Initiatives to Enhance Generation Safety of Paks NPP

Tamas Siklossy[a], Attila Bareith[a], Nora Eigemann[a], Jenő Nigicser[a], Peter Siklossy[a]
[a] Nuclear Safety Research Institute Ltd., Budapest, Hungary, siklossyt@nubiki.hu

Abstract: The ageing of the Paks Nuclear Power Plant (NPP) and the occurrence of occasional unplanned outages and power reductions (derates) due to corrective maintenance have increased the importance of systematically identifying the dominant failure modes leading to generation losses. A thorough understanding of these contributors enables the implementation of targeted measures to enhance plant availability and achieve tangible economic benefits, especially with regard to current plant life time management efforts. To support this objective, the approaches commonly used in Probabilistic Safety Assessment (PSA) have been extended beyond the traditional focus on nuclear safety to help improve generation safety. Two complementary analytical initiatives have been launched: (1) the identification of Single Point Vulnerabilities (SPVs), and (2) Generation Risk Assessment (GRA). Components classified as SPVs are those whose failure may directly prevent continuous and stable power generation, thus representing significant contributors to generation risk. In order to minimize their impact, a dedicated SPV program was established, within which PSA models were utilized to the maximum practical extent to systematically identify SPVs. In parallel, a methodological framework for GRA was developed to quantify the probability and expected magnitude of future generation losses resulting from system and component failures. GRA provides a quantitative basis for risk-informed decision-making aimed at enhancing generation safety and operational reliability. The analysis of several balance-of-plant (BOP) systems is currently ongoing. To date, detailed generation risk models have been developed for 13 BOP systems and one safety-related system. Building on these analyses and the underlying GRA models, the development of a derate monitor has recently been initiated. This tool can quantify the frequency of plant outage and different levels of derate for a given plant configuration and identify dominant failures that require mitigation. This paper presents the methodological framework and summarizes the main results of these analysis efforts aimed at enhancing generation safety and availability at the Paks NPP.

Keywords: Generation Risk Assessment, Single Point Vulnerability, Trip/Derate Monitor, Generation Safety.

1. INTRODUCTION

The safe and reliable operation of nuclear power plants requires not only the management of nuclear safety, but also a systematic understanding of the factors that affect stable continuous power generation. In a market environment where plant availability directly influences economic performance, unplanned outages and power reductions represent significant operational and financial challenges. This is particularly relevant to ageing plants, where the frequency of corrective maintenance and the associated generation losses tend to increase over time.

The four VVER-440 units of the Paks NPP have been in operation for around four decades, and plant life time management has become a key priority. Recently, the need has emerged to systematically identify the dominant failure modes leading to generation losses and, if necessary, to implement targeted measures to enhance plant availability. To address this need, the well-established methods of Probabilistic Safety Assessment have been extended beyond their traditional focus on nuclear safety to support the assessment and management of generation safety – an area where PSA tools and methodologies offer significant, yet historically less utilized potential. Two complementary analytical initiatives have been launched in pursuit of this objective: (1) the identification of Single Point Vulnerabilities (SPVs), and (2) Generation Risk Assessment (GRA). This paper describes the methodological framework underlying both initiatives and presents the results achieved to date.

2. IDENTIFICATION OF SINGLE POINT VULNERABILITIES

2.1. Objectives and Scope

At the Paks NPP, Single Point Vulnerabilities (SPVs) are defined as individual component failures that may directly cause an automatic reactor trip or result in a condition requiring the operating personnel to immediately shut down the unit based on limiting conditions of operation specified in operating procedures or the Technical Specifications. This plant-specific SPV definition covers reactor trips initiated by an automatic protection signal as well as procedure-driven manual shutdowns, and it forms the basis for all analyses described in this section.

The Paks NPP has decided to establish and operate a dedicated SPV program, with the ultimate goal of eliminating SPVs or, where elimination proves too costly or infeasible, reducing the associated trip risk or applying a bridging strategy. As an essential first step of the program, it was necessary to systematically identify all potential SPVs across the plant to provide input for subsequent program steps such as prioritization, elimination, and mitigation. To support this objective, a methodological framework was developed, combining three mutually reinforcing approaches to SPV identification.

