A PILOT STUDY ON DEVELOPING A SITE RISK MODEL

Attila Bareith[1], David Hollo[1], Zoltan Karsa[1], Peter Siklossy[1], Tamas Siklossy[1]

[1] *NUBIKI Nuclear Safety Research Institute, Konkoly-Thege Miklos ut 29-33., Budapest, Hungary, 1121, nubiki@nubiki.hu*

A study was conducted to examine the feasibility of developing a site risk model and quantifying site level risk for the four VVER-440/213 type reactor units of the Paks Nuclear Power Plant in Hungary based primarily on the use of the existing unit specific PSA models. A small scale analysis was subsequently done for the loss of off-site power initiating event to further research the risk modeling and quantification options outlined in the feasibility study. An initial multi-unit PSA model of this initiating event was constructed and evaluated in the small scale analysis for units 1 and 2 of the plant. Grounded on the findings of the two-stage study, recommendations were made to responsible plant personnel to move forward with the analysis and evaluation of site risk using multi-unit and multi-source PSA modeling for a wide range of initiating events and plant operational states. A full scope level 1 PSA for the Paks site is now in preparation by making use of the achievements of the preparatory analyses performed so far.

I. INTRODUCTION

Unit specific probabilistic safety assessment (PSA) models are available for the four VVER-440/213 type reactor units of the Paks Nuclear Power Plant. The PSA covers full power as well as low power and shutdown operating modes, internal events, and internal and external hazards. The analysis addresses both the reactor and the spent fuel pool at each unit. A study was performed to examine the feasibility of developing a site risk model and quantifying site level risk based primarily on the use of the existing unit specific PSA models. A small scale analysis was subsequently conducted for the loss of off-site power initiating event to further research the risk modeling and quantification options outlined in the feasibility study. The pilot study was intended to underpin the decision on how to perform site risk assessment and to identify the most important challenges in performing a full scale analysis.

II. FEASIBILITY STUDY

The feasibility study included a review of risk measures applicable to quantifying site level risk focusing mostly on level 1 measures with some discussion on level 2 aspects. Combined plant operational states of the four reactors and the adjacent spent fuel pools were characterized using the distinct plant operational states defined for the unit level PSA models. The modeling needs of different types of initiating events in a site level analysis were identified. Most importantly, approaches seen viable to assessing site level risk were discussed and evaluated. A preliminary multi-unit PSA model of the loss of off-site power initiating event was then constructed for units 1 and 2 of the plant by experimenting with the analysis approaches outlined in the feasibility study. Besides the use of common PSA methods, the analysis included some developmental work for risk quantification software too.

The feasibility of a site level risk analysis for the Paks NPP was assessed by reviewing publicly available information on international experience in this analysis area and giving considerations to the specifics of the existing unit level PSA studies and models for the plant. The review of international experience covered the activities of the International Atomic Energy Agency (Ref. 1), the conclusions of an international workshop organized by the Canadian Nuclear Safety Commission in this subject (Ref. 2) and interim findings of the European ASAMPSA_E (Advanced Safety Assessment Methodologies: Extended PSA) research project (Ref. 3). Since it was found that site level risk assessment and the associated multi-unit PSA were quite in the early phase of development world-wide, good practices could not be identified. Thus the feasibility assessment had to be based mostly on the judgement of the analysts. In the study particular emphasis was placed on the following, largely interrelated aspects:

- metrics applicable to describing risk at a multi-unit site
- definition of site level plant operational states with considerations to multiple source of releases

- selection of initiating events important to modeling multi-unit effects
- modeling of concurrent (combined) multi-unit or multi-source accident sequences
- description of human reliability in case of a multi-unit or multi-source accident
- modeling and quantification techniques.

II.A. Risk Metrics

Although various types of risk metrics could in principle be applied to characterize site risk, the discussion below focuses on those ones that were found most appropriate for the purpose of the study. The level 1 PSA for NPP Paks includes the quantification of core damage frequency (*CDF*) in the reactor PSA and fuel damage frequency (*FDF*) in the spent fuel pool PSA separately for each of the four units. In principle, the frequency of single and multiple core damage and fuel damage sequences have to be known and aggregated correctly to quantify risk at site level. It is noted that fuel damage can be regarded as a generic term and core damage sequences, most commonly quantified in a level 1 PSA, represent a subset of the entire space of fuel damage situations. However, for the sake of simplicity let us just consider core damage to indicate the measures that can be used for quantifying plant risk. This formalism can then be easily extended to severe accidents of potential release sources other than the reactors at a site, including spent fuel pools in particular.

