Review of Probabilistic Safety Assessment as Part of the Periodic Safety Review for NPP Paks

Attila Bareith
NUBIKI Nuclear Safety Research Institute, Budapest, Hungary

Abstract: Review of plant specific PSA and its applications by the licensee was an important component in the latest periodic safety review for the Paks NPP. The review was performed in 2017 in accordance with the recommendations of a specific guide issued by the Hungarian Atomic Energy Authority, and it included analysis scope, analysis methods and assumptions, input information, analysis tools and results, and uses of PSA in safety management. The review results confirm that the Paks PSA broadly satisfies the PSA related regulatory requirements and recommendations. The importance of maintaining the existing living PSA program to continuously improve PSA quality and strengthen the basis for PSA applications is supported by the review findings. The need to make advancement in site level risk assessment for the plant was also identified in the review. Some corrective actions have been proposed based on a limited number of non-compliances revealed in the review. These proposals are currently subject to regulatory evaluation, just as the entire periodic safety review report.

Keywords: PSA, Periodic Safety Review, NPP Paks, Corrective Actions

1. INTRODUCTION

According to nuclear safety regulations, a periodic safety review (PSR) of a nuclear power plant (NPP) should be performed in every 10 years in Hungary. The latest PSR for the Paks NPP was conducted in 2017. The plant consists of four PWR units of Russian design, labeled as VVER-440, Model 213. The plant is located near the town of Paks, virtually in the middle of Hungary. The net output of 440 MWe was increased to 500 MWe for each unit in 2009. The Hungarian Atomic Energy Authority (HAEA) has issued a regulatory guide [1] that describes recommendations concerning the goal and the technical contents of the review as well as the approach to be followed by the licensee during the review. Review of safety analyses is a most important part of the PSR, and it covers analysis of design basis accidents, complex beyond design basis accidents, severe accidents and probabilistic safety assessment (PSA). The review of the level 1 PSA for NPP is discussed in this paper with some references to level 2 PSA aspects too. The actual review of PSA included analysis scope, analysis methods and assumptions, input information, analysis tools and results, and use of PSA in safety management.

2. REVIEW REQUIREMENTS

The Hungarian regulatory guide on PSR recommends that it should be evaluated in detail whether or not the analysis

- fulfills the PSA related regulatory requirements,
- complies with the regulatory guide on PSA and with good practices,
- gives a true and credible representation of the actual plant conditions by adequately incorporating the effects of plant changes implemented and lessons learned from operating experience in the last 10 years,
- is suitable for an up-to-date characterization of plant safety from a PSA perspective,
- is appropriate for use in fulfilling regulatory requirements on PSA applications in support of safety management at the plant.

Top level mandatory regulatory requirements on nuclear safety are specified in the so-called Nuclear Safety Codes (NSC) in Hungary. These were the most important requirements considered in the review. Volume 3 of the NSC [2] includes design requirements for existing NPPs. PSA related requirements are also specified in this volume. These requirements define the expected scope and levels of PSA, the analysis methods and associated assumptions for some key PSA tasks (e.g. analysis of dependent failures, human reliability analysis, risk quantification, etc.) on a general level and the acceptability of quantified risk measures. In short, a full scope level 1 and level 2 PSA is required for a nuclear power plant. Acceptance criteria, as opposed to probabilistic safety goals, are given in the NSC as 10^{-4}/year for core damage frequency (CDF) and 10^{-5}/year for large release frequency (LRF). Volume 4 of the NSC [3] list requirements related to the operation of NPPs. These requirements include expected PSA applications with focus on support to risk-informed safety management. The list of required applications corresponds very well with "Issue O: Probabilistic Safety Analysis" within the reference levels of the Western European Nuclear Regulators Association (WENRA) that were updated in 2014 [4] to incorporate lessons learned from the Fukushima Dai-ichi accident.

It is noted that a ministerial decree on fire protection requirements in NPPs was also considered in the review as this decree contains specific requirements for fire risk assessment too.

The HAEA has issued a guide on PSA for existing NPPs [5]. The guide includes recommendations on performing the various PSA tasks so that the analysis can be considered acceptable by the HAEA. The recommendations specifically address key PSA steps ranging from identification of initiating events to risk quantification. The guide also provides specific recommendations for analysing internal events, internal hazards and external hazards, uncertainty and sensitivity analyses, and PSA documentation. The features of the Paks PSA were compared with the recommendations of the regulatory PSA guide. Similarly, use was made of the IAEA guides on level 1 and level 2 PSA [6], [7], although it should be noted that the regulatory PSA guide reflects very well the contents of these IAEA documents.

3. PSA SCOPE

The scope of the plant PSA was examined by using the following scope attributes:

- levels of the analysis,
- sources of potential large releases,
- initiating events,
- plant operational states,
- range of accident sequences models.

