (equipped with four VVER-440/213 type units) in Hungary since 1997. Until 2011, post-initiator operator actions (so-called type C human interactions) in the LP&SD PSA were identified and quantified based on event-based emergency operating procedures (EOPs). After the implementation of symptom oriented EOPs (SOEOPs) for full power operation in 2003, similar procedures were introduced in 2011 for LP&SD conditions as well. Consequently, the whole area of HRA for type C actions had to be reconsidered and renewed. PSA model development and re-quantification in view of EOP improvement were completed in 2013. Besides modifications induced by EOP changes, the assessment identified several other potential model upgrades and established safety enhancement proposals for risk reduction.

*Technical Description of the Issue*

The Level 1 PSA model for low power and shutdown conditions of the Paks NPP considers 24 different POSs representing a typical refueling outage performed annually. Full power operation is represented by POS 0, while the POSs for low power and shutdown conditions are designated as POS 1 through POS 24. These POSs are analysed separately by calculating the core damage risk for each of them. The new, stand-alone symptom-oriented EOPs (hereafter L-SOEOP) shall be used only under those low power and shutdown conditions when the core flooding tanks are disconnected from the primary loop, namely in POSs 4 - 22. For all the other POSs the full power SOEOP shall be used.

The upgrade of the PSA to model the effects of new L-SOEOPs included:

- the review and modification of the accident sequence models in accordance with the new procedural requirements for emergency operations,

- the re-definition of human failure events for type C errors in the PSA model,

- the quantification of operator reliability for the re-defined failure events, and

- the re-quantification of accident sequences.

Following the implementation of the modifications into the PSA model listed above as well as risk quantification, the results show a total risk decrease by more than 4 % for all plant internal events analysed (internal and external hazards were assessed separately at a later point in time). It should be noted that not only the implementation of the new EOPs causes the difference in the core damage probabilities (CDPs), but many other refinements identified during the re-assessment. Since the PSA model has been changed substantially, the effects induced purely by the implementation of L-SOEOP were not quantified separately.

The modification process of the PSA model motivated by the change in EOPs revealed some possible changes that can enhance safety. These are mainly concerned with changes or refinements in the L-SOEOPs, as well as with modifications to the maintenance strategy at Paks. Some of the most important proposals for safety improvements are listed below:

- In case of interfacing system LOCAs, an instruction should be introduced for refilling the emergency core cooling system (ECCS) tanks from the bubbling condenser trays, especially when the reactor is open. Although, both the full power SOEOP and the former, event-based EOPs for LP&SD conditions required the abovementioned operator action in interface LOCA situations, the instruction was missing from the early version of the new L-SOEOP. Credit was given to this modification in the assessment

since the plant management has already made commitment to perform it. Without having this instruction introduced, the annual CDP for the POSs 4 - 22 would increase by 14 %.

- If the ECCS tanks are depleted in a non-interface LOCA situation in those reactor states when the reactor is open for refueling, a warning for the operators should be introduced to switch the suction line of the ECCS pumps from the tank to the sump because the automatic actuation to switch is blocked if the reactor is open. In the lack of an open line to the sump, the long-term core cooling with ECCS is not possible. Credit was already given to this modification in the assessment since the plant management has already made commitment to perform it. Without having this warning introduced, the annual CDP for the POSs 4 - 22 would increase by 890 %.

- In open reactor states, the sump is covered to prevent its mechanical failure and to ensure protection against debris, which would result in the unavailability of long-term cooling after the ECCS tanks are depleted if a non-interface LOCA situation occurs. This action was modified by the operating personnel right after the risk was quantified.

- The maintenance of the emergency feedwater pumps, and the auxiliary emergency feedwater pumps should only be performed when the corresponding safety trains are on maintenance or when the reactor is open for refueling, and the availability of the pumps should be ensured in all other POSs. If this measure is introduced, the appropriate pumps are available for accident mitigation when the reactor is closed. Corresponding changes should also be implemented in the relevant procedures. Credit was already given to this modification in the assessment since the plant management has already made commitment to perform it. Without having this measure introduced, the annual CDP for the POSs 4 - 22 would increase by 43 %.

*Lessons Learned*

The following lessons learned have to mentioned according to /BAR 15/:

- A detailed PSA assessment seemed to be an appropriate tool to identify inadequacies in recently implemented emergency operating procedures and maintenance practices. The role of the identified factors can be quantified in most cases; therefore, decisions can be made if a modification is urgently necessary or not.

- The PSA assessment was also proven to be an appropriate tool to compare the risk associated with the new and the previous emergency operating procedures which was the main goal of the assessment.

### 5.6.2 PRELIMINARY ASSESSMENT OF THE IMPLEMENTATION OF AN ONLINE MAINTENANCE STRATEGY USING RISK MONITOR

*Background*

According to the Technical Specifications of the Paks NPP, the safety systems in full power as well as in near-full power operational states were permitted to be unavailable (for a limited time) due to random failures. Meanwhile, in several NPPs worldwide, online maintenance has been practised for a long time. The reason for this can be explained as decreasing maintenance burden during outages so that the relaxed workload of staff can have a beneficial effect on equipment reliability as their maintenance are more efficient. Reducing the amount of maintenance activities during outages is only possible by conducting maintenance at full power as well. The risk-increasing effect of this procedure is compensated by the increased equipment reliability and risk-awareness which is the basic condition of performing online maintenance work. Moreover, according to countries with online

maintenance experience, the risk-increasing effect of the strategy is not just compensated, but the increasing equipment reliability results in the decrease of total cumulative risk over time.

The risk-decreasing effect due to online maintenance could be recently proven based on long-term operational experience, but it is also possible to preliminarily assess the effect of the strategy on the momentary (CDF) and cumulative (CDP) risk. This was done using a dynamic risk assessment tool called risk monitor. The analysis procedure, the scenarios analysed, and the results are discussed below (for details see /KAR 12/ and /KIS 16/).

*Technical Description of the Issue*

In a first step, the emergency diesel generators were selected to be the target of the assessment. According to the Technical Specifications, the unavailability of the diesel generators is not allowed if the temperature of the primary circuit is higher than 150 °C or lower than 150 °C during heat-up, except the unavailability is due to the draining of the service water system, providing cooling water to the diesel generators, during an outage. For assessing the implications of online maintenance, the removal of this limiting condition was considered.

By processing and incorporating the operational data – recorded in the electronic logs of the power plant – into the risk monitor, risk curves were produced for the time period between January 2009 and December 2011 for all four units. Together these twelve re-actor years formed the basis for a more in-depth investigation of maintenance scheduling.

The online maintenance of the diesel generators decreases maintenance duration of the affected safety system during outages from, on average, three to seven days, which results in risk reduction during an outage. Under these conditions, the unavailability of these safety systems during an outage is determined by the maintenance of the safety system trains themselves as opposed to the maintenance of diesel generators.

Three scheduling strategies were evaluated for the online maintenance of diesel generators:

- Maintenance of the safety systems during outage (lasting for three instead of seven days), the time required for online maintenance of the diesel generators (7 days/unit) is uniformly distributed during full power operation.

- Maintenance of the safety systems during outage (lasting for three instead of seven days), consecutive online maintenance of each diesel generator (seven days/unit) at full power right before the start of the refueling outage.

- Maintenance of the safety system during outage (lasting for three instead of seven days), consecutive online maintenance of each diesel generator (seven days/unit) at full power right after start-up following the refueling outage.

The maintenance time intervals of the diesel generators were hypothetically rearranged in the risk monitor assuming the abovementioned strategies. The results of the modifications for Unit 1 in 2010 are presented in Figure 5.2 and Figure 5.3. In the figures the purple line represents to the original maintenance schedule (not assuming online maintenance), dark blue witnesses' strategy no. 1, green indicates strategy no. 2 and light blue refers to strategy no. 3. Figure 5.3 is an enlarged picture of the outage period from Figure 5.2.

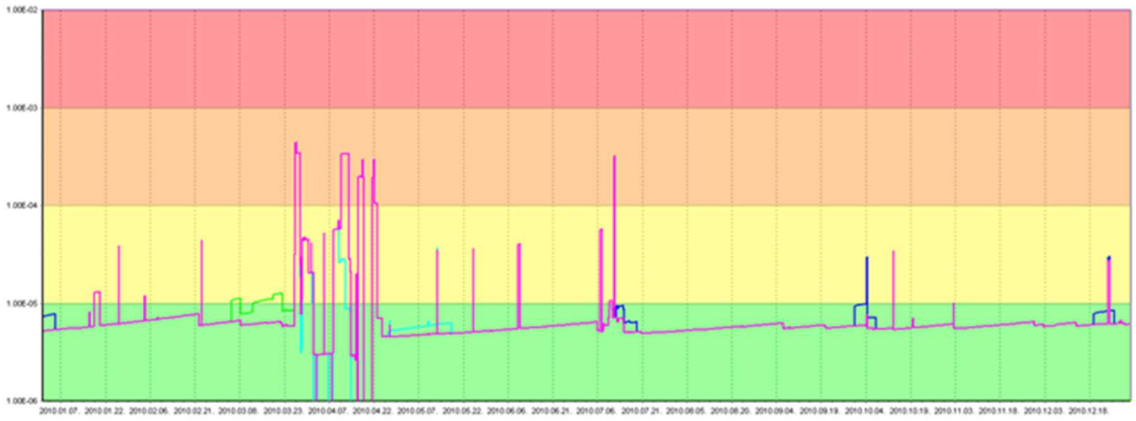

*Figure 5.2 Risk curves for a reference unit in 2010 (In the figures the purple line represents to the original maintenance schedule (not assuming online maintenance), dark blue witnesses' strategy no. 1, green indicates strategy no. 2 and light blue refers to strategy no. 3.)*

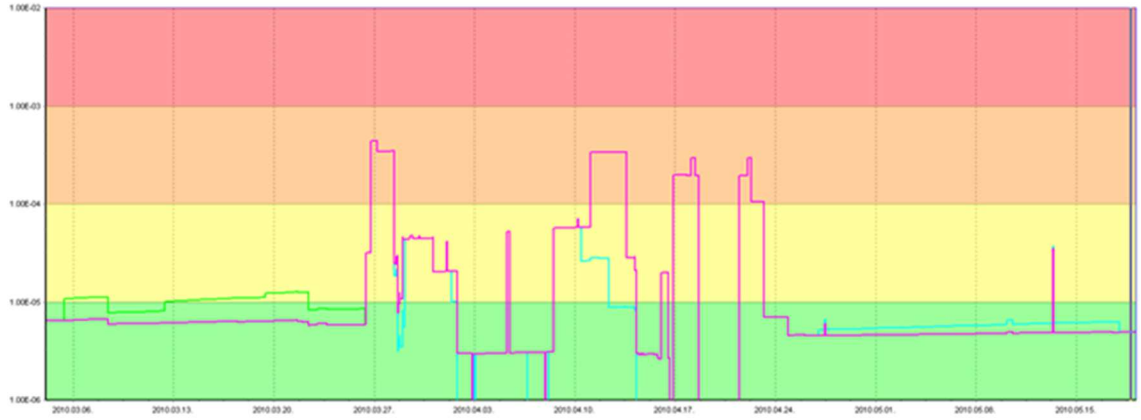

*Figure 5.3 Risk curves for a reference unit focusing on outage (Figure 5.3 is an enlarged picture of the outage period from Figure 5.2.)*

The risk reduction due to shortening of the maintenance interval during outage can be observed in Figure 5.3 where the light blue curve moves below the purple one. Only the purple and light blue curves show up during the outage period because the other curves run together with these two. Risk increase due to online maintenance of the diesel generators can be observed right before the outage (where the green curve moves above the purple one) representing strategy no. 2. and right after the outage (where the light blue curve moves above the purple one) representing strategy no. 3. Strategy no. 1 with a dark blue curve can be differentiated just in Figure 5.2.

The question whether online maintenance of the diesel generators has an advantageous effect on the total risk or not can be answered based on determining cumulative risk or the annual CDP. Figure 5.4 shows the cumulative risk curves over a year for the different strategies.

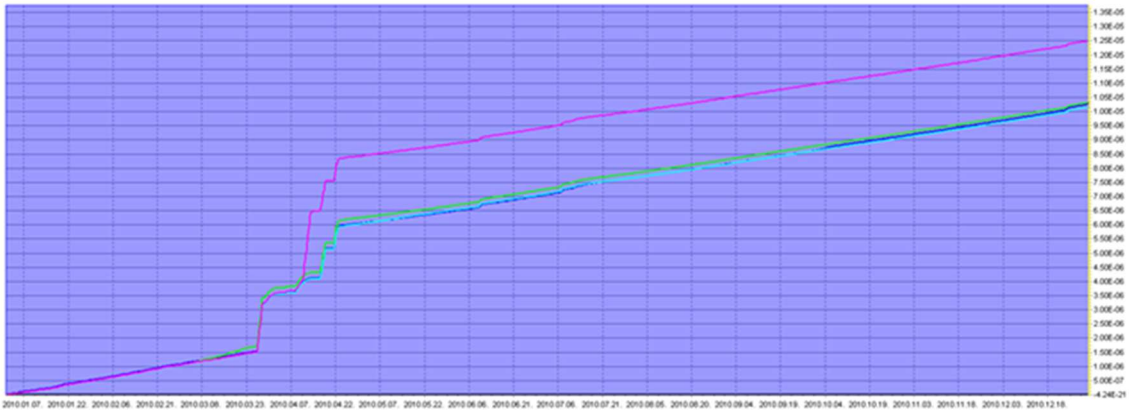

*Figure 5.4 Cumulative risk curves for a reference unit in 2010*

It can be concluded that the unavailability of the diesel generator due to online maintenance causes the cumulative risk to be higher in the case of strategy no. 2 until shutdown for outage begins. After the outage is completed, the cumulative risk in the reference case is always significantly higher than in the alternative cases describing online maintenance. The quantitative results for the four units of the NPP in the period between 2009 and 2011 show a decrease in the cumulative risk in the most cases. There are only two cases identified for which the cumulative risk increased slightly with the online maintenance of the emergency diesel generators. The calculation results for the three different strategies show minimal differences, but strategy no. 3 always resulted in the lowest cumulative risk.

*Lessons Learned*

The following lessons learned are important:

- Online maintenance of safety systems can lead to a decrease in the total risk of the NPP.