The site level core damage frequency (*SCDF*) for a four-unit site like Paks can be expressed as given in Eq. (1).

$$SCDF = \sum_{i=1}^{4} CDF_i + \sum_{i=1}^{4}\sum_{\substack{j=1 \\ i\neq j}}^{4} CDF_{ij} + \sum_{i=1}^{4}\sum_{\substack{j=1 \\ i\neq j}}^{4}\sum_{\substack{k=1 \\ i\neq k \\ j\neq k}}^{4} CDF_{ijk} + CDF_{1234} \qquad (1)$$

where
CDF_i is the cumulative annual frequency of accident sequences leading to core damage at a single unit out of four,
CDF_{ij} is the cumulative annual frequency of accident sequences leading to core damage at exactly two units (i and j) out of four ($i \neq j$),
CDF_{ijk} is the cumulative annual frequency of accident sequences leading to core damage at exactly three units (i, j and k) out of four ($i \neq j$, $i \neq k$, $j \neq k$),
CDF_{1234} is the cumulative annual frequency of accident sequences leading to core damage at all the four units.

The value of CDF_i cannot be precisely quantified by using the existing unit specific analyses. This is partly because some of the core damage sequences included in the unit specific PSA models may overlap, i.e. some portion of the unit specific CDF figures may be attributable to multiple core damage sequences. In addition, there can be transients affecting more than one unit at a time, although core damage occurs at one unit only. Such scenarios have not been fully analyzed in the unit specific analyses. The quantification of terms CDF_{ij}, CDF_{ijk} and CDF_{1234} assumes the development of a multi-reactor risk model.

For the purpose of level 2 PSA the frequency of large releases from single as well as multiple sources has to be determined to quantify risk at site level. If there is a single end-state of the level 2 analysis, e.g. large release or large early release, then the frequency of site level release (*SLRF* or *SLERF*) can be obtained by using a formalism similar to the one applied to core damage in Eq. (1). Accordingly, 15 combinations of large releases from the four reactors have to be considered for the Paks plant. By taking large releases from the spent fuel pools into account the number of release combinations grows up to 2^8-1 = 255. It is emphasized that there can be serious differences between the consequences of the different release combinations. From the perspectives of level 2 PSA the magnitude of release associated with combined releases are also of concern, not merely an estimate on the overall large release frequency. This aspect is of particular importance if one intends to take an account of environmental consequences (e.g. implications for level 3 PSA). In the level 2 PSA for NPP Paks there are 15 source term groups for reactor accidents and 2 source term groups for spent fuel pool accidents. For the four reactors and for the four spent fuel pools the number of source term group combinations is in the order of 10^6 if source term groups used in the unit specific level 2 PSA are combined mechanistically for multiple sources of release. This is not manageable in practice, therefore the feasibility study suggested that a limited number of site level release groups should be defined as opposed to literally combining source term groups applied in the unit specific PSA for a single unit. Since the work was focused on level 1 analysis, the definition of such release groups was beyond the scope of the study.

II.B. Plant Operational States

There are 25 plant operational states (POS) in the reactor PSA for a single unit of the Paks plant. These states cover full power and 24 low power and shutdown states representing a refueling outage. The operational states of the spent fuel pool are decomposed into 4 categories in the PSA based on the level of decay heat, the number and storage configuration of fuel assemblies, and water inventory (normal operational level and refueling level) of the pool.

In the analysis of an initiating event that impacts on multiple units or release sources the operational state of the four reactors and the four spent fuel pools at the time of the event has to be taken into account. For example: an initiating event can find the plant in such a state that the reactors of units 1 to 3 operate at full power (POS No. 0 in reactor PSA) with the corresponding spent fuel pools characterized by normal operational volume of water inventory and low level of decay heat (POS No. 4 in spent fuel pool PSA), while the 4th reactor is subject to refueling (POS No. 10 in reactor PSA), its spent fuel pool is filled up to refueling level and the decay heat level is medium in the pool (POS No. 2 in spent fuel pool PSA).

The operational cycles of the four reactors and spent fuel pools as well as the practice of refueling outages (relative schedule to one another and duration) were analyzed, which led to the definition of 123 distinct overall plant operational states. Each overall state is characterized by a unique and physically viable combination of operational states for the four reactors and four spent fuel pools. A high level and simplified representation of these states normalized for a year (8760 hours) assuming a total refueling outage at unit 3 is given in Fig. 1. Simplification lies mainly in the fact that most of the low power and shutdown states of the reactors are represented by a single bar or two, although they have, in effect, markedly different features.