As to the levels of the analysis, level 1 PSA and level 2 PSA have been performed for the Paks NPP in agreement with the requirements of the NSC. Fulfillment of the quantitative risk criteria for CDF and LRF was the primary objective of these analyses, but, naturally, the intent was to meet all other PSA related regulatory requirements too. The need to provide support to safety related decisions by the plant management was considered during the developments of the PSA model. In this respect the use of the level 1 PSA to develop proposals for preventive safety improvement measures and to evaluate the effectiveness of these measures should be highlighted. Risk-informed evaluation of decisions related to plant operation and maintenance is another general area of applying the level 1 PSA model. Level 2 PSA played a significant role in the implementation of severe accident management measures and guidelines at the plant. Both level 1 and level 2 PSAs were already available at the time of the previous PSR performed in 2007. However, substantial improvements were made to the analysis in terms of scope (i.e. ranges of initiating events covered) and details of the analysis (e.g. elaboration of system fault trees) between 2007 and 2017 which was the target period of the latest PSR.

Detailed PSA is available for the reactor and for the spent fuel pool (SFP) as sources of large releases. A screening analysis was performed to justify that this scope was sufficient as potential releases from other sources were found inferior to that of the reactor core and the SFP. As accidents during fuel handling other than storage in the SFP may directly affect plant personnel, a dedicated probabilistic

analysis has also been performed for fuel manipulations with the refueling machine. This is a new element in comparison to the previous PSR in 2007. With this scope the Paks PSA satisfies not only the requirements of the NSC but also the WENRA recommendations that explicitly indicate the need to include the SFP in PSA. The Paks PSA is made up of unit specific analyses and the corresponding four unit specific PSA models. So far, multi-unit or multi-source issues have not been examined and evaluated in detail, and thus site-level risk assessment is not available for the plant at present. However, developmental work has already started in this emerging PSA area.

The PSA covers an analysis of internal events, internal hazards and external hazards as main categories of initiating events for both the reactor and the SFP. The scope of the analyzed internal events was more or less the same during the previous review in 2007, although some refinements were made including a more detailed classification of loss of power events and events leading to inadvertent primary circuit dilution in low power and shutdown states. Within internal hazards, internal fires, internal flooding and heavy load drops were subject to PSA modeling. Again, the scope was identical at the time of the previous PSR in 2007. However, the input data and the PSA model for internal fires and internal flooding were updated several times and considerably modified between 2007 and 2017. The PSA for external events include seismic events, extreme weather (straight wind, snow, rainfall, ice formation, low and high temperatures, lightning and tornado) and riverine events endangering water intake from the river Danube. All other natural and man-made external hazards have been screened out from the analysis. Even though a lot of developments are still ongoing in the area of external events PSA for the Paks plant, the scope of the current PSA is a lot broader than it was during the previous PSA, as detailed PSA modeling was limited to earthquakes in 2007.

Full power as well as low power and shutdown states of the plant have been considered in the PSA for the reactor and for the SPF. The analyzed low power and shutdown modes are representative for complete and partial refueling outages too. The duration of the different PSA plant operational states (POSs) was refined during the latest PSR period using feedback from operating experience. POS definitions remained unchanged despite the fact that a 15-month fuel cycle was introduced at the plant in 2016 instead of the earlier 12-month fuel cycle.

Table 1 gives an overview of the PSA scope for the Paks NPP.

Table 1. Scope of Level 1 PSA for NPP Paks at the Time of the Latest PSR

Release Source	Operating Mode	Initiating Event	Unit 1	Unit 2	Unit 3	Unit 4
Reactor	Full power	Internal	Done	Done	Done	Done
		Int. Fire	Done	Done	Done	Done
		Int. Flooding	Done	Done	Done	Done
		Earthquake	Ongoing	Ongoing	Done	Ongoing
		Extreme weather	Basis: Unit 3	Basis: Unit 3	Done	Basis: Unit 3
		Riverine events	Basis: Unit 3	Basis: Unit 3	Done	Basis: Unit 3
	Low power & shutdown	Internal	Done	Done	Done	Done
		Int. Fire	Done	Done	Done	Done
		Int. Flooding	Done	Done	Done	Done
		Earthquake	Ongoing	Ongoing	Done	Ongoing
		Extreme weather	Basis: Unit 3	Basis: Unit 3	Done	Basis: Unit 3
		Riverine events	Ongoing	Ongoing	Ongoing	Ongoing
SFP	All	Internal	Done	Done	Done	Done
		Int. Fire	Done	Done	Done	Done
		Int. Flooding	Done	Done	Done	Done
		Earthquake	Ongoing	Ongoing	Done	Ongoing
		Extreme weather	Basis: Unit 3	Basis: Unit 3	Done	Basis: Unit 3

During the development of the Paks PSA it was a declared aim to develop detailed accident sequence models for the consequences of each screened-in initiating event to the greatest extent seen practically

achievable. Of course, limitations in deterministic simulations of plant transients and lack of knowledge about plant responses to some complex accidents (including multi-failure scenarios in particular) required the use of simplifying and/or bounding assumptions in some cases, which imposed limitations on the completeness of the accident sequence models. The models are subject to regular reviews within the living PSA program for the plant. It helps to maintain and improve the scope and the credibility of accident sequence descriptions in the PSA.