- A dynamic risk assessment tool such as a risk monitor can be used to support maintenance planning and determine the expected risk profile in advance of performing maintenance.

- Such risk-informed applications can be a useful aid in helping the operating personnel and maintenance planners shift their way of thinking to a "risk credit management mode".

## 5.7 Slovenia

### 5.7.1 EVALUATION OF IMPACT OF THE NEK SAFETY UPGRADE PROGRAM IMPLEMENTATION ON THE REDUCTION OF THE TOTAL CORE DAMAGE FREQUENCY

*Question/Issue*

Following the Fukushima Dai-ichi accidents in 2011, the Krško NPP (NEK) was required by the Slovenian Nuclear Safety Administration (SNSA) to perform consequential actions in order to reduce the risk of severe accidents and their consequences as low as feasible. NEK analysed the response to the severe accidents, and based on the results of this analysis, proposed some measures to be implemented within the shortest possible time period. The following summary was prepared based on /VUK 16/.

*Approach/Procedure*

As a short-term action mobile equipment was purchased (e.g. diesel generators of different rated power, air compressors, water pumps, vehicles for transportation of mobile equipment). The modifications regarding some of the existing systems were performed to allow a connection of new

mobile equipment to adequate connection points.

As long-term actions and in response to the SNSA request NEK has developed the safety upgrade program (SUP), consisting of three phases. The SUP contains a com-prehensive set of measures for plant safety improvements. Phase 1 of the SUP has been implemented during the outage in 2013 with installation of a passive containment filtering vent system and passive autocatalytic recombiners. For the phases 2 and 3 of the NEK SUP an assessment of the impact of plant modifications planned for implementation on the quantitative figure of merit for the plant risk significance – total CDF – has been performed.

The methodology for assessment in power operation mode uses a probabilistic approach, including the necessary engineering judgements. The scope of this application was focused on Level 1 PSA modelling and quantification. The total CDF, from both plant external and internal initiators, was determined. The analysis was performed by employment of the second generation of the MS Windows® OS based RiskSpectrum® PSA.

Initiator categories analysed include:

- internal initiating events (IIE) – 16 categories,

- internal fire events (FIRE),

- internal flooding events (FLOOD),

- high energy line break (HELB) events,

- seismic events and liquefaction (SEISMIC), and

- other external events (OEE) covering natural hazards such as external flooding, severe winds, glaze ice, extreme drought and natural external fires as well as human induced hazards such as aircraft and other transport accidents, industrial and military accidents, turbine generated missiles, pipeline (gas) release of chemicals.

The analysis was conducted in two consecutive steps. In the first step, the plant modifications planned for implementation in SUP phase 2 were modelled in the PSA model and quantified. In the second step, in addition to the plant modifications modelled in the first step, the plant modifications planned for implementation in phase 3 of the SUP were modelled and quantified. The final stage was the quantification of the NEK PSA model.

*Results*

The starting point and the basis for the evaluation was the NEK baseline at-power PSA plant model, which reflects the plant status with modifications from phase 1of the SUP implemented. The total CDF obtained was estimated at 4.69 E-05 /ry (baseline total CDF). Before implementing SUP Phase 1 total CDF obtained was estimated at 7.06 E-05 /ry

The SUP phase 2 plant modifications modelled include:

- Construction of an emergency control room (ECR) and the technical support centre (TSC) in the bunkered building 1 (BB1);

- Additional pressurizer power operated relief valve (PORV) bypass valves for RCS pressure relief;

- Upgrade of the flooding protection for the nuclear steam supply system (NSSS) is-land;

- Upgrade of the operating support centre (OSC) with additional emergency power supply capacities and conditions for long term presence of operating personnel during accident. These modifications were not addressed in PSA model since the OSC is not a system for performing a safety function and directly mitigating a sequence leading to core damage.

- Alternative SFP cooling (additional sprinklers for SFP cooling and connections for mobile heat exchanger). This modification was not addressed in the PSA model; it should be reflected in the NEK SFP PSA model.

- Additional alternative residual heat removal (A-RHR) heat exchanger for alternative long-term RCS / containment cooling and decay heat removal. An attempt was made to address the impact of installation of Alternative RHR system (A-RHR) on the CDF in NEK PSA model, and the result has shown almost no change in the CDF. The reason for this lies in the fact that a typical mission time of 24 hours, used in the standard PSA model, is considered to be sufficient to reach a stable state after the accident. As the development of the accident over time takes more than 24 hours, the impact on the CDF may not be demonstrated for the long-term low pressure recirculation mode. Consequently, the importance and benefit of implementing an alternative RHR train is not "visible" through the CDF metric which is "driven" by a mission time of 24 hours.

Additionally, the installation of the shielding of essential service water (ESW) pumps' motors from the spray water source was considered in the PSA model, which is not part of the phase 2 of the SUP but was identified during NEK analyses of potential safety improvements.

As shown in Table 5.2 the total CDF posterior to the implementation of SUP phase 2 was estimated at 3.20 E-05 /ry, which represents a reduction of 32 % (reduction factor of 1.5) as compared to the baseline total CDF (4.69 E-05 /ry).

| Initiators' Group | Baseline CDF [1 /ry] | CDF | Initiators' Group | Baseline CDF [1 /ry] | CDF | Initiators' Group |
|---|---|---|---|---|---|---|
| IIE | 1.22 E-05 | 1.22 E-05 | 0.00 E+00 | 0.0 % | 1.0 | 0.0 % |
| FIRE | 1.26 E-05 | 2.90 E-06 | - 9.70 E-06 | - 76.9 % | 4.3 | - 20.7 % |
| FLOOD | 4.88 E-06 | 6.71 E-07 | - 4.21 E-06 | - 86.3 % | 7.3 | - 9.0 % |
| HELB | 1.48 E-06 | 1.46 E-06 | - 1.51 E-08 | - 1.0 % | 1.0 | 0.0 % |
| SEISMIC | 1.12 E-05 | 1.10 E-05 | - 2.19 E-07 | - 2.0 % | 1.0 | - 5 % |
| OEE | 4.54 E-06 | 3.73 E-06 | - 8.06 E-07 | - 17.8 % | 1.2 | - 1.7 % |
| TOTAL | **4.69 E-05** | **3.20 E-05** | **- 1.49 E-05** | **- 31.9 %** | **1.5** | **- 31.9 %** |

*Table 5.2 Comparison of the CDF per Initiators' Group (Phase 2 addressed versus Phase 1 addressed) (from Table 1 of /VUK 16/)*

The SUP phase 3 plant modifications modelled include:

- Installation of an alternative safety injection (A-SI) pump and an associated alternative borated water tank (A-BWT) for RCS injection with borated water (primary injection) in BB2 building;

- Installation of an alternative auxiliary feedwater (A-AF) pump and an associated alternative condensate water tank (A-CYT) with water inventory for SG injection (secondary injection) in the BB2 building;

-Construction of interconnections between BB1 and BB2 buildings and interconnections between BB2 building and NSSS island, which are seismically designed and resistant to liquefaction. This is not explicitly listed as a modification in phase 3 of the SUP. But there is a NEK requirement that equipment and interconnections from new design extension condition (DEC) systems to the

existing systems equipment shall be designed to meet seismic performance requirements during and after a DEC earthquake with a peak ground acceleration (PGA) intensity of 0.6g.

- Plateau for mobile equipment seismically designed for 0.6g PGA with mobile diesel generator mounted with seismic isolation.

As shown in Table 5.3, the total CDF posterior to the implementation of phase 3 of the SUP was estimated at 1.2 0E-05 /ry, which represents a significant reduction of 63 % (a reduction factor of 2.7) as compared to the total CDF obtained posterior to Phase 2, and reduction of 43 % as compared to the baseline total CDF (4.69 E-05 /ry).

| Initiators' Group | CDF Posterior to SUP phase2 [1°/ry) | CDF Posterior to SUP phase3 [1°/ry) | Absolute Delta CDF [1 /ry | Delta CDF Related to Baseline CDF due to Initiators' Group [%] | Total CDF Reduction Factor (RF) | Delta CDF Related to Baseline Total CDF [%] |
|---|---|---|---|---|---|---|
| IIE | 1.22 E-05 | 2.22 E-06 | - 9.98 E-06 | - 81.8 % | 5.5 | - 21.3 % |
| FIRE | 2.90 E-06 | 1.18 E-06 | - 1.73 E-06 | - 59.5 % | 2.5 | - 3.7 % |
| FLOOD | 6.71 E-07 | 2.86 E-08 | - 6.42 E-07 | - 95.7 % | 23.4 | - 1.4 % |
| HELB | 1.46 E-06 | 1.05 E-07 | - 1.36 E-06 | - 92.8 % | 14.0 | - 2.9 % |
| SEISMIC | 1.10 E-05 | 4.81 E-06 | - 6.17 E-06 | - 56.2 % | 2.3 | - 13.2 % |
| OEE | 3.73 E-06 | 3.63 E-06 | - 1.00 E-07 | - 2.7 % | 1.0 | - 0.2 % |
| **TOTAL** | **3.20 E-05** | **1.20 E-05** | **- 2.00 E-05** | **- 62.5 %** | **2.7** | **- 42.6 %** |

*Table 5.3 Comparison of the CDF per initiators' group (phase 3 addressed vs. phase 2 addressed) (Table 2 of /VUK 16/)*

For obtaining insights of the cumulative effect of plant modifications planned in both phases 2 and 3, a comparison of contributions from all initiator categories to the total CDF between is summarized and presented in /VUK 16/. The total CDF evaluated on the basis of implemented plant modifications in Phase 1, as well as scope of modifications planned in the phases 2 and 3 is estimated, as mentioned before, at about 1.2 E-05 /ry. The cumulative reduction of the total CDF is about 3.5 E-05 /ry, which is a significant decrease of the total CDF by 75 % (reduction factor of nearly 4), when compared to the baseline total CDF (32 % in phase 2 plus 43 % in phase 3)

| Initiators' Group | Baseline CDF [1 /ry] | CDF Posterior to SUP Phase 3 [1 /ry] | Absolute Delta CDF [1 /ry | Delta CDF Related to Total CDF Due to Initiators' Group [%] | Total CDF Reduction Factor (RF) | Delta CDF Related to Baseline Total CDF [%] |
|---|---|---|---|---|---|---|
| IIE | 1.22 E-05 | 2.22 E-06 | - 9.98 E-06 | - 81.8 % | 5.5 | - 21.3 % |
| FIRE | 1.26 E-05 | 1.18 E-06 | - 1.14 E-05 | - 90.7 % | 10.7 | - 24.4 % |
| FLOOD | 4.88 E-06 | 2.86 E-08 | - 4.85 E-06 | - 99.4 % | 170.4 | -10.3 % |
| HELB | 1.48 E-06 | 1.05 E-07 | - 1.38 E-06 | - 92.9 % | 14.1 | - 2.9 % |
| SEISMIC | 1.12 E-05 | 4.81 E-06 | - 6.39 E-06 | - 57.0 % | 2.3 | - 13.6 % |
| OEE | 4.54 E-06 | 3.63 E-06 | - 9.06 E-07 | - 20.0 % | 1.2 | - 1.9 % |
| **TOTAL** | **4.69 E-05** | **1.20 E-05** | **- 3.49 E-05** | **- 74.5 %** | **3.9** | **- 74.5 %** |

*Table 5.4 Comparison of the CDF per initiators' group (phase 3 addressed vs. phase 1 addressed) (Table 3 of /VUK 16/)*

Upon a completion of the phases 2 and 3 the most dominant total CDF reduction will be for internal fire events in absolute value of 1.1 E-05 /ry (reduction of baseline total CDF for 24 %) primarily due to the installation of the ECR as part of BB1 project in phase 2 (21 %).

The second largest contributor to the reduction of the total CDF are internal initiating events, for which a reduction of about 1.0 E-05 /ry was obtained (reduction of baseline total CDF for 21 %), primarily due to considering the installation of A-AF and A-SI pumps and associated tanks (A-CYT and A-BWT) in the BB2 building (Phase 2).

The third largest contributor to the reduction of total CDF are seismic events, for which an absolute reduction of about 6.4 E-06 /ry was obtained (reduction of baseline total CDF by 14 %) due to considering construction of interconnections between the BB1 and BB2 buildings and interconnections between the BB2 building and the NSSS island, which are seismically designed to withstand a PGA of 0.6g and are resistant to liquefaction (phase 3).

The fourth largest contributor to the reduction of the total CDF are internal floods, for which an absolute reduction of about 4.9 E-06 /ry was obtained (reduction of baseline total CDF by 10 %) primarily due to installation of ESW pumps shielding against water spraying in phase 2 (9 %).

The results show that a continuous trend of a total CDF reduction is present at NEK and is foreseen to be lowered even more in mid-term by additional safety measures and plant modernisations defined by the scope of the NEK SUP.

## 5.8 Switzerland

### 5.8.1 RISK IMPORTANCE OF ERRORS OF COMMISSION BASED ON TWO PLANT-SPECIFIC STUDIES

*Background*

In state-of-the-art PSA, the human reliability analysis (HRA) focuses on errors leading to the non-performance of the required actions, so-called errors of omission (EOOs) /ANS 08/. Yet, a review of selected events from the industry experience shows that operators in NPPs may contribute to accidents and accidents precursors with inappropriate actions that aggravate the course of events /NRC 00/, which are referred to as errors of commission (EOCs).

Correspondingly, the interest in EOCs has grown; for example, "Good practices for implementing HRA" /KOL 05/, dedicates a chapter to EOCs: two good practices are to address EOCs in future HRA and PSA and, as a minimum, search for conditions that may make EOCs more likely.

Efficient means to identify EOC situations are a challenge for treating EOCs in PSA /REE 08/ (there are potentially many inappropriate actions that can aggravate a scenario /NRC 00/). A review of methods /REE 08/ – ATHEANA, MERMOS, the EOC HRA method developed by GRS /FAS 03/, the MDTA method and CREAM – points out short-comings in the prioritization of the accident scenarios to consider for the EOC search. A second, related issue is the estimation of the probabilities of the EOCs. Many EOCs are related to decision errors. Decision-making performance can be affected by many factors and the factors that are important in a given decision situation depend strongly on the context: this challenges the collection of performance data to quantify decisions.