Three categories of SPVs are distinguished: active SPVs that operate or change state by means of some moving parts; passive SPVs that do not require movement or energy to perform their function; and situational SPVs, being either active or passive components, that can cause plant trip only in certain plant operational states and associated plant configurations that are different from normal operation. While the primary focus of the identification effort was on active SPVs, the methodology also covered passive and situational SPVs to ensure completeness of the program scope.

2.2. Methodology

A comprehensive review of relevant international literature and plant-specific information, including plant process descriptions and the operating experience database, was performed to establish the methodological basis for SPV identification. Key references included the EPRI Single-Point Vulnerability Process Guide (Revision 2, 2022) [1], the WANO guidelines on SPV identification [2], and the INPO AP-913 equipment reliability process documentation [3]. In addition, the results of a series of SPV consultations organized with an EPRI expert at the Paks NPP and the insights from a scram reduction workshop of the WANO Paris Centre were utilized in the development of the methodology.

In line with international good practices, three complementary methods were applied in combination to compile a comprehensive SPV list:

- Systematic component-by-component review;
- Analysis of operating experience;
- Targeted evaluation of the PSA (and GRA) model.

The SPV candidates identified through the three methods should undergo further screening and review by a multidisciplinary expert panel with operational and maintenance experience before being confirmed as SPVs.

Method 1 – Systematic component-by-component review. In this step, a multidisciplinary expert panel reviews each plant component and evaluates them based on the SPV definition to determine whether or not their failure can cause a plant unit trip. This assessment can most effectively be carried out within the framework of the equipment reliability program, as part of the criticality categorization process for plant system components. During the evaluation, the direct impact of each component failure on plant process systems is examined from a systems engineering perspective. This constitutes a bottom-up approach, considering individual component failures and assessing their plant-level consequences.

Method 2 – Analysis of operating experience. Plant-specific operating experience is reviewed to identify SPVs that have already caused unexpected generation losses. The analysis covers the review of trip records from the past (ten years in the case of the Paks NPP), monthly operational summaries, and event investigation reports. Events that caused plant trip, i.e. total loss of power generation are selected for detailed review, and the relevant operating procedure entries or/and automatic protection signals are identified.

For each selected event, the following is determined based on a detailed evaluation of the event investigation reports:

- The event was caused by an SPV or not;
- The SPV in question is a situational SPV or not;
- The description and identifier of the SPV and its corresponding system;
- The actual failure mode that triggered the event if it can be determined;
- The scope of similar SPVs, including redundant components performing the same function within the system, support system components that leads to the same consequence if they fail, and components performing the same function in other plant units;
- Possible means of identifying a given SPV and similar SPVs in a comprehensive review, for example through the occurrence of a specific protection actuation signal or a procedure-based operator action;
- Scope of passive SPVs that have previously caused unit trips (only these passive SPVs need to be considered in the SPV program);
- Input information for prioritizing SPVs for elimination or other corrective actions.

Method 3 – Targeted evaluation of the PSA (and GRA) model. The PSA (or GRA if available) model is used to systematically identify SPVs, particularly those arising from support system dependencies and instrumentation and control interactions that may not be readily apparent from the component-by-component review. This method follows a structured, top-down approach comprising five main steps.

In the first step, the undesired end states that are based on the SPV definition are characterized: all reactor protection actuation signals leading to a plant trip, as well as operating procedure entries and Technical Specification conditions requiring the operator to shut down the unit are systematically collected and presented.

In the second step, the set of events leading to the undesired end states is determined. Since the PSA initiating events were identified with the aim of covering all plant disturbances that could lead to core damage under adverse conditions, the initiating event list encompasses all events that could initiate reactor protection actuation signals, albeit in some cases in an aggregated form. Consequently, the list of internal initiating events in PSA constitutes the set of events leading to the undesired end states defined for the purposes of SPV identification.

In the third step, the systems and components associated with each identified initiating event are determined using a top-down approach: the system function failures that can lead to the undesired end states are identified first, and then the systems, system trains and individual components involved in fulfilling each function are determined. Support systems are also explicitly included in the scope. In the risk assessment of the Paks NPP, internal hazards PSA contains the component failures that can cause internal initiating events. Consequently, this model part was primarily utilized to support the identification of component failures that can lead to an initiating event.