4. METHODOLOGICAL ASPECTS

Two important factors helped simplify the review of the Paks PSA from the point of view of the adequacy and acceptability of the analysis methods applied:

1. There is a living PSA program in place for the plant.
2. The HAEA performed detailed independent expert reviews of the plant PSA during the reference period of the PSR.

The Paks living PSA program has been introduced in accordance with the recommendations of the regulatory PSA guide [5]. 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. The summary report of the PSA is identical to Chapter 15.3 of the FSAR. Thus this FSAR chapter is also kept up-to-date as a result of the living PSA. Moreover, the licensee submits the complete electronic PSA documentation and the PSA model to the HAEA after each update for information. The regulators can follow and check the evolution of PSA in this manner.

Two independent regulatory reviews of the plant PSA were performed in the latest PSR period: one for full power PSA [8] and one for low power and shutdown PSA [9]. As a conclusion of these detailed reviews, the HAEA defined a number of obligations and non-mandatory recommendations to improve the quality of the PSA to satisfy their requirements and enable the use of the analysis in different PSA applications. These improvements had been made and the corresponding documents had been submitted to the regulatory authority for evaluation well before the PSR.

Under these circumstances, a top level review was performed in the PSR concerning analysis methods and the most important assumptions made during PSA model development and quantification. The major steps of the PSA were in the focus of attention in this part of the review: analysis of initiating events, development of accident sequence models, system analysis and fault tree development, analysis of dependent failures, human reliability analysis, assessment of input reliability data, analysis of internal and external hazards, risk quantification, and documentation and quality assurance.

4.1. Analysis of Initiating Events

Table 1 lists the major categories of initiating events that were subject to analysis in the Paks PSA. Markedly different approaches were used to select and characterize the specific initiating events belonging to these categories due to the differences in the nature of underlying initiators and in the data and analytical methods that can be used to determine their frequency of occurrence. As an example, Table 2 shows the internal initiating events of the full power PSA. The review found that the PSA documentation provided a reasonably detailed and transparent description of the initiating event analysis process. The regulatory PSA reviews concluded that the causes and contributions to loss of normal power supply should be investigated in more detail, and there was a need to update some initiating event frequencies using more recent data. These required improvements have since been made leading, among others, to the distinction between loss of off-site power (LOOP) and loss of normal power supply induced by on-site power supply faults.

The initiating events included in the Paks PSA can be considered as various types of single internal events, single internal hazards and single external hazards, respectively. In the analysis of internal and external hazards the plant transients that can be induced by a hazard were modeled in fine details

(including multiple plant transients). However, correlated external hazards have not been analyzed systematically yet.

Table 2. List of Internal Initiating Events in the Full Power PSA for NPP Paks

Initiating Event	
ID	**Description**
A1	Gross Reactor Vessel Rupture
A2	Control Rod Ejection
B1	Large Loss of Coolant Accident (LOCA): Loops 2, 3, 5 Cold Leg
B2	Large LOCA: Loops 1, 6 Cold Leg
B3	Large LOCA: Loop 4 Cold Leg
B4	Large LOCA: Loops 1, 2, 3, 5, 6 Hot Leg
B5	Large LOCA: Loop 4 Hot Leg
C1	Medium LOCA not Affecting ECCS Operation (larger break size)
C2	Medium LOCA Affecting Low Pressure ECCS Operation
C3	Medium LOCA Affecting High Pressure ECCS Operation(larger break size)
C4	Medium LOCA not Affecting ECCS Operation (intermediate break size)
C5	Medium LOCA Affecting High Pressure ECCS Operation (intermediate break size)
C6	Inadvertent Opening of Pressurizer Safety Valve
C7	Medium LOCA not Affecting ECCS Operation (smaller break size)
C8	Medium LOCA Affecting High Pressure ECCS Operation (smaller break size)
C9	Inadvertent Opening of Pressurizer Safety Relief Valve
D1	Small LOCA Initiating ECCS Operation
D2	Small LOCA not Initiating ECCS Operation
E1	Primary Water Flow to Secondary Side in Steam Generator not Initiating ECCS Operation
E2	Primary Water Flow to Secondary Side in Steam Generator Initiating ECCS Operation
E3	Interface LOCA Initiating ECCS Operation
E4	Interface LOCA not Initiating ECCS Operation
F1	Trip of Three Reactor Coolant Pumps
G1	Loss of One Feedwater Pump
G2	Loss of All Feedwater Pumps
G3	Feedwater Collector Rupture
G4	Feedwater Line Rupture Outside Containment
G5	Rupture of Feedwater Pump Line
G6	Feedwater Line Rupture Inside Containment
H1	Inadvertent Closure of Main Steam Valve
I1	Inadvertent Opening of Steam Generator Safety Relief Valve
I2	Inadvertent Opening of Main Steam Atmospheric Relief Valve
I3	Steam Line Rupture
I4	Main Steam Collector (Header) Rupture
J1	Trip of One Turbine
J2	Trip of Both Turbines
J3	Electric Load Drop
K1_B	Loss of Normal Power Supply Induced by On-Site Power Supply Faults
K1_K	Loss of Off-Site Power
K2	Loss of One 6 kV Busbar
K3	Loss of Uninterruptible Power Supply to Control Room Indications
K4	Spurious Actuation of ECCS
L1	Loss of Intermediate Cooling to Reactor Coolant Pumps
L2	Loss of Intermediate Cooling to Control Rods
L3	Loss of Make-up Water Pump (Backup Pump Fails to Start)
M1	Spurious Reactor Trip
N1	Uncontrolled Control Rod Withdrawal
N2	Uncontrolled Control Rod Group Withdrawal
N3	Inadvertent Dilution in Primary Circuit