Experience with comprehensive studies for identification and quantification of EOCs is limited – one example is /JUL 95/, addressing a PWR. The Paul Scherrer Institute (PSI), Switzerland, has contributed to this experience with three studies addressing two different plant designs, a PWR (referred to in this paper as Pilot I /REE 04/) and a BWR (Pilot II /POD 13/). The commission errors search and assessment (CESA) method, developed at the PSI, was used for the identification of the EOCs (i.e. which events shall be modelled within PSA) /REE 04/.

*Lessons Learned*

Based on the experiences from two studies performed with CESA, one for a PWR and one for a BWR, this note presents some overall insights on the treatment of EOCs in PSA.

Neither study identified critical plant vulnerability connected with EOCs. However, in both cases, consideration of EOCs in the PSA did lead to a noticeable change of the quantified CDF (about + 20 % and 5 % in Pilot I and II, respectively). A common lesson learned from both studies can be drawn: the top EOC contributions are comparable to that of the top EOOs and not negligible; efforts for a systematic treatment of EOCs in PSA should continue.

Besides the quantitative impact of EOCs in the risk profile, the type of EOCs found has been addressed: most relate to errors inducing failure of injection, in the reactor and steam generator, others relate to errors inducing component damage and electrical power unavailability.

The following insights were derived:

- Inappropriate actions related to performance of procedures in response to loss of support systems largely contributed to the results. It is recommended to include these procedures in the search for EOCs in future studies.

- Efforts towards systematic treatment of EOCs in PSA should continue. Although neither study identified critical plant vulnerabilities connected with EOCs, the contribution from these errors is comparable to that of EOOs and should be included to improve the quality of the risk profile assessment.

| Study | EOC Split Fraction (operator action contributes to failure of ...) | Scenario (due to initiating event) | EOC Probability | Risk Impact [ry] (CDF increase) |
|---|---|---|---|---|
| I /REE 04/ | IC. EOC1- ... reactor coolant pumps integrity control (induces seal LOCA) | Primary component cooling degraded by equipment failure | 1.2 E-02 | 1.6 E-06 (+ 20 %) |
| | FN. EOC1 - ... special and emergency feedwater (FW) | Secondary component cooling degraded by equipment failure | 6.2 E-04 | 4.9 E-08 (+ 0.6 %) |
| | H3*H2. EOC1 - ... special and normal SI | Small LOCA | 6.4 E-05 | 1.5 E-08 (+ 0.2 %) |
| | RW.EOC4B - ... refuelling water storage tank | Total loss of AC power scenarios | 1.1 E-03 | 8.4 E-09 (+ 0.1 %) |
| II /POD 13/ | HPCS.EOC2 - ... high pressure injection | Total loss of feedwater with reactor core isolation cooling (RCIC) unavailable (operator failure to control) | 2.5 E-01 | 1.3 E-08 (+ 3 %) |
| | HPCS. EOC1 - ... high pressure injection | Total loss of feedwater with RCIC unavailable (hardware failure) | 2.5 E-03 | 7.4 E-09 (+ 2 %) |
| | LPCS&I. EOC1 - ... low pressure injection | Total loss of FW and high pressure injection | 1.0 E-03 | 1.3 E-09 (+ 0.3 %) |
| | DP&HPCS. EOC2 - ... high pressure injection | Total loss of FW with RCIC unavailable (operator failure to control) | 2.5 E-01 | 9.2 E-10(+ 0.2 %) |
| | DP&HPCS. EOC1 - ... high pressure injection | Total loss of FW with RCIC unavailable (hardware failure) | 2.5 E-03 | 3.8 E-10 (+ 0.1 %) |

*Table 5.5 Risk impact of the quantified EOC spilt fractions in the two pilot studies*

Note:

The two studies had a different scope: internal and area events for Pilot I, internal events for Pilot II. The CDF measures refer to these scopes correspondingly.

### 5.8.2 PSA-INFORMED REVIEW OF EMERGENCY PROCEDURAL GUIDANCE

*Background*

In NPPs, the procedural guidance in response to abnormal, emergency and accident conditions is subject to thorough analysis and validation from multiple perspectives and at different design stages /ANS 08/, /NRC 00/. Potential improvements in the content of these procedures are continuously investigated and implemented as necessary.

In this context, PSA provides an opportunity to enhance the content of the plant procedural guidance, typically the

Emergency Operating Procedures (EOPs) and Accident Management (AM) procedures, which guide most of the actions modelled in the PSA. Indeed, the plant PSA provides a quantitative characterization of the risk profile, in terms of risk figures-of-merit such as the CDF as well as the important risk contributors. Indeed, the PSA-based determination of important human actions, systems and accident sequences is one of the dimensions to be considered when determining the operational conditions for human factors verification and validation, according to Chapter 11 of /OHA 12/

This paragraph presents a procedure based on the use of PSA information to prioritize and inform the review of the plant EOPs and AM procedures. PSA supports the procedure presented in this section by identifying:

- the most risk significant operator tasks in response to abnormal, emergency and accident conditions,

- the most risk significant PSA scenarios (initiating events and equipment and/or preceding operator failures) where these tasks are required,

- information on the development of accident scenarios over time (from the thermal hydraulic analyses underlying the PSA accident sequence models and success criteria definition), and

- a characterisation of the operator performance conditions during these tasks (from the HRA).

Generally speaking, the contribution of PSA to the review procedure discussed here is twofold. Firstly, PSA supports the prioritization of the procedure review effort on the most significant PSA contributions (operator tasks and scenarios). Secondly, PSA provides information on the evolution of specific accident scenarios in which the procedural guidance will be applied.

The review procedure presented in this paragraph emphasizes the adequacy of the guidance for specific scenarios. It examines, for instance, the expected indications, their timing, the procedural guidance criteria, and the expected timing of the operators' progression through the guidance. It thus has a narrower scope than the review of operating and emergency operating procedures specified by the U.S. NRC in its Standard Review Plan /NRC 07/ and more generally of the Human Factors Engineering Program /OHA 12/ The latter emphasize the review of the comprehensive program for development, implementation and maintenance of the procedural guidance, ultimately to make sure that the procedural guidance thereby produced is technically accurate, comprehensive, consistent, explicit, easy to utilize, and validated. Along the same lines, the IAEA good practices with respect to the development and use of NPP procedures /IAE 98/ addresses their verification and validation, emphasizing their general applicability across a variety of scenarios. /IAE 98/ includes example checklists for verification and validation that address different dimensions of the procedural guidance (ergonomics, technical accuracy, usability, clarity, usefulness, etc).

Note that the concepts behind the presented procedure can be generally applied to the review of the Severe Accident Management Guidance (SAMG) as well. However, due to the character of these guidelines and of the plant conditions in which these are expected to be applied, the topics for SAMG review may be different, as well as the recommended level of procedural guidance details.

An important feature of the approach is that it evaluates the guidance on specific accident scenarios as defined by the dominant PSA contributors. The latter information is important because it allows adopting a complementary perspective compared to that followed in the procedural guidance development. Indeed, the guidance is generally developed with the

aim of coping with multiple scenario variants. The PSA still provides specific variants and identifies the most-risk significant among these in which the guidance will be applied. Once the quality of the procedural guidance on the specific scenarios is assessed, the decision of implementing possibly identified improvements has to be determined on a case-by-case basis considering the implications for its general applicabiity.

*Method: Procedure for a Risk-informed Review of the Emergency Procedural Guidance*

The first step of the procedure is the identification of the most risk significant operator actions. The risk importance measures associated to the actions are used for this purpose, the Fussell-Vesely (FV) importance or risk achievement worth (RAW) importance. At least two scopes need to be considered: contributions to 1) the internal events CDF and 2) the total CDF also considering area events, e.g. fire and internal flooding, and external events, e.g. seismic or severe weather, should be considered. The selected FV and RAW thresholds determine the analysis effort and the risk implication of the findings. The appropriate threshold values depend on the risk profile as well as on the review resources available.

The next step is the analysis of the most important minimal cut sets (MCSs) that include the operator actions selected in the previous step. Again, a threshold (generally related to the MCS CDF contribution) has to be defined to focus the review on risk significant contributors. Similar considerations on the implications of the threshold definitions as in the previous step apply here. The MCSs provide information on the specific scenarios in which the operator tasks are required. The MCS analysis should include the description of the PSA scenarios (initiating event and additional failure or events) and of the timing of relevant events, actuations, and appearance of indications.

The first two steps allow defining the operator actions and the specific PSA scenarios for which the procedural guidance is reviewed. The review questions for each of the identified tasks and scenarios are given below. The purpose of the questions is to guide the review to follow the operator response over the whole scenario evolution, following and evaluating all procedural transfers from the initiating event to the steps with the implementation details for the task. (Table 5.6 below gives some guidelines for addressing these.)

1. Is the action instructed in any procedure?
2. Is the procedural criterion for taking action met in the scenario?
3. Is there adequate guidance for reaching the relevant step of the guidance?
4. Is there adequate guidance for transfer to appropriate procedure section?
5. Is there adequate guidance for choosing the appropriate procedure (among different alternatives)?
6. Is there adequate guidance for reaching the transfer to the applicable procedure?
7. Is the procedural guidance on execution details?
8. Is there procedural guidance on execution details dispensable?
9. What is the adequacy of further guidance details (consistency, priority etc.)?

The key indication for the evaluation of the adequacy of the guidance as guided by the above questions is the available indications in the specific scenarios and their timing of appearance, relative to the indication criteria mentioned in the procedural guidance and

the expected timing of the operators progressing through the guidance.

| Review Question | Guideline for Assessment |
|---|---|
| 1. Action instructed in applicable procedure? | If yes, indicate the step at which the action is instructed. |
| 2. Are the procedural criteria for taking action met in the scenario? | This question relates to the criteria specific for the performance of the action as indicated in the procedure step.<br>The criteria should be evaluated with reference to the specific scenario. Emphasis should be placed also on the time when the criteria are met. |
| 3. Adequate guidance for reaching the relevant step of the guidance? | This question relates to the procedural path to the relevant step instructing the action (within the procedure supporting the action under analysis).<br>The transfers and key decision steps in the procedure path should be evaluated with reference to the specific scenario in terms of the plant conditions, available indication and speed of progression. |
| 4. Adequate guidance for transfer to appropriate procedure section? | In case the procedure includes multiple sections, this question evaluates the transfer to the appropriate section. |
| 5. Adequate guidance for choosing the appropriate procedure (among different alternatives)? | This question refers to the transfer to the appropriate procedure. The transfer step may include multiple procedures (applicable under different criteria or priorities). This question evaluates the transfer to the appropriate procedure (criteria and/or priorities).<br>Criteria and priorities are to be evaluated with specific reference to the scenario analysed. |
| 6. Adequate guidance for reaching the appropriate transfer? | This question relates to the procedural path into the procedure containing the transfer.<br>Note: questions 4-6 should be repeated for all procedures and procedural transfers involved in the scenario response. |
| 7. Procedural guidance on execution details? | This step should include a summary of the relevant steps required, with explicit reference to whether they are covered or not by the procedural guidance. Consideration shall be given to whether the guidance allows completion of the action within the available time as per the scenario progression. |
| 8. Procedural guidance on execution details dispensable? | In case some / all execution details are not included in the procedure, this question evaluates whether their omission can be justified (e.g. typically, because execution is considered skill-of-the-craft or / and because it is included in the system operating procedures) |
| 9. Adequacy of further guidance details (consistency, priority etc.)? | This question addresses aspects such as:<br>-Consistency of entry criteria and conditions for taking the action. This relates to whether these criteria and conditions match and/or the reasons for mismatch and whether all transfers to the relevant procedure have the same transfer criteria (or warnings) and/or the reasons for mismatch.<br>-Is there any conflict among priorities in the scenarios? E.g. multiple procedures being simultaneously applicable without clear prioritization.<br>-Potential for misinterpretation of the entry criteria and conditions for taking the action (e.g. due to unclear formulation)<br>Reference to supportive information (e.g. graphs, tables, location of required equipment etc.) |

*Table 5.6 Guideline for the assessment of the review questions*

*Results: Types of Potential Improvements Typically Identified*

Some of the most recurrent types of potential improvements found from our review experience address the following issues:

- Missing details for carrying out (implementing) specific operator actions

(when execution steps are not obvious) or missing transfers to the system operating procedures providing these details;

- Applicability of entry criteria into EOPs and AMs in specific accidents during shut-down conditions;

- Need for early preparation for implementation of alternate measures in scenarios with fast progression (generally relevant for AM actions).

It is worth pointing out that these improvements refer to specific scenario conditions, for which the procedural guidance, designed to cope with a larger set of scenario variants, may not be optimal. As mentioned earlier, the decision to finally implement the improvements depends on the implications that the changes may have on the general applicability of the procedures. Indeed, the optimization for a specific scenario may not be the best decision for the overall procedure applicability.

In the following, selected examples of such improvements are given.

*A. Early Preparation of Alternative Measures*

A typical finding for this type of review relates to the injection from alternative water reservoirs (external to the plant site) and/or fire water system sources. Generally, aligning these sources requires performing local actions (i.e. not carried out from the main control room) involving manual operation of valves, connection of hoses, alignment of movable pumps – depending on the cases. Based on the PSA-informed review, it was possible to identify scenarios for which early preparation of these options can further increase the margin for success of alternative injection.

The first example relates to a BWR. From the PSA importance measures, the operator action modelling alignment of alternate injection resulted in a relatively large FV importance (say, above 0.1). Note that in many cases these actions have quite low RAW values because their estimated failure probabilities are large (generally, above 0.05). The action was selected for review based on its FV importance. The review of the MCSs including this action showed that the scenarios mostly contributing to the CDF are initiated by a total loss of Feedwater (direct loss or due to support system failures), with additional, independent failures of all the high- and low-pressure injection systems (originated from different combinations of events).

The response to the initiating event is guided by the main post-scram procedural guidance, which, in case of loss of feedwater, directs the operators to take actions to maintain the reactor level with the available emergency high- and low-pressure systems (which are automatically actuated by the respective low-level signals). The procedural guidance is recursive and the instruction to maintain the reactor level between two different reference set-points is repeated in a number of places (the specific set-points may differ). Alignment of the alternate injection is instructed if the reactor level cannot be maintained above a specific low-low level (which corresponds to the procedural transfer criterion to the pertinent AM procedure).