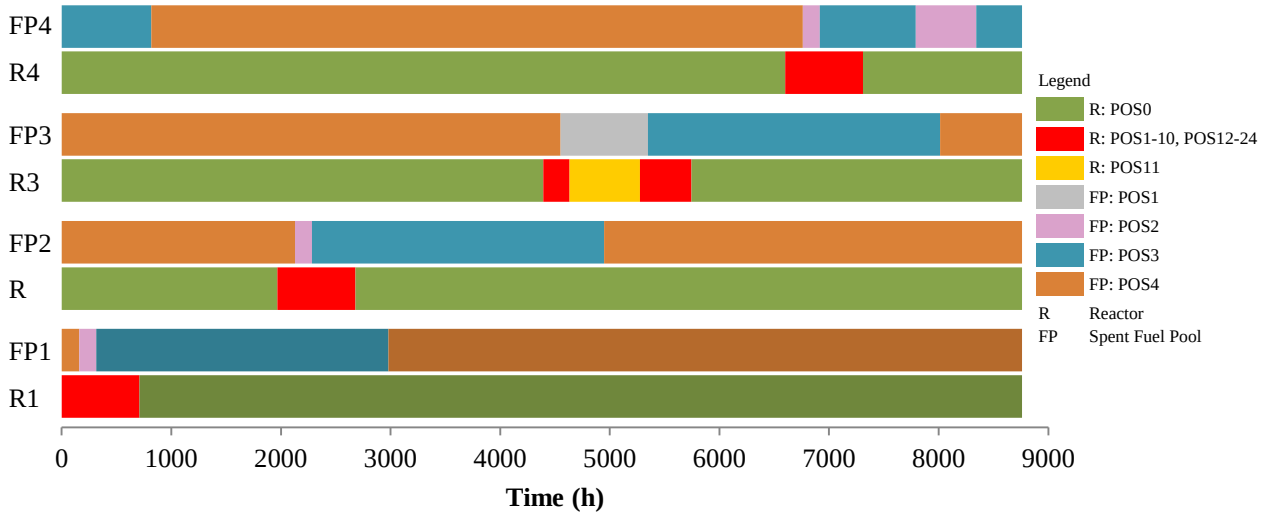

Fig. 1. PSA-Based Plant Operational States in a Year for Four Reactors and Four Spent Fuel Pools at NPP Paks

In principle, a sub-model within the multi-unit risk model has to be developed for each overall plant state to appropriately represent the distinguishing characteristics of a state. In practice, there may be ways to reduce the number of overall plant states based on further, comparative analyses of the states to find bounding plant states for some groups of states (e.g. merging states with similar operational features, bounding low frequency states with less favorable states, etc.).

II.C. Initiating Events

The internal events PSA for the reactors of the Paks plant includes 70 initiating events grouped into 14 categories as follows:

A Reactor vessel damage, 4 initiating events
B Large loss of coolant accidents (LOCA), 8 initiating events
C Medium LOCA, 11 initiating events
D Small LOCA, 3 initiating events
E Interfacing system LOCA (including primary to secondary leaks), 6 initiating events
F Decrease in primary coolant flow, 2 initiating events

G Loss or reduction of feedwater flow, 9 initiating events
H Decrease in steam flow, 2 initiating events
I Loss of steam, 4 initiating events
J Transients causing turbine trip, 4 initiating events
K Electric power supply and instrumentation and control faults, 5 initiating events
L Support system failures and common cause initiators, 4 initiating events
M Unplanned reactor trip, 1 initiating event
N Reactivity induced transients, 7 initiating events

Loss of coolant accidents (initiating event groups A to E) impact only on a single unit directly. Therefore there is no need for a multi-unit model as far as the direct consequences of these events are concerned. However, a LOCA event at a unit can indirectly lead to transients at other units if there are severe consequences of a LOCA induced accident sequence outside the boundaries of the affected unit. Forced shutdown of the neighboring units due to the radiological impact of a LOCA initiated severe accident is an example of such indirect effects that require considerations during the development of a site risk model. Such domino effects should, in general, be taken into consideration for any types of initiating events included in the unit specific PSA. The limiting conditions of operation, the actual as well as the foreseeable consequences of an accident at a unit determine the required response to the accident at other units. The decision on the response should be made by a responsible person or team. The responsible entity can be the unit shift supervisor, the shift supervisor (common for the four units) or the emergency response team, depending on the status of accident progression.