4.2. Development of Accident Sequence Models

The undesired level 1 end-states of the Paks PSA are core damage in the reactor PSA and fuel damage in the SFP PSA, although boiling was also explicitly modeled in the shutdown states with an open reactor and in the SFP PSA. The "small event tree – large fault tree" concept was applied during the construction of the PSA model. Accordingly, the accident sequences are represented as event tree branches. The event trees describe the consequences of functional successes and failures so that the responses of the main mitigating systems and the operators are given in event tree headings. The details of system failures, including that of support systems, are modeled in system fault trees linked to the event trees. Usually a single event tree belongs to each initiating event. In some cases, use of continuing event trees was also found necessary (e.g. LOCA induced by given LOOP scenarios).

The mission time used in the full power PSA is 24 hours under the condition that the processes do not deteriorate beyond this time frame if the sequence specific features modeled in the PSA remain unchanged, i.e. safe stable conditions can be assured. Longer, sequence specific mission times are applied in the low power and shutdown PSA to ensure that the occurrence of the undesired end-state can be avoided with high confidence. As an example, 168 hours is used for the expected duration of water make-up by the emergency core cooling system following LOCA assuming that a stable condition can be achieved within this time frame by appropriate interventions (e.g. fuel upload). Dedicated analyses supported the definition of mission times longer than the typical 24 hours.

The definition of success criteria in the event trees for internal events was an essential task during accident sequence modeling, as the composition of the PSA model was also based on the use of the internal events PSA. Success criteria were determined in the following main steps:

1. delineation of preliminary accident sequence models and definition of associated success criteria by a multi-disciplinary expert panel of design engineers, plant operators, training instructors, deterministic safety analysts and PSA experts,
2. verification of some analysis assumptions by performing accident simulations at the full scope training simulator with considerations to limitations on simulator capabilities,
3. accident simulations using validated computer codes for thermal-hydraulics and neutron physics,
4. review and update of success criteria during annual PSA updates,
5. modification of success criteria as required by independent expert reviews of the PSA,

As part of plant response and fragility analysis, dedicated hazard specific assessments were performed in the PSA for internal and external hazards in order to determine hazard induced failure modes of systems, structures and components (SSCs) that play a role in generating or/and mitigating a plant transient. Multiple plant transients induced by a single hazard were modeled using the assumption that the undesired end-state in such complex situations can only be avoided if each and every plant transient (as internal initiating event) is adequately mitigated. This approach has led to complex accident sequence models for internal and external hazards.

Generally, proceduralized actions were credited as operator responses to accidents in the definition of event sequences. Recovery actions during the progression of an accident were not considered in most cases, unless the performance conditions making recovery feasible could be justified.

Substantial improvements were made in the accident sequence models as a result of the regulatory PSA reviews. The most important improvements were concerned with a complete revision of human reliability analysis for type C human interactions (initiated prior to the regulatory reviews) and a refined analysis of scenarios leading to inadvertent boron dilution in the primary circuit. The latter largely reduced the conservatism in low power and shutdown PSA.