The accident scenario was analysed considering the relevant event timing (parameter evolutions, set points triggering and system actuations) from the thermo-hydraulic analyses supporting the PSA. It was found that, in the specific scenario, the procedural guidance may benefit by providing instructions of early preparation (early referring to a reactor level height higher than the low-low condition corresponding to the transfer to the AM procedure) of the alternate sources (e.g., hose connections) so that the injection can be started as soon as the corresponding procedural criteria are met.

It is important to remember that this potential improvement is specific to the analysed scenario (loss of feedwater with additional loss of all high- and low-pressure injection systems). The final decision to implement should be made with care. On the one hand, the scenario is among the most important contributors to the CDF according to the PSA, even if per se very unlikely. On the other hand, there may exist other scenarios for which early preparation of alternate injection could distract from the priority of maintaining level with other available systems; typically, these scenarios are more likely because they involve fewer component failures subsequent to the initiating event.

Another example, also related to preparation of alternate injection for a BWR, relates to the prioritization of different injection options. As in the first example, the PSA action modelling alternate injection was selected because of its relatively high FV contribution. Again, the action is modelled in scenarios involving total loss of feedwater with failure of all high- and low-pressure injection emergency systems (induced by a large internal flood affecting the whole lower level of the reactor building).

The corresponding AM procedure is not specific for alternate water reservoirs (external to the plant site) and/or fire water system sources, but includes about 20 options, among which the direct injection via the fire water system and/or from the external reservoir (presented after about 10 options). The other options include different alignments involving combinations of emergency systems among themselves and between emergency and alternate systems. The various options require different systems being available, different levels of permissions (e.g. from emergency response leader), and different levels of complexity for the alignments.

In the specific scenario analysed, which involves the total unavailability of the emergency options, alternate injection is the sole option. Without a proceduralised prioritization of the options, the operators would have to (quickly) assess the feasibility of a number of these, before getting to the appropriate alignment. As the result of the review, a prioritization of the options based on the expected unavailability of the systems, the complexity of the alignments and the permission requirements could be suggested.

Again, this potential improvement has been derived specifically for the analysed scenario: its appropriateness has to be assessed at overall level of accident response. In particular, the prioritization of the fire water injection in this scenario (total unavailability of the injection systems) allows its timely alignment. However, in other scenarios, typically with partial unavailability or/and functional failures different from the one considered (due to large internal flood), other options involving alternate alignments of the emergency systems may be more appropriate. This indeed requires careful evaluation by plant specialists.

### *B. Entry of Criteria Into EOPs and AMs During Shutdown Conditions*

The first example of this type refers to the PSA action of injecting makeup into the reactor, in case of a loss of coolant accident (LOCA) from the residual heat removal (RHR) system into the suppression pool (in a BWR). The PSA scenario is initiated while the plant is in the refueling phase, with the reactor well flooded.

The relevant procedure for LOCA events during shutdown ("RHR failure during shutdown"), applicable for cases of reactor vessel head off, emphasizes the restoration of RHR cooling covering the different cases of reactor water level below the vessel flange and of the reactor well flooded. For the reactor level restoration, the procedure transfers to the level control instructions of the main post-scram procedure. The latter procedure is specific for at-power conditions and refers to reactor level indications far

below the height reached by the water when the reactor well is flooded. The result is that the operators would have to anticipate the entry criteria to avoid waiting until the water level in the reactor reaches the set point low level before starting with the injection. If the LOCA is initiated with the reactor well flooded, this entails a long delay before actions to restore level are taken.

The procedural guidance review led to the recommendation of developing (or, adjusting as necessary) procedures with entry criteria directly relevant for LOCA and loss of RHR cooling events during shutdown states with reactor vessel head flooded and with vessel head on (the latter condition arising from a similar review case, relative to plant shutdown conditions with vessel head on).

The last example of this type refers to a PWR and relates to the accident management action of injecting fire water into the reactor vessel during shutdown conditions (while the reactor coolant system is at mid-loop). The accident initiates with a LOCA from the vessel to the fuel pool due to misalignments during the operations of aligning one RHR train from fuel pool cooling to reactor cooling. The action of injecting fire water is instructed in the dedicated AM procedure, entitled "Injection of fire-extinguishing water into the reactor pressure vessel".

The review of the procedural guidance in support of the specific scenario (LOCA during shutdown) found no transfer from the applicable emergency operating procedure ("Accidents during shutdown conditions") to the specific AM procedure. The review resulted in the suggested improvement that the provision of the direct transfer also for accidents during shutdown conditions (as it is the case for accidents initiated while the plant is at power) would be beneficial for the operators - although the fire water option is well known to the operators, independently of the presence of the explicit transfer.

## 5.9 Ukraine

### 5.9.1 COMMON CONTAINMENT FOR THE REACTOR SYSTEM AND THE SPENT FUEL POOL OF VVER

*Question/Issue*

In Ukraine, for Level 2 PSA the large release frequency (LRF) risk metric is applied while the release timing characteristics (i.e., early or late release) are not considered. Large release is defined as the one requiring public evacuation at the boundary of the protection area.

In the frame of a full scope PSA, all events except those from seismic hazards for all reactor and SFP POSs were considered. As results of the PSA, the CDF and spent fuel damage frequency (SFDF) were quantified. Since Level 2 PSA for the reactor core and for the SFP were performed separately, two individual LRF values were obtained for these radiation sources, one for the reactor core and another one for SFP. However, considering that for VVER plants designs both the reactor system and SFP are located inside a common containment, the progression of accidents in the reactor system and in the SFP may both contribute to the conditions inside the containment affecting its integrity. Thus, for example, separate analyses of severe accident sequences for the reactor core do not account for additional hydrogen production from the SFP. It shall also be noted that the same systems and components may be used in the reactor core and the SFP accident sequences.

*Approach/Procedure*

The description above allows to conclude that in Level 2 PSA the combined analysis of accidents for the reactor core and for the SFP is more appropriate for VVER designs, and the integration of separate Level 2 PSA models is needed for the correct

interpretation of the PSA results in terms of compliance to quantitative safety criteria.

Since Level 1 PSA results are interpreted using CDF and FDF metrics, correct accounting of both sources requires to extend the existing Level 1 PSA studies to incorporate the end states that account for core and SFP fuel damage timing (which may be significantly different for accidents in the reactor core and in the SFP). For extended mission times this question becomes even more complicated and requires additional evaluation.

Concluding the above, to establish an appropriate basis for Level 2 PSA of NPPs with the SFP inside the containment it seems reasonable to use those time-dependent CDF and FDF values which allow to reflect differences in the chronology of accident progression for the reactor core and the SFP in cases that lead to initiating event occurrences affecting both of these radiation sources and to identify an appropriate set of end states that allows to account the generation of release products in each of the sources (and their combination) in Level 2 PSA. This task could be facilitated by incorporation of such Level 2 PSA metrics as LERF and large late release frequency (LLRF) in Ukrainian PSA-related requirements and methodologies. As a result, the long-term influence of SFP accidents most likely would be associated to the LLRF range.

For early containment failure caused by severe accidents progression in reactor system the contribution of radioactive releases from the SFP shall also be considered. Depending on the SFP fuel damage timing this can contribute to LERF or LLRF.

Alternatively, to account an influence of accident progression in the reactor core on the SFP and vice versa the events that potentially affect both radiation sources could be excluded from existing PSA models and analysed in a dedicated PSA model. Then the modified (reduced) PSA models need to be re-quantified. As a result, correct values of the LRF will be obtained. However, an application of time-dependent metrics in Level 1 and Level 2 PSA and the use of a combined PSA model to estimate PDS and source term frequencies seems to be more appropriate (especially if a further extension to Level 3 PSA is foreseen).

*Results*

The above-mentioned issue has been indicated for the operator during the full scope PSA review process and was categorized as an industry-wide one. To address the issue the working procedure is developed that involves:

- Adjustment of the reactor system and SFP models to ensure correspondence in POSs, system models, basic events, CCFs of systems and components which are used both for reactor core and SFP fuel accident sequences;

- Identification of initiating events and accident sequences that affect both the reactor core and the SFP (e.g., total station blackout, loss of essential service water, internal fires in I&C compartments);

- Deterministic analyses to provide information on overall accident progression and timing;

- Evaluation of operator actions to be performed to cope with accidents that affect the reactor core and the SFP, update of human reliability analysis;

- Modelling of Level 1 PSA event trees for events that affect both the reactor core and the SFP taking into account that the same systems and components may be needed in accident sequences for the reactor core and the SFP;

- Identification of plant damage states resulting from the accident sequences affecting both the reactor core and the SFP, development of corresponding containment

event trees and identification of release categories;

- Re-quantification of the model.

The activities mentioned above are to be performed for the pilot unit. Following the analysis of the results and their comparison with the CDF/FDF/LRF values obtained previously in separate calculations for the reactor core and the SFP, the decision on the corresponding update of the PSA models for other operating units will be made.

## 5.10 United Kingdom

### 5.10.1 PSA CURRENT TOPICS OF FOCUS/DEVELOPMENT IN THE UNITED KINGDOM CIVIL NUCLEAR INDUSTRY

PSA development in the United Kingdom civil reactor sector is generally split into two areas (a) Periodic and general updates of existing station PSAs to modern standards and (b) Development of new PSAs for prospective new reactor designs to the United Kingdom. For both existing and prospective new reactor designs, recent areas of development include the following:

- Integrated fault tree and event tree modelling, including conversion/update of 'spreadsheet' based PSA models;

- Dependency / common mode failure (CMF), including dependencies between initiating events and protection/mitigation claims;

- HRA including the consideration of dependencies between multiple operator and ad-ministrative claims;

- Use of PSA for risk-informed decisions on proposed design changes, maintenance changes and operational changes;

- Risk monitors, i.e. development of station-based PSA tool for assessing changes in risk with reduced plant availability.

Of particular interest in the PSA development of new reactor designs is the potential inclusion of modelling for:

- Single hazards and hazard combinations, e.g. fire and flood;

- Inclusion of SFP and reactor/SFP combinations events;

- Multi-unit PSA modelling.

### 5.10.2 EVOLUTION OF PSA

The United Kingdom has been undertaking reactor PSA work since the 1970's. Early work on the PSA for the steam generating heavy water reactor (SGHWR) at Winfrith eventually led to its adoption for all nuclear reactors in the United Kingdom and then to other major United Kingdom nuclear facilities, particularly in the wake of the Three Mile Island incident in the United States. These PSA studies are undertaken and extensively reviewed by the regulator before each reactor is allowed to commence operation and then every 5/10 years during operations at routine PSRs.

PSA has also been used to support the GDA prospective (new) to United Kingdom re-actor designs.

PSA is one of the three fundamental techniques (the others being design basis analysis and severe accident analysis (SAA)) used to underpin fault analysis on United Kingdom reactors. This is illustrated in the step diagram in Figure 5.5 below (Figure 1 from ONR Safety Assessment Principles (SAPs)). However, there should be a clear relation be-tween the fault sequences used in the DBA, the accident states and scenarios used in the SAA, and the fault sequence development of the PSA.

**FIGURES**

Figure 1: Schematic showing the general ranges of applicability of the 3 methods of Fault Analysis.

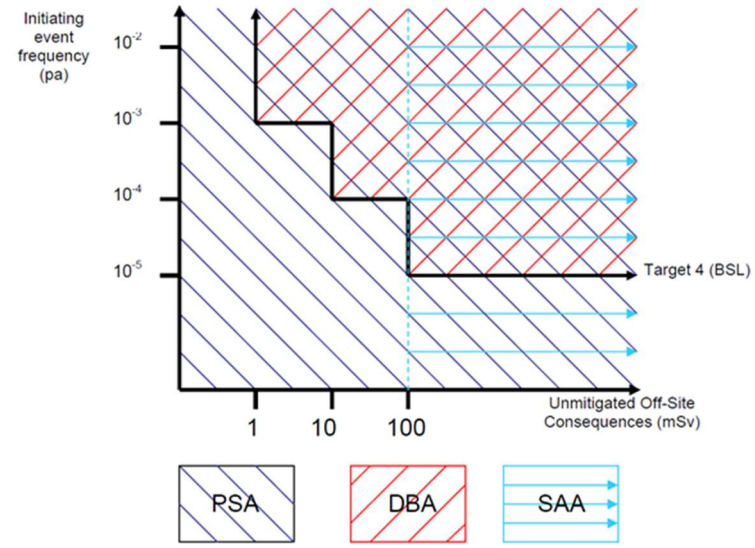


*Figure 5.5 Schematic showing the general ranges of applicability of the three methods of fault analysis*

The United Kingdom regulatory authority – the Office for Nuclear Regulation (ONR) – has published its Safety Assessment Principles (SAPs) which are intended for use by its inspectors when they assess the safety of nuclear facilities; these are supported by Technical Assessment Guides (TAGs) in different subject areas. The United Kingdom regulatory regime is non-prescriptive, and the operator is at liberty to demonstrate safety in a way different from that described in the SAPs and TAGs. There is, however, a legal duty on all licensees to reduce risks so far as reasonably practicable (SFAIRP or ALARP); this is not specific to the nuclear industry.

Having said that, for new NPPs, the regulatory expectation is for a full scope (all POSs, SFP, non-reactor faults, internal and external hazards) Level 1 to 3 PSA to be performed.

Current United Kingdom practice is that PSA is used to understand the overall risk pre-sent from a design and to compare this with the licensee's own numerical targets. ONR will assess the risk against its numerical targets as set in the SAPs (Target 4 for DBA and Targets 5 - 9 for PSA). As mentioned above, it should also be used to support the demonstration that risks from such facilities are ALARP– the fundamental principle governing safety risk management set out in United Kingdom Law.

The primary SAP assigned to PSA (FA.10) states "Suitable and sufficient PSA should be performed as part of the fault analysis and design development and analysis." This also captures the equally important aspect role of PSA i.e. that PSA should inform design development. The above is an extract from the SAP addressing the need to undertake PSA. This is complemented by similar principles addressing the validity, scope and extent as well as the adequacy of (system) representation by the PSA model(s).

In essence, the PSA should assist the designers in achieving a balanced and optimised design; it should directly relate to the current/existing facility (design), reflect site information, data and documentation, and should cover all significant sources of radioactivity, all permitted operating states and all relevant initiating faults at a level of

detail sufficient to ensure that it is realistic, and all dependencies are captured.