In the fourth step, an event logic model is developed for SPV identification purposes. Unlike the traditional PSA model – which focuses on initiating events and the subsequent response of safety systems – the SPV-oriented model addresses situations where the failure of a single system, train, or component is in itself sufficient to cause an undesired end state. Fault trees are constructed for each relevant system function, with the failure of that function as the top event. The resulting fault trees are connected via OR-gates to create a comprehensive model that covers all the end states.

Three aspects are considered critical from a modeling perspective. First, a functional analysis is performed for each system to establish success criteria and develop a failure logic model based on FMECA (Failure Mode, Effect and Criticality Analysis) and subsequent fault tree construction. Second, functional dependencies – failures of shared support systems or common components supporting multiple systems – are explicitly modeled using identical fault tree elements to ensure consistent treatment and avoid double-counting. Third, spurious actuation of plant protection systems is evaluated to determine whether a single component failure can cause an inadvertent reactor trip, and if so, the corresponding failure modes are explicitly represented in the model.

However, it should be noted that existing PSA models in their original form cannot be used directly and completely for SPV identification for the following reasons:

- initiating events are generally (with some exceptions) represented as single basic events, rather than being broken down into component-level failures in the fault trees;
- many balance-of-plant systems are not included in the PSA fault tree models;
- even if the PSA model includes some balance-of-plant systems, they are modeled from the perspective of accident mitigation, rather than maintaining normal operation;
- relevant information from the internal hazards PSA is primarily stored in a separate, dedicated pre- and post-processing PSA tool and needs to be fed into the PSA model.

Consequently, the PSA model needs to be substantially restructured and supplemented. It is noted that the work performed to date has included this restructuring effort as well as the evaluation of GRA models (see Section 3) developed prior to the commencement of the SPV identification project started. Restructuring of fault trees meant, in particular, the reorganization of component failures in the PSA model and the database supporting the PSA for internal hazards into new fault trees suitable for SPV identification.

In the fifth step, the restructured event logic model is evaluated using Boolean algebra to derive the minimal cut sets for each undesired end state. First-order minimal cut sets directly represent potential SPVs, as they describe single component failures that are alone sufficient by themselves to cause plant trip. To identify relevant situational SPVs during online maintenance, the model is re-evaluated setting the basic event representing the given online maintenance configuration to TRUE and interpreting the resulting first-order minimal cut sets accordingly. It is noted that a trip monitor, if available, would be best suited for identifying situational SPVs, as it allows real-time assessment of trip risk for any given plant configuration.

2.3. Key Findings and Lessons Learned

As part of the systematic component-by-component review, the initial SPV list for the Paks NPP was compiled based on the first decision point of the equipment reliability criticality categorization procedure. The scope of potential SPVs identified using the original wording of the first decision point was found to be limited, and the list was further reviewed and revised in light of a refined wording of the decision point.

The analysis of operating experience from the past ten years resulted in the identification of 22 SPVs, 2 of which were classified as situational SPVs. The SPVs found using this method were exclusively electrical and instrumentation and control system components, reflecting the nature of the events recorded in the plant operating experience database.

The targeted evaluation of the PSA model, combined with the evaluation of the GRA model available at the time of the study, yielded a total of 469 potential SPVs. Of these, 304 were identified based on the GRA model of the main condensate system, while the remaining 165 were identified using the restructured PSA model. According to the targeted evaluation of the PSA model, single component failures may lead to the following initiating events:

- loss of all feedwater pumps;

- inadvertent opening of the atmospheric relief valve;
- failure of the intermediate cooling system of reactor coolant pumps;
- loss of both turbine generator units;
- inadvertent reactor trip;
- interface LOCA initiating emergency core cooling injection.

In terms of component types, the 469 SPVs identified using the PSA and GRA models comprise cables (241), transmitters (8) and contact output devices (220), highlighting the dominant role of electrical and I&C components in generation risk at the Paks NPP – a finding that is consistent with the results of the analysis of operating experience.