4.3. System Analysis and Fault Tree Development

The most important features and the associated modeling techniques applied during the construction of system fault trees in the Paks PSA can briefly characterized as follows:

1. Similarly to event tree development, the system fault trees built up in the internal events PSA were used as a basis for fault tree developments for all the other categories of initiating events.
2. Failure mode and effect analysis (FMEA) was carried out in support of fault tree development to help the identification of all the credible component failure modes that can affect system reliability.
3. Component boundaries were defined with an attempt to cover the entire failure space, avoid double counting and establish an agreement with component boundaries assumed during the collection of component failure data.
4. The component reliability models were defined in accordance with the capabilities of PSA software used for model development.
5. A modular fault tree structure was established with detailed modeling of mechanical, electrical and instrumentation and control system failures.
6. A dedicated analysis was performed for the failures of equipment in the 400/120 kV switchyard as part of the fault tree analysis for the electric power supply system.
7. Over and above the changes in the availability of safety systems, the analysis took the variations in system configuration and operating conditions (e.g. reduction in the scope of automatic actuations) into account in low power and shutdown states.
8. Schedule maintenance activities are explicitly modeled: if a system is taken out of service for maintenance, the unavailability of the system is modelled by a TRUE event in the entire duration of the associated POS. (POSs were defined so that this distinction was feasible.)
9. Boundary conditions (logic switches) are used extensively in the system fault trees to enable POS and sequence specific definitions of success criteria and operating conditions.

In the analysis of internal and external hazards, the fault trees of the internal events PSA were modified and significantly extended by incorporating the results of hazard specific plant response and fragility analyses. Some distinguishing features of this challenging exercise can be highlighted as arbitrary examples:

- Electrical circuit analyses were performed to help determine and model the effects fire induced hot shorts,
- In the analysis of internal flooding, component failure modes associated with the following effects were examined: submerging under water, water spray, steam spreading, steam or water jet, pipe whip due to high-energy pipe breaks,
- The seismic PSA included a detailed relay chatter analysis to model earthquake specific failure modes of contact devices.

Several modifications and refinements had to be made to the system fault trees based on the conclusions of the regulatory PSA reviews. Also, the transparency of fault trees and the quality assurance manual for PSA updates needed to be improved as a result of these reviews.

4.4. Analysis of Dependent Failures

An attempt was made to explicitly model dependent failure events to a great extent. For example, functional dependence is represented by dedicated sub-models in the system fault trees made up of low (component) level failures of common support systems. Similarly, time related dependence (e.g. phased missions of a system) is directly taken care of in the accident sequence models. Analysis of physical dependence was in the focus of attention in the PSA for internal and external hazards, as the physically induced plant transients and failures in mitigating systems were identified in plant response and fragility analysis. The PSA model for hazards is built up so that physical dependence appears explicitly in the event trees and system fault trees. To this end, it is also noted that the definition of internal initiating events also considers physical dependence. For example, as it can be depicted from Table 2, there is a distinction between LOCA initiating events in accordance with the physical impact

of the event on safety systems. Human related dependence was a task of human reliability analysis (HRA). Dependence between pre-initiator human actions and errors is included in the system fault trees so that the unavailability due to inappropriate human actions is modeled at system train level, and the associated human error probability was obtained by considering the effects of dependence. Dependence between post initiator actions was assessed by analyzing the performance conditions determining the success of different actions and using feedback from dedicated simulator studies [10].

Residual dependent events not modeled explicitly were regarded and quantified as common cause failures (CCFs) by the use of parametric modeling. Diversity analysis helped the identification of common cause component groups, although mostly active redundant components were grouped together. The β factor model as the simplest single-parameter model was chosen for the quantification of CCFs.

The regulatory review of the full power PSA for Paks had emphasized the need to introduce a more sophisticated and appropriate multi-parameter CCF model as opposed to the β factor model. As a result, the feasibility of this change was examined, and a corresponding work plan was proposed with focus on using the α factor model. This plan has not been implemented so far.

4.5. Human Reliability Analysis

The most commonly applied categorization of human actions and human failure events was used in human reliability analysis: pre-initiator (type A) actions, initiator (type B) actions and post-initiator (type C) actions. Human failure events were identified during initiating event analysis and PSA model development. Quantification of human errors required the use of markedly different approaches for these categories due to the differences in failure mechanisms, failure modes and associated contextual conditions [10].

Type A human errors that may occur during maintenance or testing were identified by making a combined use of different information sources: plant data records, observations of test and maintenance activities, interviews with plant personnel and targeted analyses of test and maintenance procedures. A decision tree based approach was used for quantification. The trees describe the relationship between human error probability (HEP) and the most important performance shaping factors as task complexity, quality of relevant procedures, functional tests following maintenance, etc. Type A human errors are included in the system fault trees on system train level with considerations to dependence between human actions related to the components of a system.

The contribution of type B human errors is implicitly included in the frequencies of internal initiating events in the full power PSA. Specific analyses were performed to determine and quantify type B human errors that can occur in low power and shutdown modes. Typical examples of such errors are spurious changeover of an operational loop, spurious drainage of an operational loop, dismantling of wrong equipment, heavy load drops and inappropriate actions causing boron dilution. Type B human errors were also considered as potential causes of internal fires and internal flooding in all the plant operational states.