PSA modelling in existing United Kingdom civil nuclear facilities meets these principles in part by periodic reviews to incorporate, where appropriate, any changes to plant de-sign and configuration as well as updates to data based on operational experience. PSA models are also increasingly being used to provide risk-informed decision-making when assessing potential design changes, operational procedure changes as well as changes to testing and maintenance intervals.

PSA development to 'modern standard' for a number of existing facilities over the last few years has involved the conversion of spreadsheet based PSAs to fully integrated fault tree and event tree models. As well as providing clearer representation of fault sequence progression, these updated models better capture dependencies between initiating events and protection and mitigation claims, including potential dependencies be-tween multiple operator and administrative claims.

For PSA models being used to support the GDA process for prospective United Kingdom reactor designs, these new models have explicitly been developed to provide a wider usage of application, including usage as a design development tool. The scope of these new PSA models has also been extended to include consideration of all operational states, e.g. at power and shutdown; the incorporation of internal and external hazards, including hazard combinations, e.g., fire and flood, and the SFP and reactor-SFP combination events. The GDA considers a single unit at a generic representative United Kingdom site. All the current proposed new developments in the United Kingdom comprise multiple units adjacent to existing sites which have either operating reactors, reactors undergoing decommissioning or other nuclear facilities. Consequently, consideration is being given to multi-unit PSA, particularly in relation to hazards and loss of grid faults.

### 5.10.3 UNITED KINGDOM NPP FUEL ROUTE PSA DEVELOPMENT TO MODERN STANDARDS

As a result of PSRs conducted for two of the United Kingdom power stations it was decided to update the fuel route PSA to modern standards and provide a consistent approach and level of detail for the two stations.

It was considered that there would be a benefit to have a common model between the two stations to allow a pooling of experience and harmonization of approach going for-ward.

The fuel route at each station is defined by its own nuclear safety case claims. 14 safety cases in total required to be updated to "modern standards".

The PSAs supporting each of the safety cases were not considered to be in a modern format and were generally in the form of Hazard and Interlock Schedules (similar to fault schedules). These were originally developed to cover both stations, but were subsequently updated independently, leading to some large disparities between stations in how the PSAs for the same facility were presented.

The strategy used to develop the PSA models for the two stations was based on the following:

- Development of a set of assessment criteria ("best practice");

- Review of the existing fuel route PSAs against these assessment criteria;

- Development of solutions to remedy any shortfalls found;

- Implement solutions and update the PSAs (14 cases).

Establishing the "best practice" assessment criteria was based on the operating company's internal guidance and standards as well as national and international guidance and standards (cf. /IAE 06a/, /ANS 02/ and /ONR 24/). The following assessment criteria were considered:

1. General Scope – to ensure that the PSA objectives and scope are clearly defined.

2. PSA Methods – to ensure that the methods and procedures adopted are adequate to demonstrate validity of the PSA process.

3. Fault Identification – to demonstrate that all relevant initiating events have been covered and adequately addressed.

4. Accident Analysis – to ensure that fault sequence modelling and the identification of the end sequences for each fault provides adequate representation of the faults and hazards.

5. Success Criteria – to ensure that protection against each identified hazard is sup-ported by relevant and sufficient deterministic analyses.

6. System Analysis – to demonstrate that the method and adequacy of the systems/interlock modelling is suitable for a PSA application.

7. Human Reliability – to demonstrate that all of the operator actions that have the potential to lead to an accident as well as those that could mitigate an accident have been systematically identified and addressed.

8. Component Data – to demonstrate that failure data is applicable to the fuel route equipment and a process is in place to capture plant specific/generic data.

9. Dependent Failure – to ensure that the method and adequacy of dependent considerations is sufficient to capture inter and intra system dependencies.

10. Quantification – to ensure that the results have been produced and that modelling assumptions are clearly defined.

11. Conclusions – to ensure that the documentation captures the key elements of the process and provides adequate representation of the results to ensure compliance with the Nuclear Safety Principles.

Each of the existing fuel route PSAs were reviewed against these assessment criteria and solutions to remedy any shortfalls were developed.

The first major step was to develop/update the initiating event fault schedules and to 'harmonise' the fault schedules across the two stations. This harmonisation process involved a cross comparison of faults across the two stations to ensure all appropriate faults were included for both stations. The fault schedules were also structured to ensure:

- Ease of updateability;

- Interlocks can be easily found;

- Station personnel can easily manipulate the schedules to examine 'Defeat of Interlocks' and understand impact:

Once the fault schedules were produced then faults with the potential for off-site radio-logical releases were modelled in RiskSpectrum using integrated fault tree and event tree models.

Fault trees were generated to group together similar initiating events for input into each event tree.

Event trees were then used to model the accident sequences post fault, with faults trees also being developed to model protection systems and systems required post fault (e.g. decay heat boilers).

Summated off-site risk by dose band (i.e. magnitude of radiological release) were then calculated using RiskSpectrum and compared with the licensee's target frequencies.

*Outcome*

- Five years of effort with a maximum of ten PSA engineers;

- Well documented safety case underpinned by PSAs with:

- more clarity on dominant faults,

- easily updated,

- auditable,

- impact of design changes reviewable using the models.

- easier to use by station personnel, and

- a team of experienced fuel route safety case / PSA engineers with extensive fuel route plant knowledge.

### 5.10.4 UNITED KINGDOM NPP NEW BUILD GENERIC DESIGN ASSESSMENT PSA

Hitachi-GE proposed to build ABWR (Advanced BWR) plants in United Kingdom, based on an enhanced Japanese ABWR design – the United Kingdom ABWR – and currently the Government's preferred approach is for new designs to first undergo the Generic Design Assessment (GDA) before site licensing for construction at specific sites.

The generic Pre-Construction Safety Report (PCSR) was the main submission for GDA supplied by Hitachi-GE /HIT 17/. The PSA for United Kingdom ABWR was provided as part of the PCSR and provided an integrated and structured analysis that combined engineering design and operational features in a consistent framework used to assess the plant risks, to identify potential plant vulnerabilities and to quantify the public and worker risks.

The objectives of the United Kingdom ABWR GDA PSA were;

- to quantify the overall risks represented by the facility to allow comparisons to be made against its own and ONR's Risk Targets as defined in the Safety Assessment Principles (SAPs) /ONR 14/ and other risk metrics used internationally, including CDF and LRF,

- to assess and document the strengths and weaknesses of the design,

- to support the evaluations of potential modifications to the plant or improvements in operating conditions as part of ALARP demonstration, and

- to support other applications of safety decision-making.

The elements quantitatively studied were as follows:

■ Detailed PSA for:

- Internal events at power (Level 1 – Level 3);

- Internal events during shutdown (Level 1 – Level 3);

- Internal events for SFP (Level 1 – Level 3);

- Internal fire at power (Level 1 – Level 3));

- Internal flooding at power (Level 1 – Level 3);

- Seismic events at power and for the SFP (Level 1 – Level 3);

- Fuel route (Level 1 – Level 3);

■ Scoping analyses for:

- Internal fire during shutdown and for the SFP (Level 1);

- Internal flooding during shutdown and for SFP (Level 1);

- Seismic hazards during shutdown (Level 1);

- Bounding assessments to determine the risks from:

- Tornado missiles (Level 1 – Level 2);

- Turbine missiles (Level 1 – Level 2);

- Accidental aircraft impact (Level 1 – Level 2);

- Events not leading to core (fuel) melt:

- Level 1 PSA success sequences; (Level 3);

- Non-reactor faults (e.g., fuel route, release from radioactive waste treatment systems) (Level 3).

The summed CDF, LRF and LERF for the GDA United Kingdom ABWR were 4.3 E-06 /ry, 1.6 E-06 /ry and 1.1 E-06 /ry, respectively.

Internal events (at power, shutdown and SFP) contributed 17 % to the risk of core damage. The risk of core damage from internal fire, internal flooding and seismic hazards were shown to dominate the current risk results, with contributions of 12 %, 42 % and 29 % of the overall CDF, respectively.

Similarly, internal events (at power, shutdown and SFP) contribute 10 % to the risk of large release. The LRF from fire, flooding and seismic hazards are shown to dominate the current risk results, with contributions of 17 %, 11 % and 62 % of the overall LRF, respectively.

The GDA United Kingdom ABWR PSAs were performed using the design information that was available at the time analysis was performed. This by necessity resulted in simplification/conservatism being made in the assessments. This is particularly true in the case of the hazards assessments where some aspects of the detailed design, such as cable layouts, were not finalized.

Multiple peer reviews were organized and performed for the United Kingdom ABWR PSA using a similar process as performed in the United States (i.e., the NEI 05-04 process /NEI 08/). Their purpose was to demonstrate that the United Kingdom ABWR PSA meets international PSA standards, including adequate methods and a complete PSA scope i.e., modern standard.

The United Kingdom ABWR PSA was reviewed against the Technical Assessment Guide (TAG) developed by ONR /ONR 24/, ASME/ANS PSA standards (cf. /ANS 09/, /ANS 13/, /ANS 14/, /ANS 14a/ and /ANS 17/) to help determine the overall adequacy of the PSA by international experts /HEN 17/. It was confirmed that large part of requirements is met for Capability Category II or III in the ASME/ANS PSA standard.

As part of the GDA United Kingdom ABWR PSA, a review for potential plant improvements was undertaken using the PSA results. In addition, an integrated review of design options and possible actions needed to demonstrate ALARP was performed across all fault groups. The purpose of this review was to identify any design options and/or possible action items that were present in multiple faults in order to recognize those options/items that may have more of a significant impact than others. To support the integrated review, the cut set file of each PSA was merged into single cut set file for CDF and LRF, and integrated importance analysis was performed.

Examples of risk-informed improvements are provided below.

- Internal events at power PSA identified a specific pipe segment which had relatively large contribution to the risk from Interfacing System LOCA (ISLOCA). Although the CDF and LRF from ISLOCA were already small, a recommendation was raised from the PSA to increase the thickness of that pipe segment for further risk reduction. That recommendation was as a

result of considering the consequence: a core damage following an ISLOCA could directly lead to large release due to the containment bypass.

- The shutdown PSA identified heavy load drop onto the refueling deck, reactor well or dryer/separator pit as one of the dominant contributors to the FDF during shut-down. This insight was informed to the generic design of fuel handling machine and reactor building overhead crane which introduced provisions against heavy load drop.

- The internal events SFP PSA identified a human -induced initiating event that was potentially more significant than any other initiating event. This insight was provided to the designers, and it was agreed to introduce measures to avoid this initiating event in the detailed design phase.

*Outcome*

Hitachi-GE developed the United Kingdom ABWR PSA to provide a demonstration of the compliance with its own numerical risk targets and those defined in ONR's SAPs and to support the ALARP assessment.

The internal events PSA results helped demonstrate that the basic design and design features of the United Kingdom ABWR are ALARP.

The above summary is based on. /HIR 18/. The PSA submission for the GDA and its assessment by ONR can be found in /HIT 17/ and /ONR 17/, respectively.

### 5.10.5 UNITED KINGDOM NPP NEW BUILD GENERIC DESIGN ASSESSMENT LEVEL 3 PSA

A full scope PSA was provided as an integral part of the safety case for the United Kingdom ABWR GDA, and this included a Level 3 PSA. The main objectives of the Level 3 PSA for GDA were to provide a demonstration of the compliance, for a single unit United Kingdom ABWR, with the applicant's numerical risk targets and those defined in ONR's Safety Assessment Principles (SAPs) and to support the ALARP assessment.

The United Kingdom ABWR is the third reactor design to complete the GDA process, but it is the first to include a Level 3 PSA and, in respect of some accident scenarios involving both the reactor core and the SFP, is the first-of-a-kind application of modern-standards Level 3 PSA in the United Kingdom.

The high-level methodology for demonstrating the acceptability of the postulated United Kingdom ABWR accidents, for members of the public, was set out as part of the GDA. The methodology involves (i) performing semi-probabilistic (probabilistic aspect of meteorological conditions not considered) dose calculations for the assessment against facility dose bands (using the United Kingdom Atmospheric Dispersion Modelling Liaison Committee (ADMLC) methodology /NRP 79/, /NRP 81/, /NRP 83/ implemented in soft-ware referred to as PUMA), and (ii) fully probabilistic consequences calculations for the assessments against the risk targets (using an updated version of PC COSYMA //HPA 07/). Initially, a 'demonstration of methodology' was completed using available data for the existing Japanese ABWR design and submitted to ONR. During the course of the GDA, the methodology was refined as a result of model developments and to address specific questions from ONR (in the form of Regulatory Queries (RQs)).

The final methodology was subjected to a peer review, considering the requirements of the SAPs and the draft ASME/ANS Level 3 PSA standard /ANS 16/. The full scope PSA and its results also provided supporting information to enable a demonstration of 'Practical Elimination' of early or large fission product release for the design to be made /ANG 18/.

The PSA submission for GDA and its assessment by ONR can be found in /HIT 17/ and /ONR 17/ respectively.

# 6 RECOMMENDATIONS FROM THE EXPERT GROUP'S POINT OF VIEW

Representing a flexible and versatile analytical tool, PSA has been continuously evolving and currently is able to consider and incorporate plant modifications, new events or new knowledge. Depending on the type of work performed by the TSOs, there are two types of recommendations from the ETSON PSA experts summarized in the following:

**Recommendations resulting from lessons learned from reviewing PSA**

- For a better credibility of the PSA results, independent reviews are important. More-over, the review accompanying the elaboration process of a PSA (simultaneous review) seems to be more efficient than a review performed after the PSA has been completed (follow-on review). However, in the case of a simultaneous review, a for-mal interaction process is needed between PSA developers and PSA reviewers, to adequately improve the PSA model during the development/ update /upgrade process. Moreover, for a simultaneous review to be effective, a high quality of the avail-able PSA documentation (and related presentations and discussions) is needed during the whole PSA elaboration process, while access to the PSA model itself is a significant additional advantage;

- The development of a PSA model by reviewers, independent from the PSA developers, is obviously an appealing approach. However, maintaining a full-scope independent PSA requires significant resources. Instead of developing the whole PSA model, the reviewers often make use of limited-scope analyses, focused on areas of interest, which can still provide valuable insights into the review process.