Most of the transient initiating events included in groups G to N also impact only on a single unit directly, which suggests that a consequential initiating event at other units should not be expected. However, some high energy feedwater and steam line breaks within initiating event groups G and I can lead to multi-unit transients attributable mostly to inter-system interactions in the turbine hall. Thanks to the capabilities of the applied modeling tools, these transients can be identified and evaluated on the basis of the existing internal flooding PSA for the Paks plant, as discussed further below.

Loss of power supply to the three 6 kV safety buses of a unit due to on-site failures is described by initiating event K1_B in the Paks PSA. A fault tree has been developed for this initiating event that includes various types of electric component failures at a unit and in the switchyard that lead to loss of power without loss of off-site power. The feasibility study found the fault tree (that is available for all the four units) appropriate for identifying single-unit as well as multi-unit on-site power failure events. The multi-unit power supply failures should then be the subject of multi-unit PSA modeling.

Initiating event K1_K is loss of off-site power in the unit specific PSA model for Paks. This event has a site level effect. Although the PSA model for the K1_K initiating event takes the possibility of ensuring power supply to a unit in island mode of operation of multiple units into account, this option is considered individually for each unit in the unit specific analyses. For a more realistic characterization of handling an off-site power event, a multi-unit PSA model is required.

PSA modeling of internal hazards covers internal fires and internal flooding for Paks. The internal hazards PSA was largely supported by a dedicated database and analysis system. This analysis tool can be used to determine the consequences of a fire or internal flood event in terms of induced failures of systems, structures and components that cause a plant transient and degradations in mitigating systems. Relevant data for all the four units are included in this database and analysis system, which makes it appropriate for determining multi-unit fire or flood induced transients and their consequences too.

The PSA model for external events covers seismic events, high winds, extreme snow as well as ice formation (glaze ice and frost). Numerous other external events were considered in the analysis; most of them were screened out from detailed modeling, though follow-on analysis is still ongoing for a range of external hazards. Unlike internal events and internal hazards, the PSA for external events is currently available for a reference unit of the plant and not for each unit. External events included in the Paks PSA typically impact on the whole site. The feasibility study stressed the need for developing a site level multi-unit PSA model for these events to correctly quantify risk. In effect, external events should be in the focus of attention in a site level risk analysis.

The above statements on the role of the different types of initiating events in site level risk modeling are equally valid for the reactor and for the spent fuel pool, respectively. However, the transients that can lead to fuel damage in the spent fuel pool are limited to loss of cooling and loss of coolant accidents. These transients can occur due to either external or internal failure causes. (For the sake of completeness, fuel damage caused by a direct impact such as large structural damage needs to be mentioned too.)

In summary, the study found that the following categories of initiating events should be subject to modeling multi-unit (and multi-source) effects in PSA:

- Loss of power due to on-site causes
- Loss of off-site power
- Internal hazards included in the single unit PSA: internal fires and internal flooding

- All external hazards included in the single unit PSA: seismic, high winds, extreme snow, ice formation and others
- Any single-unit initiating event that indirectly causes a transient (e.g. forced shutdown) at other units (domino effect).

II.D. Major Challenges in Modeling Multi-Unit Accident Sequences

In general, for all those categories of initiating events that should be in the scope of modeling multi-unit effects, multiple transients affecting some of the four reactors and the four spent fuel pools should be identified, and the responses of the reactor and spent fuel pool systems as well as the operating personnel should be modeled and quantified in an integrated manner in a multi-unit PSA. The feasibility study included a review of the most demanding and crucial tasks in developing such a model. Following is a concise description of some important conclusions of the review.

II.D.1. Power Transfer between Units

The design features and operating procedures of the four Paks units allow transfer of electric power from a plant unit to other units in island mode of operation at house load in case of loss of off-site power. Although disconnection from the grid and power runback to house load are made automatically and separately for each unit, establishment of a stable island mode operation of the four units, including power transfer between units, as needed by the power supply configuration or by failures subsequent to loss of off-site power, requires interventions by the plant personnel. These interventions assume coordinated actions for all the four units that have to be modeled if PSA gives credit to such operating modes and the associated power transfers between units.