Mostly errors of omission (EOOs) were analyzed as type C human errors. Errors of commission were taken into account as lower level failures to the extent such errors can contribute to the occurrence of an EOC type PSA human failure event. The methodology used in the HRA for type C human errors is a result of significant developmental efforts supported by numerous dedicated simulator observations performed at the simulator center of NPP Paks between 1993 and 2005. Findings from the simulator studies were used in combination with interviews of training instructors and expert opinion to identify four basic error modes that can lead to misdiagnosis. A detailed procedure analysis was performed for each human failure event to identify pathways of crew deviations from the expected responses. The pathways for diagnosis failures as well as task execution failures were converted into fault trees. Quantification of human failure events included solving of the associated fault trees. Lower level operator actions represented as basic events in these fault trees were quantified by using generic

reliability data, simulator insights and expert opinion in combination. In the PSA for internal and external hazards the aggravating effects of hazard induced conditions on performance influences were considered in HRA.

As noted in Chapter 4.2 in relation to the development of accident sequence models, the regulatory PSA reviews triggered substantial improvements in HRA and its documentation including a refined analysis of type C human errors in particular. The most significant improvement during the PSR period was concerned with modeling the effects of new emergency operating procedures implemented at the plant for full power and for low power and shutdown conditions as well.

4.6. Assessment of Input Reliability Data

The frequencies of internal initiating events at full power were determined by applying generic data and plant experience. Preference was given to using plant experience, although Bayesian update of generic data was necessary in a number of cases due to insufficient plant experience, and generic data were applied to infrequent transients. Internal events in low power and shutdown modes were assessed on the basis of the full power PSA and by performing dedicated reliability analyses (e.g. for heavy load drops and for human induced events). Fire and flood frequencies were estimated by using mostly generic data [11], [12], with considerations to the available limited plant experience. The frequency-magnitude relationships for external hazards were expressed and used as frequency of exceedance curves obtained from dedicated probabilistic hazard assessments.

Component reliability data for random failures were assessed by a combined use of generic data and plant specific experience applying the same priorities as in the estimation of initiating event frequencies. As discussed in Chapter 4.3, unavailability due to planned maintenance is explicitly modelled, as opposed to using unavailability values in the system fault trees. The probabilities of SSC failures induced by the effects of different hazards were determined as a result of hazard specific fragility analyses. Naturally, human errors were quantified in within HRA, as summarized in Chapter 4.5.

In addition to the need to improve HRA, the HAEA specified four tasks in relation to refinements in the assessment of initiating event frequencies and component failure rates for random failures. The need to use more recent data in the assessment was the common driver for these obligations.

4.7. Analysis of Internal and External Hazards

The analysis of internal and external hazards includes some key specific tasks:

- identification, screening and probabilistic description of hazards,
- analysis of plant response to hazard induced loads and assessment of fragility of SSCs,
- event sequence modeling with emphasis on the progression and mitigation of multiple hazard induced plant transients,
- risk quantification tasks specific to hazards PSA including point estimates, uncertainty, importance and sensitivity analyses.

These specific tasks were mapped into the overall PSA process, and their review was made accordingly. For example, the specifics of event sequence modelling in the internal and external hazards PSA were evaluated during the entire review of the accident sequence models – as briefly noted in Chapter 4.3.

A number of requirements had been defined in the conclusions of the regulatory PSA reviews to enhance traceability of the hazards PSA and investigate some phenomena in more detail within the PSA for internal fires and internal flooding. A refined analysis of fire and flood induced structural damage to SSCs was the most important consequence of these requirements that has led to considerable changes in PSA results too.

4.8. Risk Quantification

Quantification of the accident sequence models was based on the most commonly used approaches including generation of minimal cut sets for the PSA end-states and calculation of end-state frequencies. The RiskSpectrum PSA code [13] was the major quantification engine. In the external hazards PSA use was also made of dedicated software developed to enable convolution of hazard and fragility curves and numerical uncertainty analysis. The point estimates of risk were used for comparisons with numerical risk criteria.

Uncertainty analysis addressed mostly aleatory uncertainties quantitatively, although quantitative uncertainty analysis in the external hazards PSA covered uncertainties in knowledge too. The effects of epistemic uncertainties were predominantly described in a qualitative manner. Sensitivity of the results to important model parameters and assumptions were studied and evaluated in accordance with the recommendations of the regulatory PSA guide. Most importantly, the necessity of plant improvements was assessed using support from sensitivity analyses.

The resolution of regulatory PSA reviews addressed deficiencies in the documentation of PSA results and the need to underpin the cut-off values used in risk quantification. These deficiencies have been eliminated by now.