- A close interaction with knowledgeable non-PSA experts, e.g., plant inspectors, developers of procedures, training instructors, etc. is very helpful in acquiring knowledge of the technical systems, operational practices and procedures, including recent developments in the domain;

- Access to the whole PSA model of the utility by the regulator is desirable (direct or by utility nominated contact). Without access to the whole model, it is difficult to con-sider the effect of even minor changes. The regulator may also have a nominated contact/organisation

who holds a copy of the model and reviews this when required on their behalf.

- Before performing a peer review to check conformity with the requirements of national standards or international guidance, (i.e., high-level requirements and the more detailed Supporting Requirements) that are developed for the different PSA capability levels (for example, so-called PRA Capability Categories I, II and III in ASME ANS guides), it is quite important to identify, as much as possible, the PSA applications for which the PSA will be used, in order to determine, during the peer review, the applicable capability category to aim at for each requirement. If this is done beforehand, the reviewers can focus on those findings and recommendations that are most relevant to the next updating of the study, in view of the intended PSA applications. Even a simple PSA can be used for identifying several important safety improvements (e.g., case of EPR PSA, where although the PSA results were not the only basis for making decisions, the preliminary PSA has played a role in several design improvements). On the other hand, aiming at a global capability for seemingly any future applications, or using some selection criteria a-posteriori (e.g. based on the expected impact on PSA results or on intended PSA applications), may lead to less substantiated findings and recommendations for PSA improvement.

- Peer review against national standards or international guidance (e.g., ASME, NUREGs, IAEA) is still to be complemented with a more detailed technical review by people having good knowledge of plant-specificities (design and operation) in addition to knowledge of PSA techniques/methodologies;

- Developing internationally agreed standards for the PSA of Low-Power and Shut-down States, SFP and for Level 2 PSA will be beneficial for the development and review of PSA. In addition, for some hazards PSA, the guidance should be better developed, including Level 1 as well as Level 2 PSA.

- Verification of the adequacy of the different PSA elements (e.g. initiating event analysis, data, human reliability analysis) is an important task of the review; however, the review should also address the resulting "overall picture". In this perspective, it is useful to review selected minimal cut sets, or groups of minimal cut sets, and analyse the adequacy of the underlying accident representation in light of the plant system response and procedural guidance.

- A good practice is to focus detailed review to risk significant elements (e.g., failure events, components, operator actions, etc.), as well as accident sequences. Focus-sing on risk significance ensures that eventual review issues have an impact on the PSA results and, ultimately, that the review process has a recognizable role in ensuring plant safety. Spot checks on low significance PSA elements and sequences are also recommended, especially addressing unexpected low risk contributions or changes in the risk contributions (PSA elements that decrease their significance across different PSA updates).

- The progress which is made in PSA over time is sometimes not very well documented. That is why documentation has to remain a challenge to achieve when per-forming a PSA. Depending on the specific analysis, documentation sheets may be developed to make sure assumptions and data are linked to the relevant sources.

**Recommendations resulting from case studies performed**

- An opportunity to further improve PSA models is to take into account the insights of PSA based event analysis (PSAEA) (or precursor analysis). This analysis is most helpful in the overall process of operational experience feedback (lessons learned from real incidents, identification of corrective actions, etc.), but is also often useful to improve PSA models through the identification of missing elements in the PSA model (e.g., missing initiating events, accident scenarios or human actions), short-comings of modelling (e.g., regarding dependencies, combinations), needs for more detailed modelling (such as I&C systems), etc;

- The modelling of accident sequences, systems, and human actions is generally more elaborated in Level 1 PSA, whereas Level 2 PSA is often hampered by a less detailed modelling of possible mitigating strategies, measures, equipment, or manual actions. In addition, Level 1 PSA quantifies CDF/FDF and importance measures as well, it uses dedicated computer code for model development and risk quantification, while Level 2 PSA, which primarily aims to determine large or early release frequencies – LRF/LERF – , often uses different computer codes without a fully automatic interface between Level 1 and Level 2. As result, Level 1 PSA generally offers more opportunities for PSA applications than Level 2 PSA. Level 2 PSA is a good tool to help improve severe accident management and to evaluate the effectiveness of severe accident management measures and guidelines. There is a wide range of Level 2 PSA applications that can be useful, even if the focus has tradition-ally been on Level 1 PSA applications. Level 2 PSA shall provide indications on the dominant contributors to the risk of radioactive releases and thus help defining important risk reduction options.

- A risk monitor tool can be used to support maintenance planning and determine the expected risk profile in advance of performing maintenance. Such risk-informed ap-plications can be useful for the operating personnel and maintenance planners to shift their way of thinking to a "risk awareness mode". However, the PSA models to be used for such applications need to be specifically tailored (symmetrical models) and carefully checked for their response in case of a large number of plant possible configurations.

- For adequately addressing single and/or combined internal as well as external hazards in PSA, a systematic identification of all single and combined hazards applicable to the site and plant is needed followed by a comprehensive screening of all types of single as well as combined hazards and by site-specific "(probabilistic) hazard analyses". This process leads to the identification of the relevant hazards to be analysed in detail. In this context, combinations of causally related, so-called consequential hazards, as well as hazards correlated by a common cause, so-called correlated hazards, must be modelled adequately. Combinations of coincidental hazards (occurring independently of each other simultaneously by coincidence) also need to be included in the analyses. Multi-unit and multi-source issues need to be addressed as well.

- The efforts towards a systematic treatment of EOCs in PSA should continue. The contributions from these errors may have a non-negligible influence.

- When the PSA results are used for decision-making, it is necessary to understand the limitations and uncertainties of PSA. Despite all the

efforts and developments regarding PSA methodologies and applications, the challenges in efficiently and effectively applying PSA studies are still present, being related to:

- Limitations in PSA scope (e.g., only internal events) or level of detail (e.g. accident sequences that are not developed in further detail since it is considered that a safe end state is reached, systems that are not modelled or modelled in a simplified way because their safety importance is a priori judged to be minor) can also lead to limitations in the applicability of PSA models for specific risk evaluations and/or PSA applications (e.g. risk-informed Technical Specifications).

- Even the most sophisticated PSA models cannot fully represent reality, which is why the issue of PSA completeness is an important aspect important to consider.

- An obvious challenging issue is the availability, quality and relevance of data used in the PSA model. Nowadays, even if data uncertainty remains a significant challenge, PSA studies can be used to identify and assess the significance of such uncertainties in safety assessment.

- There are some issues that are not fully or systematically considered in the present PSAs (unforeseen operator actions, multi-unit issues, or frequencies of natural disasters). Some of them are just a matter of choice (that may be reconsidered in the future), and do not represent a methodological deficiency.

- There is a wide range of PSA guidance available that aims to fully cover all is-sues of safety significance. However, when performing PSA under the real restraints of budget and resources, many issues must be ignored or dealt with in a manner which does not really represent the state-of-the-art.

- Aggregating PSA parts assessed with different levels of conservatism and un-certainties is a challenge. which may lead to an incorrect view of the risk contributions and therefore to potentially inappropriate decisions.

- Different PSA objectives (e.g., safety assessment to demonstrate compliance with regulatory requirements, evaluation of proposed plant modifications, risk monitoring, etc.) may require substantially different levels of detail implemented in PSA model. Therefore, use of the model beyond its original intent requires careful examination of the initial model scope, assumptions, simplifications and, in most of cases, laborious effort on model update and extension to ensure that limitations of the original model do not compromise PSA results and conclusions for an extended use.

- When the detail required in defining safety issues exceeds that which can be identified solely by the peer review based on the regulatory standards, a TSO needs to rely on a more detailed technical review of the PSA and its supporting studies. How-ever, the lack of a sufficiently broad range of supporting studies is a recurrent issue for Level 1 and Level 2 PSA, for example for the validation of success criteria (particularly Level 1 PS1), thermal hydraulic analyses to underpin various HRA accident sequences or lack of MELCOR calculations for representative severe accident scenarios. Thus, this report recommends that sufficient and suitable supporting studies for example thermal hydraulic studies for various accident sequences, HRA, MELCOR calculations for representative severe accident analyses need to be undertaken and be subject to independent technical review prior to submission to underpin all levels of PSA modelling.

- In the frame of Level 1 PSA there is a well-known and universally accepted figure of merit: the core damage frequency.

(However, discussions continue, e.g., about risk aggregation and interdependencies from multiple units and/or further radioactive sources, such as the spent fuel storage in case of spent fuel accidents). In Level 2 PSA, there is no comparable category. Instead, release categories or source terms are used. It seems that a universal figure of merit (e.g., the sum of release frequencies times for the released activities [Bq /ry] of radionuclides) could promote the application of Level 2 PSA. Some PSA in Germany have come up with such a figure applying it for assessing plant modifications (Level 2 PSA).

- Level 2 PSA can better inform site (and off-site) planning and emergency response arrangements including providing an input to trans-boundary impact assessments. For example, if the purpose of a Level 2 PSA is to determine the frequency of large and/or early releases, it is most likely to help identify severe accidents to consider in emergency planning. However, if characteristic release categories (source term groups) and their frequencies are also described in the Level 2 P SA, the analysis can better support emergency planning for the on-site and off-site consequences of different severe accidents (groups of accidents).

- External Hazards PSA, especially if the facility has an extended design life (including post-operational phases) should consider the effect of climate change; for example, a modern new NPP may need to persist in the order of 100 years.

- Multi-unit PSA techniques may be required for sites with more than one reactor or even for a single unit where there are multiple separate sources of radioactivity such as the reactor and SFP from which coincident releases could occur.

- Considering the effects of applicable safety culture in PSA modelling either implicitly or explicitly (for example through reliability data selection or the approach to model-ling operator responses to faults) can have a significant effect on the quality of the analysis.

APPENDIX 1

# REFERENCES


/ANG 18/ Ang, M., et al. :A Demonstration of Practical Elimination of Early or Large Fission Product Release for the United Kingdom ABWR Generic Design Assessment, in: Proceedings of The 26th International Conference on Nuclear Engineering (ICONE-26), London, United Kingdom, July 2018.

/ANS 02/ American Society of Mechanical Engineers (ASME) / American Nuclear Society (ANS): Standard for PSA for nuclear power plant application, ASME/ANS RA-S-2002, 2002.

/ANS 08/ American Society of Mechanical Engineers (ASME) / American Nuclear Society (ANS): Standard for Level 1 / Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-S-2008, 2008.

/ANS 09/ American Society of Mechanical Engineers (ASME) / American Nuclear Society (ANS): Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-Sa-2009, February 2009.

/ANS 13/ American Society of Mechanical Engineers (ASME) / American Nuclear Society (ANS): Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-Sb-2013, September 2013.

/ANS 14/ American Society of Mechanical Engineers (ASME) / American Nuclear Society (ANS): Standard for Low Power and Shutdown Modes Probabilistic Risk Assessment for Nuclear Power Plant Applications, ANS/ASME-58.22-2014, 2014.

/ANS 14a/ American Society of Mechanical Engineers (ASME) / American Nuclear Society (ANS): Severe Accident Progression and Radiological Release (Level 2) PRA Standard for Nuclear Power Plant Applications for Light Water Reactors (LWRs), ASME/ANS RA-S-1.2 - 2014, 2014.

/ANS 16/ American Society of Mechanical Engineers (ASME) / American Nuclear Society (ANS): Standard for Radiological Accident Offsite Consequence Analysis (Level 3 PRA) to Support Nuclear Installation Applications, ASME/ANS RA-S-1.3 (draft), February 2016.

/ANS 17/ American Society of Mechanical Engineers (ASME) / American Nuclear Society (ANS): Standard for Radiological Accident Offsite Consequence Analysis (Level 3 PRA) to Support Nuclear Installation Applications, ASME/ANS RA-S-1.3, 2017.

/ASN 04/ Autorité de Sureté Nucléaires (ASN): Options de sûreté du projet de réacteur EPR, Paris, France, 28 September 2004.

/BAR 15/ Bareith, A., et al.: Upgrade of the PSA for NPP Paks to Model the Effects of New Low Power and Shutdown Emergency Operating Procedures, Paper 12301, in: Proceedings of ANS PSA 2015 International Topical Meeting on Probabilistic Safety Assessment and Analysis, Sun Valley, ID, USA, April 26-30, 2015, on CD-ROM, American Nuclear Society, LaGrange Park, IL, United States of America, 2015.

/BMU 05/ Federal Ministry for the Environment, Nature Conservation, Building and Nuclear Safety (Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit, BMUB): Safety Requirements for Nuclear Power Plants as amended and published on November 22, 2012, and revised version of March 3, 2015,

http://www.base.bund.de/SharedDocs/Downloads/BASE/EN/hns/a1-english/A1-03-15-SiAnf.html.

/CNS 14/ Canadian Nuclear Safety Commission (CNSC): Summary Report of the International Workshop on Multi-Unit Probabilistic Safety Assessment, Ottawa, ONT, Canada, November 2014.

/COR 06/ Corenwinder, F., et al.: Improving Quality of Nuclear Power Plant PSA by International Comparisons, Paper PSAM-0265, in: Conference Proceedings of 8th International Probabilistic Safety Assessment and Management Conference (PSAM8), New Orleans, LA, USA, May 2006, American Society of Mechanical Engineers (ASME), New York, NY, United States of America, 2006.

/DEC 17/ Decker, K., H. Brinkman: List of external hazards to be considered in ASAMPSA_E, Technical report D21.2, Reference IRSN

PSN-RES/SAG/2017-00011. Advanced Safety Assessment

Methodologies: Extended PSA (ASAMPSA_E), European Commission, Petten, The Netherlands, 2017, www.asampsa.eu.

/ENS 15/ Swiss Nuclear Safety Inspectorate (ENSI): Probabilistic Safety Analysis: Applications. Guideline for Swiss Nuclear Installations, ENSI-A06, Swiss Nuclear Safety Inspectorate, Brugg, Switzerland, 2015,

www.ensi.ch/wp-content/uploads/sites/5/2009/03/ENSI-A06_Edition_2015-11_E_web.pdf.

/ENS 19/ Swiss Nuclear Safety Inspectorate (ENSI): Probabilistic Safety Analysis: Quality and Scope. Guideline for Swiss Nuclear Installations, ENSI-A05 Swiss Nuclear Safety Inspectorate, Brugg, Switzerland, 2019, https://www.ensi.ch/wp-content/uploads/sites/5/2011/08/ENSI-A05_E_2019_03_11.pdf.