3. GENERATION RISK ASSESSMENT

3.1. Objectives and Scope

Generation Risk Assessment is a probabilistic analytical framework aimed at quantifying the likelihood and expected magnitude of future generation losses resulting primarily from system and component failures. By applying cost-effective risk assessment methods and models, GRA provides a basis for quantitative estimation of future generation losses, and supports decisions related to preventive maintenance, capital investment, and plant life time management. The primary output of GRA is the expected annual frequency of unplanned outages and different levels of power reduction (derates), as well as the corresponding annual generation risk, expressed in effective full power hours or energy output (MWh/year), taking into account the time required to restore plant operation at full power. In addition, GRA aims to identify dominant contributors to generation risk at the level of systems, components and component failure modes, thereby supporting risk-informed decision-making aimed at enhancing generation safety and operational reliability.

At the Paks NPP, the decision to launch the GRA program was driven by the ageing of the plant and the occurrence of unplanned generation losses due to corrective maintenance, which highlighted the need for a systematic, quantitative understanding of the dominant failure modes affecting plant availability. The need for the establishment of this program was greatly reinforced by the ongoing activities aimed at further lifetime extension of the plant. The analysis focuses primarily on failures of balance-of-plant systems, as operating experience of the Paks NPP has shown that these systems contribute most to unexpected generation losses. To date, detailed generation risk models have been developed for 13 BOP systems and one safety-related system. The results of GRA are expected to support risk-informed asset management, prioritization of maintenance activities and the identification of SPVs, as described in Section 2.

3.2. Methodology

The GRA methodology developed for the Paks NPP builds on the well-established methods of PSA, extending them to address generation safety. The GRA methodology elaborated by EPRI [4] was also utilized extensively. The analysis is carried out using the RiskSpectrum PSA software, ensuring consistency with the existing nuclear safety PSA models of the plant that are also based on this analysis tool.

3.2.1. System Selection and Review of Basic Technological Information

As a first step, the plant systems to be analyzed are selected based on operating experience on loss of power generation, system characteristics, and other relevant factors. As a result of collaboration between the plant's PSA experts and the plant's PSA developers the following systems were selected for detailed analysis:

- Main and auxiliary condensate system;
- Main feedwater system;

- Main steam system;
- Condensate cooling water system;
- Moisture separator and reheater system;
- Turbine;
- Generator;
- 6 kV electrical power supply system;
- Primary circuit;
- Reactor coolant pumps;
- Oil system of the reactor coolant pumps;
- Passive localization system;
- Control and safety protection system;
- High pressure emergency core cooling system.

For each selected system, the fundamental design and other relevant technical information is collected, including detailed system description and P&ID, relevant excerpts from operating procedures prescribing actions to be taken in the event of operational disturbances caused by component failures of the selected system, interlock description, Operational Limits and Conditions, detailed electrical circuit diagrams, and a concise description of past operational events at the Paks NPP that resulted in generation loss attributable to the analyzed system.

3.2.2. Definition of GRA-related Functional Failures

Based on the collected system information, any possible deviation from normal operation that can lead to unit shutdown or derate are identified and described as GRA-related functional failures. These GRA-related functional failures are subject to subsequent event logic modeling, following a top down approach. The end state of each GRA-related functional failure is defined in terms of the associated power reduction level or shutdown state, taking into account that the lower the parameter values characterizing the resulting operational state, the longer it will take to restore power to the nominal level and reconnect to the grid. If a large number of end states are identified, they are grouped into a manageable number of categories, each represented by the state with the lowest partial load or the lowest physical parameter values.

3.2.3. Event Logic Model Development

A fault tree analysis is performed for each GRA-related functional failure as a top event. Fault trees representing the same level of derate are connected via OR-gates. An event tree is also developed to enable the quantification of generation risk in terms of production loss (e.g. in MWh). The event tree headings examine the fulfilment of functions that prevent the corresponding load reduction or shutdown, ordered from the most unfavorable end state to the least unfavorable to avoid one failure combination contributing to multiple end states. The fault trees developed for different power reduction levels are linked to the corresponding event tree headings.