4.9. PSA Documentation and Quality Assurance

The documentation of the PSA study has gradually evolved since the early 1990s. The current version was developed to satisfy mostly the requirements of the NSC, the recommendations of the regulatory PSA guide and the specific safety guides of the IAEA. The regulatory PSA reviews helped a lot to improve PSA documentation and quality assurance as well. To satisfy one of the recommendations of these reviews, the complete PSA documentation is currently accessible electronically by means of a pdf controller. This documentation includes all the PSA reports together with the reference documents used in the analysis. Also, the PSA model and the data forms of a data base used in the PSA for internal fires and internal flooding can be accessed through this electronic platform. A specific quality assurance manual on PSA update in the Paks living PSA program was developed in response to a conclusion from the regulatory review of the full power PSA. That manual is also subject to regular reviews and updates to help ensure adequate PSA quality.

5. INPUT DATA AND ANALYSIS TOOLS

Although the regulatory guide on PSR [5] recommends that the adequacy of input information and analysis tools used in PSA should be separately reviewed and evaluated, this task was practically accomplished in close connection with the review of the different PSA steps. Input information to the plant PSA was reviewed in the following breakdown:

- input to developing accident sequence models,
- input to quantifying accident sequence models.

As can be depicted, the information sources used in PSA are complex and manifold, ranging from plant design data, information on operation and maintenance to the results of accident simulations and special-purpose supporting analyses. These sources were systematically evaluated in the PSR.

The analysis tools fall into one or both of the following categories:

- tools used directly for modelling and quantification of accident sequences,
- tools used directly to generate input information for modelling and quantification of accident sequences.

The RiskSpectrum PSA code and the dedicated database and analysis tool applied in the hazards PSA can be highlighted as directly used analysis tools. The indirectly used tools include, among others, the computer codes applied for deterministic accident analysis, for probabilistic hazard assessments and

for fragility analyses. Similarly to input information, all the analysis tools were evaluated during the course of the review.

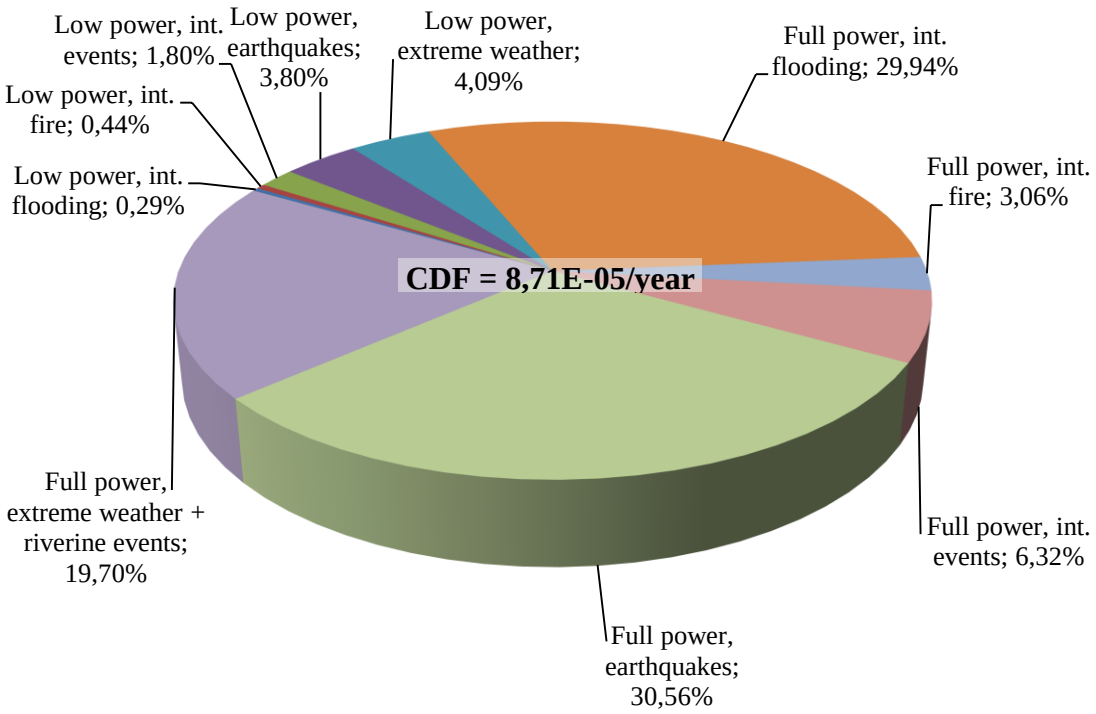
No serious deficiencies could be identified in the review of input information and analysis tools.

6. PSA RESULTS

As the Paks PSA is annually updated in the framework of a living PSA program, and the PSA results are evaluated in these updates, the results were reviewed on a high level only. The review highlighted the changes in PSA results in the 10-year period of the PSR due to evolution in PSA scope and modelling details as reflected in the living PSA program.