/EPR 09/ Electrical Power Research Institute (EPRI): Guidelines for Performance of Internal Flooding Probabilistic Risk Assessment, EPRI 1019194, Final Report, Palo Alto, CA, USA, December 2009.

/ETS 17/ ETSON PSA Expert Group EG8: Proceedings of the Workshop on PSA Lessons Learned, Paris, France, 2017.

/FAK 05/ Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für

Kernkraftwerke: Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand: August 2005, BfS-SCHR-37/05, Bundesamt für Strahlenschutz (BfS), Salzgitter, Germany, October 2005 (in German), https://doris.bfs.de/jspui/bitstream/urn:nbn:de:0221-201011243824/1/BfS_2005_SCHR-37_05.pdf.

/FAK 05a/ Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke: Daten zur Quantifizierung von Ereignisablaufdiagrammen und Fehlerbäumen, Stand: August 2005, BfS-SCHR-38/05, Bundesamt für Strahlenschutz (BfS), Salzgitter, Germany, October 2005, (in German), https://doris.bfs.de/jspui/bitstream/urn:nbn:de:0221-201011243838/1/BfS_2005_SCHR-38_05.pdf.

/FAK 16/Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke: Methoden und Daten zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand: Mai 2015, Bundesamt für Strahlenschutz (BfS), Salzgitter, Germany, BfS-SCHR-61/16, September 2016 (in German), https://doris.bfs.de/jspui/bitstream/urn:nbn:de:0221-2016091314090/3/BfS-SCHR-61-16.pdf.

/FAK 18/Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke: Methoden und Beispiele für die probabilistische Bewertung sicherheitsrelevanter Fragestellungen außerhalb der SÜ, Stand: Mai 2015, Bundesamt für Strahlenschutz (BfS), Salzgitter, Germany, BfS-SCHR-03/18, Januar 2018 (in German), https://doris.bfs.de/jspui/bitstream/urn:nbn:de:0221-2018013014519/3/BfE-SCHR-03-18_FAK%20PSA.pdf.

/FAS 03/ Faßmann, W., W. Preischl: Methode zur Untersuchung und Bewertung schädlicher Eingriffe des Operateurs, Reactor Safety Research Project No. RS 1112, GRS-A-3157, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH; Köln, Germany, 2003 (in German).

/GRY 12/ Gryffroy, D., et al.: Status and Perspectives of PSA activities in Belgium, in: 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012 (PSAM11 ESREL 2012), ISBN: 978-1-62276-436-5, Curran Associates, Inc., Red Hook, NY, United States of America, 2012.

/HAG 21/ Hage, M., G. Mayer, M. Röwekamp: Vorgehen bei Erweiterungen einer Site-Level PSA bis hin zur Stufe 2, Technischer Fachbericht, GRS-637, ISBN: 78-3-949088-26-1, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, Juli 2021,
https://www.grs.de/publikationen/grs-637.

/HEN 17/ Henneke, D., et al., The Use of Comprehensive In-Process Peer Reviews in Support of the United Kingdom ABWR PSA Generic Design Assessment Process, in: Proceedings of ANS PSA 2017 International Topical Meeting on Probabilistic Safety Assessment and Analysis, Pittsburgh, PA, USA, September 24-28, 2017, on CD-ROM, American Nuclear Society, LaGrange Park, IL, United States of America, 2017.

/HIR 18/ Hirokawa, N., et al.: Overview of PSA for the United Kingdom ABWR Generic Design Assessment, Paper 82553, in: Proceedings of The 26th International Conference on Nuclear Engineering (ICONE-26), London, United Kingdom, July 2018.

/HIT 17/ Hitachi-GE: UK ABWR Generic Design Assessment, Generic PCSR Chapter 25: Probabilistic Safety Assessment, GA91-9101-0101-25000, AE-GD-0171, Rev. C, 2017,

http://www.hitachi-hgne-uk-abwr.co.uk/gda_library.html.

/HPA 07/ Health Protection Agency (HPA): Update of PC COSYMA: Development of version 2.03 for United Kingdom use, CRCE-EA-11-2007, 2007.

/IAE 98/ International Atomic Energy Agency (IAEA): Good Practices with respect to the development and use of nuclear power plant procedures, IAEA-TECDOC-1058, Vienna, Austria, December 1998,

https://www-pub.iaea.org/MTCD/Publications/PDF/te_1058_prn.pdf.

/IAE 01/ International Atomic Energy Agency (IAEA): Applications of probabilistic safety assessment (PSA) for nuclear power plants, IAEA-TECDOC-1200, ISSN 1011–4289 Vienna, Austria, February 2001,

https://www-pub.iaea.org/mtcd/publications/pdf/te_1200_prn.pdf.

/IAE 03/ International Atomic Energy Agency (IAEA): Periodic Safety Review of Nuclear Power Plants, Safety Guide, IAEA Safety Standards Series,

NS-G-2.10; Vienna, Austria, 2003.

/IAE 06/ International Atomic Energy Agency (IAEA): Development and Review of Plant Specific Emergency Operating Procedures, Safety Reports Series No. 48, STI/PUB/1226, Vienna, Austria, February 2006,

https://www-pub.iaea.org/MTCD/publications/PDF/Pub1226_web.pdf.

/IAE 06a/ International Atomic Energy Agency (IAEA): Determining the quality of probabilistic safety assessments (PSA) for applications in nuclear power plants, IAEA TECDOC-1511. ISBN 92–0–108706–3, ISSN 1011–4289, Vienna, Austria, July 2006,

https://www-pub.iaea.org/MTCD/Publications/PDF/te_1511_web.pdf.

/IAE 10/ International Atomic Energy Agency (IAEA): Development and

Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3, STI/PUB/1430, ISBN 978-92-0-114509-3, Vienna, Austria, April 2010,

http://www-pub.iaea.org/MTCD/publications/PDF/Pub1430_web.pdf.

/IAE 10a/ International Atomic Energy Agency (IAEA): Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-4, STI/PUB/1443,

ISBN 978–92–0–102210–3, Vienna, Austria, May 2010,

http://www-pub.iaea.org/MTCD/publications/PDF/Pub1443_web.pdf.

/IAE 13/ International Atomic Energy Agency (IAEA): Periodic Safety Review for Nuclear Power Plants, Specific Safety Guide, IAEA Safety Standards Series No. SSG-25, STI/PUB/1588 978-92-0-137410-03, Vienna,

Austria, March 2013,

https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1588_web.pdf.

/IAE 18/ Poghosyan, S., et al. (International Atomic Energy Agency (IAEA)): IAEA Project: Multiunit Probabilistic Safety Assessment, Presentation No. 430, in: Proceedings of 14th International Probabilistic Safety Assessment and Management Conference (PSAM14), Los Angeles, CA, United States of America, September 2018, http://psam14.org/proceedings/Presentations/430.pdf.

/IAE 18a/ International Atomic Energy Agency (IAEA): Consideration of External Hazards in Probabilistic Safety Assessment for Single Unit and Multi-unit Nuclear Power Plants, IAEA Safety Report Series No. 92, STI/PUB/1777, ISBN 978 92 0 101917–2, Vienna, Austria, November 2018,

https://www-pub.iaea.org/MTCD/publications/PDF/P1777_web.pdf.

/IAE 19/ International Atomic Energy Agency (IAEA): Technical Approach to Probabilistic Safety Assessment for Multiple Reactor Units, IAEA Safety Report Series No. 96, STI/PUB/1820, ISBN 978 92 0 102618 7, Vienna, Austria, May 2019,

https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1820_web.pdf.

/IAE 23/ International Atomic Energy Agency (IAEA): Technical Approach to Probabilistic Safety Assessment for Multi-Unit Probabilistic Safety Assessment, Safety Reports Series No. 110, STI/PUB/1974, ISBN 978-92-0-119322-3, Vienna, Austria, September 2023,

https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1974_web.pdf.

/IAE 24/ International Atomic Energy Agency (IAEA): Probabilistic Safety Assessment Benchmarks of Multi-unit, Multi-reactor Sites, IAEA-TECDOC- 2044, ISBN 978–92–0–108324–1, Vienna, Austria, 2024,

https://www-pub.iaea.org/MTCD/Publications/PDF/TE-2044web.pdf.

/IAE 24a/ International Atomic Energy Agency (IAEA): Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Specific Safety Guide, IAEA Safety Standards Series No. SSG-3, Rev. 1, STI/PUB/2056, ISBN 978-92-0-130723-1, Vienna, Austria, March 2024, https://doi.org/10.61092/iaea.3ezv-lp4.

/IAE 24b/ International Atomic Energy Agency (IAEA): Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, Specific Safety Guide, IAEA Safety Standards Series No. SSG-4, Rev. 1, Draft DS528, Vienna, Austria, in preparation, 2024.

/IAE 24c/ International Atomic Energy Agency (IAEA): Safety Evaluation of Nuclear Installations Against External Event Induced Hazard Combinations, Draft TECDOC, Vienna, Austria, in preparation, 2024.

/IAE 24d/ International Atomic Energy Agency (IAEA): Advanced Probabilistic 06Safety Assessment (PSA) Approaches and Applications for Nuclear Power Plants, draft TECDOC, Vienna, Austria, in preparation, 2024.

/ICR 06/ International Commission on Radiological Protection (ICRP): Assessing Dose of the Representative Person for the Purpose of the Radiation Protection of the Public. ICRP

Publication 101a. Ann. ICRP 36 (3), 20026, Https://www.icrp.org/publication.asp?id=ICRP%20Publication%20101a.

/JUL 95/ Julius, J. A., et al.: A procedure for the analysis of errors of commission in a probabilistic safety assessment of a nuclear power plant at full power, Reliability Engineering & System Safety, 50:189–201, 1995.

/KAR 12/ Karsa, Z., P. Siklossy, T. Javor: Implementation and Maintenance of a Risk Monitor, Research report, NUBIKI, Budapest, Hungary, 2012 (in Hungarian).

/KIS 16/ Kiss, T.: Safety and financial considerations go hand in hand at Paks NPP, RiskSpectrum Magazine 2016, PSAM13 edition, Lloyd's Register Consulting(LRC), Stockholm, Sweden, 2016.

/KND 96/ KND 306.302-96: Requirements to the Format and Content of the Safety Analysis Report of Nuclear Power Plants with VVER Reactors at the Commissioning Stage, Kyiv, Ukraine, 1996.

/KOL 05/ Kolaczkowski, A., et al.: Good practices for implementing Human

Reliability Analysis (HRA), NUREG-1792, 2005, U.S. Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research, Washington, DC, United States of America, April 2005,

https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1792/.

/MET 19/ Met Office: UK Climate Projections (UKCP): UKCP CP18, Science Overview Report, November 2018 (Updated March 2019), https://www.metoffice.gov.uk/research/collaboration/ukcp.

/NEA 13/ Organisation for Economic Co-operation and Development (OECD)

Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear

Installations (CSNI): Use and Development of Probabilistic Safety

Assessment – An Overview of the Situation at the end of 2010", NEA/CSNI/R(2012)11, Paris, France, January 2013, http://search.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=NEA/CSNI/R(2012)11&docLanguage=En.

/NEA 14/ Organisation for Economic Co-operation and Development (OECD)

Nuclear Energy Agency (NEA) Committee on Nuclear Regulatory

Activities (CNRA): Report on Fukushima Daiichi NPP Precursor Events, NEA/CNRA/R(2014)1, Paris, France, January 2014,

https://www.oecd-nea.org/nsd/docs/2014/cnra-r2014-1.pdf.

/NEA 14a/ Organisation for Economic Co-operation and Development (OECD)

Nuclear Energy Agency (NEA) Committee on the Safety of

Nuclear Installations (CSNI): PSA of Natural External Hazards Including Earthquake, Workshop Proceedings, Prague, Czech Republic, 17-20 June 2013, NEA/CSNI/R(2014)9, Paris, France, July 2014,

https://www.oecd-nea.org/nsd/docs/2014/csni-r2014-9.pdf.

/NEA 19/ Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA), Committee on the Safety of Nuclear Installations (CSNI): Site-Level (Including Multi-Unit) PSA

Developments, NEA/CSNI/R(2019)16, and NEA/CSNI/R(2019)16/ADD, Paris, France, 2019, https://www.oecd-nea.org/nsd/docs/indexcsni.html.

/NEA 20/ Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA), Committee on the Safety of Nuclear Installations (CSNI): Use and Development of Probabilistic Safety Assessment – An Overview of the Situation at the End of 2017, NEA/CSNI/R(2019)10, Paris, France, September 2020,
https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=NEA/CSNI/R(2019)10&docLanguage=En.

/NEI 08/Nuclear Energy Institute (NEI), Risk Informed Applications Task Force (RATF) and NEI PRA Peer Review Task Force: Process for Performing Internal Events PRA Peer Reviews Using the ASME/ANS PRA Standard, NEI 05-04, Rev. 2, November 2008,

https://www.nrc.gov/docs/ML0834/ML083430462.pdf.

/NP 07/ NP 306.2.141-2008: General Provisions for the Safety of Nuclear Plants, approved by order No.162 of the State Nuclear Regulatory Committee of Ukraine, Kyiv, Ukraine, November 19, 2007.

/NP 10/ NP 306.2.162-2010: Requirements to the Safety Assessment of Nuclear Power Plants, approved by order No.124 of the State Committee on Nuclear Regulation of Ukraine, Kyiv, Ukraine, September 22, 2010.

/NRC 00/ United States Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research: Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA), NUREG-1624, Washington, DC, United States of America, May 2000,

https://www.nrc.gov/docs/ML0037/ML003719212.pdf.

/NRC 05/ United States Nuclear Regulatory Commission (NRC): EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities, Final Report, Volume 2: Detailed Methodology, NUREG/CR-6850, EPRI 1011989, DC, United States of America, September 2005,

https://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6850/v2/cr6850v2.pdf.

/NRC 07/ United States Nuclear Regulatory Commission (NRC): Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Chapter 13.5.2.1 Operating and Emergency Operating Procedures, NUREG-0800, Section 13.5.2.1, Rev. 2, Washington, DC, United States of America, 2007, https://www.nrc.gov/docs/ML0701/ML070100635.pdf.

/NRC 09/ United States Nuclear Regulatory Commission (NRC): Regulatory Guide 1.200 (Rev. 2, 2009): An approach for determining the technical adequacy of Probabilistic Risk Assessment results for risk-informed activities, Washington, DC, United States of America, 2009,

https://www.nrc.gov/docs/ML0904/ML090410014.pdf.