The fault trees are developed in two steps: first, Failure Mode, Effect and Criticality Analysis (FMECA) is performed for each system component; then, the effects of the identified failure modes on the GRA-related functional failures are described by fault trees. The fault tree models include the basic failure events within the system that may lead to the identified GRA-related functional failures, or, more generally, to the prevention of system functions being fulfilled, and reveal the logical relationships between these basic events. As in PSA, the basic failure events include hardware (or software) failures at system component or higher level, as appropriate, and human errors. Hardware failures can be independent, random events or dependent failures due to a shared cause. The PSA fault trees are utilized to the greatest extent possible, supplemented by additional modeling as needed to capture system functions related to generation safety that are not covered by the existing PSA model.

Human errors contributing to generation loss are analyzed for three groups of activities:

- Errors made during normal operation, maintenance, testing or inspection activities that cause latent unavailability of certain – typically standby – systems or components or render them in an unfavorable state in terms of their ability to prevent loss of power generation or reduce the level of derate (so called Type A errors in PSA).
- Errors made during operational or maintenance activities at power, which, alone or in combination with other failures can cause loss of power generation (similar to Type B errors in PSA). The analysis includes operator errors that can be identified by reviewing plant records on past derates, supplemented, if available, by additional errors previously identified by the analysts.
- Errors related to system operation activities aimed at preventing loss of power generation, i.e., inappropriate operator responses to failures that endanger power generation (similar to Type C errors in PSA).

Plant operating experience is used to the greatest extent possible to inform the analysis. Screening human error probabilities are applied when detailed quantitative analysis proves to be impractical due to budgetary constraints, limitations of existing HRA methods or lack of relevant data.

The GRA model fully utilizes the component reliability data contained in the PSA of the Paks NPP, including data on independent and common cause failures. Data not available from the PSA are assessed based on plant-specific operating experience, supplemented by generic data or expert judgement if necessary. Repair times are assessed by plant specialists, making use of available operating experience, information on the availability of spare parts for the different components and expert judgement.

3.2.4. Risk Quantification and Interpretation of Results

Generation risk is quantified using the Unconditional Failure Intensity (W) calculation option available in RiskSpectrum PSA. If the model has been properly prepared for this purpose by defining each basic event as either initiator or enabler type events, as appropriate, then this type of calculation can be used to determine the frequency of generation loss without the need for post-processing. The point estimates of generation risk include:

- Frequency of derate levels and shutdown with the plant operational state to be achieved;
- Expected annual production loss, expressed in MWh or Effective Full Power Hours (EFPH).

Importance and sensitivity analyses are performed to identify dominant contributors in terms of plant systems, components, failure types and human errors. Numerical uncertainty in the results is characterized through Monte Carlo simulation and fitted lognormal distributions. In interpreting the results, first-order minimal cut sets are distinguished and denoted as potential SPVs.

3.3. Key Findings and Lessons Learned

An illustrative example of the analysis results is presented below for the main feedwater system.

Four end states were identified for this system: full shutdown (100% derate), 50% derate, 30% derate, and 3% derate. The following GRA-related functional failures were identified and considered in the assessment:

- Loss of main feedwater pumps: 30% derate or 100% derate, conditional on the number of the operating pumps;
- Water level increases in the high pressure pre-heater due to spurious actuation: 3% derate (so-called 1st limit water level protection), 50% derate (additional valve failure, turbine stop), or 100% derate (2nd limit water level protection);
- Spurious closure of a control valve: 100% derate (2nd limit water level protection);

- Pipe rupture in the high pressure pre-heater: 100% derate (additional valve failure, 2nd limit water level protection).

Considering all derate levels combined, the aggregate generation risk figures for the main feedwater system are as follows:

- the annual frequency of generation loss is 6.17×10^{-1} events/year;
- the annual average generation loss expressed in effective full power hours is 1.91×10^{1} EFPH;
- and the annual expected generation loss is 9.55×10^{3} MWh.