II.D.2. Correlated Failures

External events typically lead to multiple failure events at the plant. These failure events are correlated to some extent. Induced correlated failures may occur not only within the boundaries of a single unit but also in multiple units. For example, the study pointed out that according to the assumptions and results of fragility analysis in the Paks seismic PSA, not only the seismic accident sequences of the reactor and the spent fuel pool overlap for a unit, but a number of fragility groups used in the single unit seismic PSA should be extended to actually include the relevant systems, structures and components of all the four units. This approach assumes full correlation of numerous inter-unit seismic failures, which suggest that the cumulative frequency of multi-unit seismic induced core damage sequences is close to the single-unit core damage frequency. An example of plant-wide seismic failures is damage of the large turbine building complex that is common for the four units. This building complex was handled as a single component in the fragility analysis, and the probability of total building collapse was assessed. Accordingly, a seismic failure event that is common for the four units should be included in the multi-unit seismic PSA, and the consequential component and system failures have to be identified at each unit to describe the impact of turbine hall failure. If one intends to relax the rigorous and presumably overly conservative assumption of full correlation, then substantial additional analysis and refinements have to be made to the fragility analyses available for the plant today. Similar considerations hold for other external events too, although the level of correlation among multiple failures depends strongly on the type of the external event and the associated loads, and on the types and modes of induced component and system failures.

Dependent failures within the broader category of correlated failure events should, in general, be treated similarly in a single-unit and in a multi-unit PSA. The overriding principle is to explicitly address dependence between failure events to the greatest extent possible for the various categories of dependence, including physical dependence, functional dependence as well as dependence between human failure events. For functional and human related dependence it is necessary to consider and model resources that are shared or needed to be shared when combating multi-unit or multi-source accident sequences at a time. These aspects are briefly discussed in separate sub-sections below.

Common cause failures as residual failure events not modeled explicitly in PSA can theoretically be extended to common cause failures of components belonging to different units. However, the parametric models used generally to describe and quantify common cause failures do not seem readily applicable to multi-unit common cause failure events. To this end it is noted that even inter-system common cause failures or common cause failures of a large number of components are rarely addressed in contemporary PSA. The feasibility study did not endeavor to propose a method to overcome this shortcoming.

II.D.3.Shared Resources

Shared resources that may have an important role in multi-unit accident scenarios can be basically plant design (technology) and human related. Technology related shared resources are discussed in this section; the human related ones are addressed in the next section.

Because of the design features of the Paks plant, there are resources that are common either to two twin units or even to all the four units. An example is the demineralized water system that is shared by two units. Open loop cooling by steam dump to the atmosphere is required for successful secondary side heat removal in some accident sequences, and demineralized water should be injected into the steam generators in this situation. If the inventory of the demineralized water tanks decreases below the limit prescribed in conditions of operation, then the twin unit has to be shut down according to the Technical Specifications of the plant. Thus a reactor trip transient occurs at the twin unit. This combined scenario is not modeled in the single unit PSA, but it should be considered in the multi-unit model.

The feasibility study identified 16 categories of shared technical resources for the four Paks units, including shared systems (e.g. essential service water system, heating, ventilation and air conditioning systems, etc.) shared structures (e.g. reactor hall, turbine hall, etc.) and shared plant areas outside the building enclosures. Both the success and the core damage sequences of the single-unit PSA models should be reviewed to determine whether the use of shared resources can cause a transient or require interventions that lead to a transient at other units. If such combined events are to be accounted for, then they should be modeled together in the multi-unit PSA by giving appropriate considerations to the reduced availability of shared resources.

II.D.4. Human Reliability

As modeled in the level 1 PSA for Paks, post-accident responses are governed by the symptom-oriented emergency operating procedures (EOPs), and the responses are decided and taken by the operators separately for each unit. This is mostly true for multi-unit accidents too, but it is the responsibility of the shift supervisor to decide on the use of shared resources. This decision and the associated human related dependence should be included and quantified in a multi-unit PSA.

The effectiveness of accident management actions is in the focus of level 2 PSA. In case of a severe accident there is a shift in decision from the main control room personnel to the emergency response team supported by the technical support center. The technical support staff consult the severe accident management guidelines (SAMGs) to aid decision-making. (The EOPs include exit points to the SAMGs as an instruction.) The decided accident management actions are taken by the plant operators, so they have an "execution" role, but they do not make decisions themselves any more. The single-unit level 2 PSA for Paks includes the dependence between level 1 PSA and level 2 PSA actions due to the EOP-driven transfer to the SAMGs. However, other, specific types of decisions and actions, and the associated dependence should be modeled in a multi-unit PSA. The emergency response team is responsible for deciding on the use of shared resources between units and introducing restrictive measures at the different units, using input from the shift supervisor. These decisions and actions can impact greatly on the likelihood of and releases from multiple accidents. There is only limited procedural support to help make decisions that affect multiple units, and the training of the plant personal does not specifically address the treatment of multi-unit accidents. All these aspects should be factored into the HRA of the multi-unit level 2 PSA for Paks. This is considered a very important analysis area that is in need of much developmental work.