/NRC 16/ United States Nuclear Regulatory Commission (NRC): Estimating

Loss-of-Coolant Accident (LOCA) Frequencies Through the Elicitation Process, NUREG-1829, Main Report and Appendices, Washington, DC, United States of America, last update: February 2016,

https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1829/.

/NRC 16a/ United States Nuclear Regulatory Commission (NRC): Common Cause Failure Parameter Estimations 2015, update of NUREG/CR-5497 Washington, DC, United States of America, October 2016,

https://nrcoe.inl.gov/resultsdb/publicdocs/CCF/ccfparamest2015.pdf.

/NRP 79/ National Radiological Protection Board (NRPB): A Model for Short and Medium Range Dispersion of Radionuclides Released to Atmosphere, NRPB-R91, Harwell, Didcot, Oxon OX11 ORQ, United Kingdom, September 1979, https://admlc.files.wordpress.com/2014/05/r91.pdf.

/NRP 81/ National Radiological Protection Board (NRPB): A Procedure to Include Deposition in the Model for Short and Medium Range Atmospheric

Dispersion of Radionuclides, NRPB-R122, Chilton , Didcot, Oxon OX11 ORQ, United Kingdom, September 1981,

https://admlc.files.wordpress.com/2014/09/r122_000.pdf.

/NRP 83/ National Radiological Protection Board (NRPB): Models to Allow for the Effects of Coastal Sites, Plume Rise and Buildings on dispersion of

Radionuclides and guidance on the Value of Deposition Velocity and Washout Coefficients, NRPB-R157, Chilton , Didcot, Oxon OX11 ORQ, United Kingdom, December 1983,

https://admlc.files.wordpress.com/2014/09/r157.pdf.

/OHA 12/ O`Hara, J. M., et al. : Human Factors Engineering Program Review Model, NUREG-0711, Rev. 3, U.S. Nuclear Regulatory Commission, Washington, DC, United States of America, 2012, https://www.nrc.gov/docs/ML1232/ML12324A013.pdf.

/ONR 14/ Office for Nuclear Regulation (ONR), Safety Assessment Principles for

Nuclear Facilities, 2014 Edition, Revision 0,

http://www.onr.org.uk/saps/saps2014.pdf.

/ONR 17/ Office for Nuclear Regulation (ONR) New Reactors Division: Step 4

Assessment of Probabilistic Safety Analysis for the United Kingdom

Advanced Boiling Water Reactor, Assessment Report: ONR-NR-AR-17-014, Revision 0, December 2017,

http://www.onr.org.uk/new-reactors/uk-abwr/reports/step4/onr-nr-ar-17-014.pdf.

/ONR 19/ Office for Nuclear Regulation (ONR): Use of United Kingdom Climate Projections 2018 (UKCP18) by GB Nuclear

Industry, Position Statement, March 2019, http://www.onr.org.uk/documents/2019/ukcp18-position-statement.pdf.

/ONR 19a/ Office for Nuclear Regulation (ONR): New Nuclear Power Plants:

Generic Design Assessment Technical Guidance', ONR-GDA-GD-007, Revision 0, May 2019,

http://www.onr.org.uk/new-reactors/reports/onr-gda-007.pdf.

/ONR 24/ Office for Nuclear Regulation (ONR): Probabilistic Safety Analysis,

Nuclear Safety Technical Assessment Guide, NS-TAST-GD-030

Revision 4, April 2024,

https://onr.org.uk/media/msjpkl10/ns-tast-gd-030.pdf.

/POD 12/ Podofillini, L., V. N. Dang: Progress on Errors of Commission: An Outlook Based on Plant-Specific Results, in in: 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012 (PSAM11 ESREL 2012), ISBN: 978-1-62276-436-5, Curran Associates, Inc., Red Hook, NY, United States of America, 2012.

/POD 13/ Podofillini, L., et al.: A pilot study for errors of commission for a boiling water reactor using the CESA method, Reliability Engineering and System Safety 109, pp. 86–98, 2013.

/POD 13a/ Podofillini, L., V. N. Dang, B. Reer: PSA-informed review of emergency procedural guidance, Proceedings of the American Nuclear Society Winter Topical Meeting: Risk Management for Complex Socio-technical Systems, Washington DC, United States of America A, November 10-14, 2013.

/RAI 13/ Raimond, E., et al.: ASAMPSA2 Best-practices guidelines for Level 2 PSA development and applications, Volume 2 - Best practices for the Gen II PWR, Gen II BWR L2PSAs. Extension to Gen III reactors,

Technical report ASAMPSA2/WP2-3/D3.3/2013-35, 2013, https://www.irsn.fr/sites/default/files/documents/larecherche/organisation/programmes/asampsa2/ASAMPSA2%20guidelines%20vol2%20genII-III.pdf.

/RD-95/ RD-95: Requirements to the Format and Content of the Safety Analysis Report of Nuclear Power Plant Units with VVER Reactors Operating in Ukraine, Kyiv, Ukraine, 1995.

/REE 04/ Reer, B., V: N. Dang, S. Hirschberg: The CESA method and its application in a plant-specific pilot study on errors of commission, Reliability Engineering & System Safety, 83(2): 187-205, 2004.

/REE 08/ Reer, B.: Review of advances in human reliability analysis of errors of commission — Parts 1 and 2, Reliability Engineering & System Safety, 93(8): 1991-1104, 1008.

/RFS 02/ Basic Safety Rule on PSA (Règle fondamentale de sûreté - RFS) n° 2002-01, 26 December 2002.

/ROE 18/ Roewekamp, M., et al.: OECD WGRISK – Recently Ongoing and Potential Future International Risk-related Activities, Paper 264, in: Proceedings of 14th International Probabilistic Safety Assessment and Management Conference (PSAM14), Los Angeles, CA, United States of America, September 2018.

/ROE 19/ Roewekamp, M., et al.: Insights from a WGRISK Activity on the Status of Site-Level PSA Developments, in: Proceedings of ANS PSA 2019 International Topical Meeting on Probabilistic Safety Assessment and Analysis, Charleston, SC, USA, April 27 – May 3, 2019, American Nuclear Society, LaGrange Park, IL, United States of America, May 2019.

/ROE 23/ Röwekamp, M., F. Berchtold, C. Strack: Probabilistic Analyses of Single and Combined External Hazards for A Multi-Unit Nuclear Power Plant Site and for Research Reactor Site in Germany, Joint OECD/NEA WGEV and WGRISK Workshop, IRSN, Fontenay-aux-Roses, France, September 11 – 13, 2023.

/TUD 15/ The TUD Office, Vattenfall AB: T-Book, Reliability Data of Components in Nordic Nuclear Power Plants, 8th Edition, TUD 15-12, ISBN 978-91-637-8817-8, 2015.

/TYR 18/Tyrväinen, T., I. Karanta: Level 2 PRA studies - Steam explosions and integration of PRA levels 1 and 2, VTT-R-00191-18, VTT Technical

Research Centre of Finland Ltd., Espoo, Finland, 2018.

/TYR 19/Tyrväinen, T., I. Karanta: Dynamic containment event tree modelling techniques and uncertainty analysis, VTT-R-06892-18, VTT Technical Research Centre of Finland Ltd., Espoo, Finland, 2019.

/VUK 16/ Vuković, I., R. Prosen: Evaluation of Impact of NEK Safety Upgrade

Program Implementation on the Reduction of Total Core Damage

Frequency, Proceedings of the 11th International Conference of the Croatian Nuclear Society, Zadar, Croatia, 5-8 June 2016.

/WEN 08/ Western European Nuclear Regulators Association (WENRA): WENRA Reactor Safety Reference Levels, January 2008,

http://www.wenra.org/media/filer_public/2012/11/05/list_of_reference_levels_january_2008.pdf
.

/WEN 14/ Western European Nuclear Regulators Association (WENRA): WENRA Safety Reference Levels for Existing Reactors. Update in Relation to Lessons Learned from TEPCO Fukushima Dai-ichi Accident. WENRA RHWG, 24th September 2014

http://www.wenra.org/media/filer_public/2014/09/19/wenra_safety_reference_level_for_existing_reactors_september_2014.pdf.

/WEN 21/ Western European Nuclear Regulators Association (WENRA): WENRA Reactor Safety Reference Levels Revision 2020, February 2021,

https://www.wenra.eu/sites/default/files/publications/wenra_safety_reference_level_for_existing_reactors_2020.pdf.

sqdjjbdqj

APPENDIX 2

# ABBREVIATIONS

| | |
|---|---|
| ABWR | Advanced Boiling Water Reactor |
| ADMLC | Atmospheric Dispersion Modelling Liaison Committee |
| AFW | Auxiliary Feedwater System |
| ALARA | As Low As Reasonably Achievable |
| ALARP | As Low As Reasonably Practicable |
| AM | Accident Management |
| AMR | Advanced Modular Reactor |
| ANS | American Nuclear Society |
| APET | Accident Progression Event Tree |
| ASAMPSA 2 | Advanced Safety Assessment Methodologies: Level 2 PSA |
| ASAMPSA_E | Advanced Safety Assessment Methodologies: Extended PSA |
| ASN | Autorité de Sûreté Nucléaire (French nuclear safety authority) |
| ATWS | anticipated transient without scram |
| A-AF | alternative auxiliary feedwater |
| A-BWT | alternative borated water tank |
| A-CYT | alternative condensate water tank |
| A-RHR | alternative residual heat removal |
| A-SI | alternative safety injection |
| BB | Bunkered building |
| BEL V | Belgian TSO, a subsidiary of the FANC |
| BWR | boiling water reactor |
| CC | Capability Category |

CCF common cause failure

CCDP conditional core damage probability

CCWS component cooling water system

CDP core damage probability

CESA commission errors search and assessment

CMF common mode failure

CDF core damage frequency

CNRA Committee on Nuclear Regulatory Activities

CSNI Committee on the Safety of Nuclear Installations

DBA design basis accident

DEC design extension condition

DSA Deterministic Safety Assessment

EC European Commission

ECCS emergency core cooling system

ECR emergency control room

EDF Electricité de France

ENEA Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile (Italian National Agency for New Technologies, Energy and Sustainable Economic Development)

EOC error of commission

EOP emergency operating procedure

EPR European Pressurised Reactor

EPRI Electric Power Research Institute

ESW essential service water

ET event tree

ETSON European TSO Network

EU European Union

FANC Federal Agency for Nuclear Control (Belgium)

FDF fuel damage frequency

FT fault tree

FV Fussell-Vesely

GDA Generic Design Assessment

GRS Gesellschaft für Anlagen- und Reaktorsicherheit gGmbH (German TSO)

HELB high energy line break

HEP human error probability

HLR high-level requirement

HRA human reliability analysis

IDPSA integrated deterministic and probabilistic safety analysis (IDPSA)

IAEA International Atomic Energy Agency

IIE internal initiating event

IRIDM integrated risk-informed decision-making

IRSN Institut de Radioprotection et de Sûreté Nucléaire (French TSO)

ISLOCA Interfacing System LOCA

I&C instrumentation and control

LERF large early release frequency

LOCA loss of coolant accident

LOOP loss of offsite power

LPIS low pressure injection system

LP&SD low power and shutdown

LRF large release frequency

LUHS loss of ultimate heat sink

MCCI melt core and concrete interaction

MCS minimal cut sets

MDTA misdiagnosis tree analysis

MERMOS Méthode d'Évaluation de la Réalisation des Missions Opérateurs pour la Sûreté (HRA method by EDF)

| | |
|---|---|
| NC | nonconforming condition |
| NCDP | nominal core damage probability |
| NEA | Nuclear Energy Agency |
| NPP | nuclear power plant |
| NRC | Nuclear Regulatory Commission (United States of America) |
| NSSS | nuclear steam supply system |
| OECD | Organisation for Economic Co-operation and Development |
| OEE | other external events |
| OEF | operational experience feedback |
| ONR | Office for Nuclear Regulation (United Kingdom) |
| OSC | operating support centre |
| PCSR | Pre-Construction Safety Report |
| PGA | peak ground acceleration |
| PORV | power operated relief valve |
| POS | plant operational state |
| PSA | Probabilistic Safety Analysis |
| PSAEA | PSA Event Analysis |
| PSI | Paul Scherrer Institut (Switzerland) |
| PSR | Periodic Safety Review |
| PWR | pressurized water reactor |
| RAW | risk achievement worth |
| RCIC | reactor core isolation cooling |
| RCP | reactor coolant pump |
| RCS | reactor coolant system |
| RHR | residual heat removal |
| RIDM | risk-informed decision-making |
| RIF | risk increase factor |

RPV reactor pressure vessel

RQ Regulatory Query

RRC risk reduction category

RWST refueling water storage tank

Ry reactor year

R&D research and development

SAA severe accident analysis

SAM severe accident management

SAMG severe accident management guidelines

SAPs Safety Assessment Principles

SBO station blackout

SFAIRP so far as reasonably practicable

SFP spent fuel pool

SG steam generator

SGHWR steam generating heavy water reactor

SGRV steam generator relief valve

SGTR Steam Generator Tube Rupture

SLB Secondary Line Break

SMR Small Modular Reactor

SNSA Slovenian Nuclear Safety Administration

SOEOP Symptom-Oriented Emergency Operating Procedure

SR Supporting Requirement

SSC Structures, Systems and Components

SSTC NRS State Scientific and Technical Center for Nuclear and Radiation Safety of Ukraine (Ukrainian TSO)

SUP Safety Upgrade Program

TAG Technical Assessment Guide

TSC Technical Support Centre

TSO Technical Safety Organisation

UJV Ústav Jaderného Výzkumu (Czech TSO)

VTT VTT Technical Research Centre of Finland Ltd.

WGOE Working Group on Operational Experience

WGRISK Working Group on Risk Assessment

WENRA Western European Nuclear Regulators Association

APPENDIX 3

# LIST OF FIGURES

APPENDIX 4

# LIST OF TABLES

ETSON | EUROPEAN TECHNICAL SAFETY ORGANISATIONS NETWORK

**ETSON SECRETARIAT - IRSN**
31, avenue de la Division Leclerc
B.P. 17
92262 Fontenay-aux-Roses Cedex
France

www.ETSON.eu

*Association n° W921001929*