The dominant risk contributors identified for the main feedwater system are cable failures, specifically failures of water level measurement cables in the high-pressure preheater supply cabinet, and cable failures of the control valves assuring water level in the high-pressure preheaters, which prevent valve reopening from the main control room. The distribution of generation loss frequency and annual average generation loss in EFPH across derate levels is illustrated in Figure 1 and Figure 2. A key observation is that the frequency-based and MWh-based metrics show markedly different pictures: while the 3% derate level dominates the frequency of derates (event/year), full shutdown events contribute to the largest extent to the generation loss risk due to their high derate level combined with the longer recovery times of such events. This illustrates a key insight from the GRA approach: frequency-based metrics can be misleading in themselves, and the MWh-based generation loss metric provides substantially deeper and more practical insights into maintenance prioritization and asset management decisions.

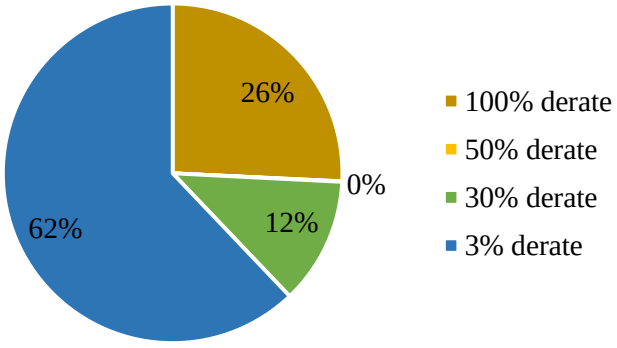

Figure 1: Frequency of power generation loss across derate levels (endstates)

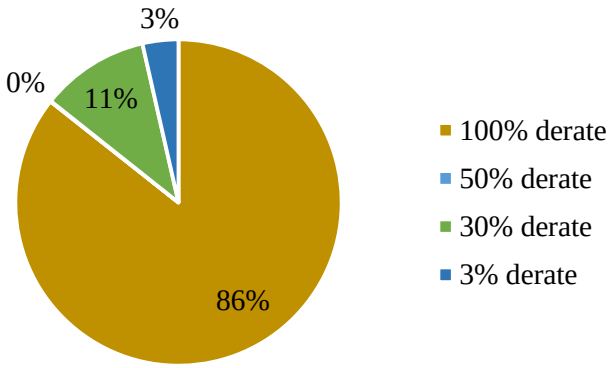

Figure 2: Annual average power generation loss in EFPH across derate levels (endstates)

The analysis of selected systems is still ongoing, and aggregate results across all modeled systems have not yet been consolidated. The calculated generation risk values were compared with the Paks

operating experience of past derate events and plant trips. The comparison generally showed a good agreement. The model-based and experience-based values typically fall within the same order of magnitude. The observed differences are attributable to conservative modeling assumptions regarding the consequences of equipment failure modes and the magnitude of associated derate levels; these can be refined in future model updates.

As part of model quality improvement, a targeted review was performed in which the GRA results were compared with historical plant events for each system analyzed, and any obvious model deficiencies that were relatively easy to address were corrected. An important methodological lesson has been learnt from this review: since GRA focuses primarily on spurious actuations, rather than functional failures, as is typical in PSA, it was necessary to revise and extend the set of failure modes considered in the PSA model. Specific additions included the failure of control valves to operate (valves stuck open due to mechanical causes), impulse line ruptures, and cable failures.

In a broader sense, the analysis of balance-of-plant systems proved significantly more challenging than expected. The identification of event sequences leading to partial load reduction and the development of detailed electrical and I&C fault trees, especially those related to spurious protection actuations, resulted in significant modeling complexity. In terms of dominant failure types, electrical and I&C components and cables contribute the most to generation risk, as they can trigger spurious actuation. The existing PSA model was found to be only marginally applicable for this purpose, which confirms the need for extensive further model development to support the assessment of generation risk and the application of an appropriate risk model.

4. FUTURE PLANS

In line with international good practice, the SPV program at the Paks NPP is intended to be operated as a living program throughout the remaining plant lifetime. To ensure that the program does not stagnate after initial implementation and remains useful over time, regular monitoring and review of the list of SPVs is recommended for all three identification methods:

- Systematic component-by-component review: any new or re-evaluated components within the equipment reliability program should be examined against the SPV definition and the SPV list updated accordingly.
- Analysis of operating experience: annual review of events at the four Paks NPP units is recommended, with particular attention to identifying SPVs that caused trip of an NPP unit and extending the SPV scope to further passive components.
- Targeted evaluation of the PSA and GRA model: to support SPV identification, it is recommended to evaluate the newly developed GRA model parts and periodically review PSA and GRA model updates, taking into account plant modifications and method improvements, to assess their impact on the scope of SPVs. The PSA model may also need to be further developed to identify SPVs that are related to system functions not yet included in the current scope of SPVs.