Figure 1 illustrates the CDF estimate and the distribution of the main risk contributors based on the latest PSA update for Unit 3. The results show that the CDF criterion of 10^{-4}/year is met. The total contribution of external hazards (earthquake, extreme weather and riverine events) to the CDF is close to 60%. Internal flooding at full power is also an important contributor to the core damage risk (almost 30%). Of course, the PSA results were reviewed in lot more details including quantitative results and qualitative findings such as PSA based evaluation of potential safety improvement measures.

Figure 1. Results of Level 1 PSA for the Reactor of Unit 3 at NPP Paks



7. REVIEW FINDINGS

The review results confirm that the Paks PSA broadly satisfies the relevant regulatory requirements and recommendations. The evaluation of compliance with PSA related NSC requirements presented in the FSAR is satisfactory, except for some requirements prescribing the use of PSA in the safety management of the plant. The importance of maintaining the living PSA program to continuously improve PSA quality and strengthen the basis for PSA applications is also supported by the findings of the review. The need to make efforts to perform site level risk assessment for the Paks plant by making use of the achievements from international co-operative research and development activities was also identified in the review.

Based on a limited number of non-compliances, the following corrective actions have been proposed:

- The external events PSA reported in the FSAR should be extended to the SFP the meet WENRA recommendations.
- A work plan should be developed for a systematic analysis of correlated external hazards, and the PSA should be enhanced by performing the analysis tasks outlined in the work plan.
- The post-Fukushima measures implemented or planned to be implemented at the plant should be subject to PSA modeling and quantification, as necessary based on the expected effects of these measures on plant risk.
- To fully meet regulatory requirements, PSA applications should be strengthened and documented in the FSAR in the following areas: training of plant personnel; support to test, inspection and verification programs; support to ensuring availability of safety significant plant components and systems.

These proposals are currently subject to regulatory evaluation, just as the entire PSR report.

8. CONCLUSION

Review of plant specific PSA and its applications in the management of plant safety was an important component in the latest periodic safety review for the Paks NPP. The review was performed in accordance with the corresponding regulatory guide. The review results show that the plant PSA and the applications of PSA broadly satisfy the relevant regulatory requirements and recommendations. However, some corrective actions have been proposed based on a limited number of non-compliances identified. These proposals are currently subject to regulatory evaluation.

References

[1] *Periodic Safety Analysis Reports of Nuclear Power Plants.* Regulatory Guide A1.39, Version 2. Hungarian Atomic Energy Authority, August 2016 (in Hungarian)

[2] *Nuclear Safety Code, Volume 3: Design Requirements for Operating Nuclear Power Plants.* Annex 3 of Govt. Decree No. 118/2011 (VII. 11) Korm.

[3] *Nuclear Safety Code, Volume 4: Operation of Nuclear Power Plants.* Annex 4 of Govt. Decree No. 118/2011 (VII. 11) Korm.

[4] *WENRA Safety Reference Levels for Existing Reactors. Update in Relation to Lessons Learned from TEPCO Fukushima Dai-ichi Accident.* WENRA RHWG, 24th September 2014

[5] *Probabilistic Safety Assessment for Nuclear Power Plants.* Regulatory Guide A3.11, Version 3. Hungarian Atomic Energy Authority, January 2018 (in Hungarian)

[6] *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants.* Specific Safety Guide No. SSG-3, International Atomic Energy Agency, Vienna, 2010

[7] *Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants.* Specific Safety Guide No. SSG-4, International Atomic Energy Agency, Vienna, 2010

[8] *Independent Expert Review of Probabilistic Safety Assessment of the Paks Nuclear Power Plant for Operation of the Reactor at Full Power.* Review Report, Revision 1.0. OAH/NBI-ABA36/07,. Ri-Man Engineering Consultant, 21 December 2007 (in Hungarian)

[9] *Independent Expert Review of Probabilistic Safety Assessment for Low Power and Shutdown Operational States of the Paks Nuclear Power Plant Units (SPSA).* Review Report III., Version 1. OAH/NBI-ABA-01/11-M (OAH/NBI-ABA-01/11-M-FJ-01), Alex-Eng. Ltd., 10 August, 2011 (in Hungarian)

[10] *Level 1 Probabilistic Safety Assessment of NPP Paks. Appendix A5. Detailed Description of Human Reliability Analysis.* Report No. 222-318-00/A5, NUBIKI Ltd., 2017 (in Hungarian)

[11] *Fire-Induced Vulnerability Evaluation (FIVE).* TR-10030, Research Project 3000-41, Final Report, Electric Power Research Institute, April 1992

[12] *Pipe Failures in U.S. Commercial Nuclear Power Plants.* EPRI TR-100380, Project 2681, Interim Report, Electric Power Research Institute, July 1992

[13] *RiskSpectrum PSA.* License No. RS-189