As far as the GRA program is concerned, the analysis of the selected plant systems is still ongoing. When completed, the assessment of aggregate generation risk for all modeled systems is consolidated, and recommendations are developed for improving generation safety. The full-scale GRA model is also planned to be used to support detailed cost-benefit analysis, strengthening the economic basis for defining targeted measures to reduce annual generation losses.

In parallel, further refinement of the GRA models is planned as follows:

- A detailed review of input reliability data is considered necessary including:
  - Repair times considering the plant’s asset management system and operating experience;
  - Component reliability data based on operating experience and, if necessary, generic data;
  - Power ascension times and load curves required to characterize recovery duration.

- A more detailed human reliability analysis is also planned, with particular focus on erroneous maintenance and operational interventions during normal operation that can cause generation loss, as well as a review of corrective operator actions manifested in past events at the plant.
- Finally, a systematic review of the modeled event sequences leading to derate or shutdown by the Paks NPP experts is foreseen, with model updates to be made where new relevant sequences are identified or existing ones are found to require removal from the model.

Building on the underlying GRA models, the development of a derate monitor has recently been initiated. This tool can quantify the frequency of plant outage and different derate levels for a given plant configuration and identify dominant failures that require mitigation. This tool should significantly improve the identification and management of situational SPVs in degraded plant configurations.

5. CONCLUSIONS

Two complementary analytical initiatives have been launched at the Paks NPP to enhance generation safety by applying PSA methods beyond their traditional use to assess nuclear safety: (1) identification of Single Point Vulnerabilities (SPVs), and (2) Generation Risk Assessment (GRA).

For the purpose of identifying SPVs, a methodological framework has been developed that combines three mutually reinforcing approaches: systematic component-by-component review, analysis of operating experience, and targeted evaluation of the PSA and GRA models. The combined use of the latter two methods resulted in a total of 491 potential SPVs. The analysis of operating experience yielded 22 SPVs, exclusively electrical and I&C components, while 469 SPVs were found from the evaluation of the PSA and GRA models, with cables and contact output devices being the dominant component types. The results confirm that a combination of the three approaches is essential for prudent identification of SPVs, as each method captures a distinct subset of plant vulnerabilities.

A methodological framework for GRA was also developed for quantifying the frequency and magnitude of future generation losses due to system and component failures. To date, detailed GRA models have been developed for 13 BOP systems and one safety-related system. The analysis has shown that MWh-based risk metrics provide substantially deeper insights than frequency-based indicators in themselves. The example of the main feedwater system illustrates this finding. The GRA results generally show a good agreement with plant operating experience, which supports the credibility of the methodology.

A most important, overarching lesson from both initiatives is that the existing PSA model, while a valuable starting point, required substantial reorganization and additions to adequately support GRA. Many balance-of-plant systems are not included in the PSA fault tree models, or if they are included, they are modeled from the perspective of accident mitigation, rather than maintaining normal operation. Therefore, balance-of-plant systems needed to be modeled or remodeled for the purposes of GRA, and the scope of failure modes had to be expanded, especially regarding spurious actuations, beyond those typically considered in PSA.

References

[1] Electric Power Research Institute, "*Single-Point Vulnerability Process Guide, Revision 2.",* Technical Report 3002023784, EPRI, 2002, Palo Alto, CA, USA
[2] World Association of Nuclear Operators, *"Single Point Vulnerabilities, WANO Guideline",* GL 2019-02, WANO, 2019
[3] Institute of Nuclear Power Operations, *"AP-913 – Equipment Reliability Process Description",* Revision 6, INPO, 2018
[4] Electric Power Research Institute, "*Generation Risk Assessment (GRA) Plant Implementation Guide",* Technical Report 1008121, EPRI, 2004, Palo Alto, CA, USA