II.E. Modeling and Quantification Options

The study raised two basic options to model and quantify site level risk:

- Option 1: event tree linking
- Option 2: minimal cut set conjunction

Option 1 is the interconnection of the unit level accident sequences for each initiating event that can lead to a transient in more than one unit or release source. Interconnection can be made by building a single large event tree that includes all the combined event trees of the four units or by connecting a continuing event tree built for a unit to each event sequence (to success as well as to failure sequences) of another unit. A small scale example of a combined single event tree for core damage is shown in Fig. 2 for an initiating event that affects units 1 and 2 simultaneously (e.g. loss of off-site power). The event tree end states are:

S – no core damage
CD1S2 – core damage at unit 1 only
S1CD2 – core damage at unit 2 only
CD12 – core damage at unit 1 and unit 2.

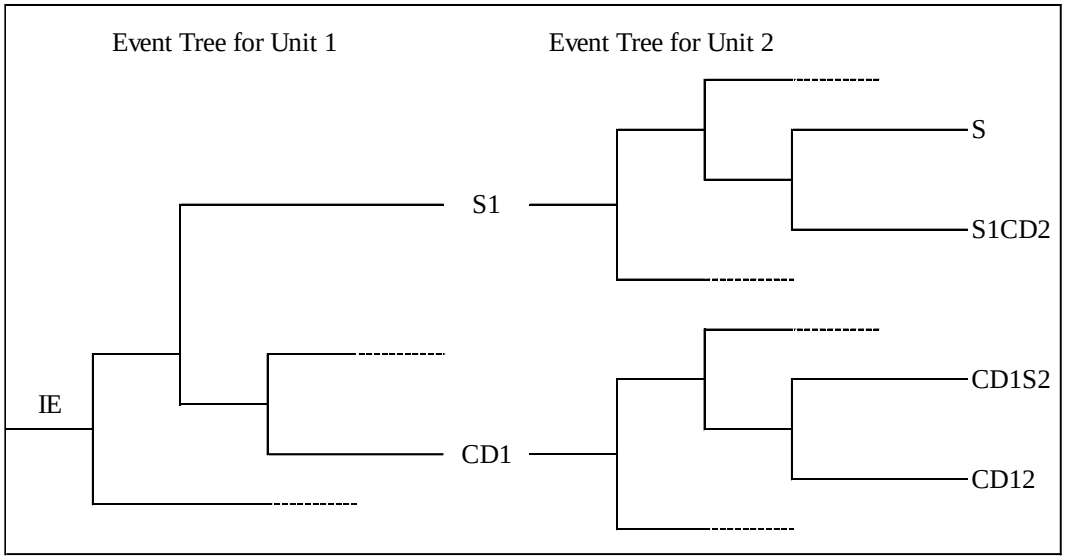

Fig. 2. Construction of a Single, Large Combined Event Tree to Model a Multi-Unit Event

The complexity of the combined event tree increases progressively as more units and more release sources are taken into account. Let us suppose that the individual event trees to be combined include n_i headers and m_i accident sequences for the reactor i. It will then lead to a combined event tree with $\prod n_i$ headers $\prod m_i$ sequences (i = 1,2,3,4). It is not practical or even possible to construct such large event trees manually. The use of continuing event trees does not simplify the modeling solution either, because the number of continuing event trees should be multiplied according to the number of end state combinations (single and multiple successes or failures for the four units) to enable a correct description of the consequences. It is therefore suggested to develop and use dedicated software for model construction in both cases. Another way of event tree linking is the conversion of all the core damage sequences of the event tree for the relevant initiating event at a unit into a fault tree. This can be done by building a fault tree representation of each core damage sequence and connecting these fault trees under an OR-gate. Fig. 3 illustrates this modeling method for the same problem depicted in Fig. 2 before. The complement of successful response at a unit is modelled by fault tree conversion of core damage sequences in the fault trees linked to the headers of the event tree. This solution does not result in a large event tree or numerous event trees, and also it can be done manually by using traditional PSA software. However, the complexity of fault trees increases greatly.

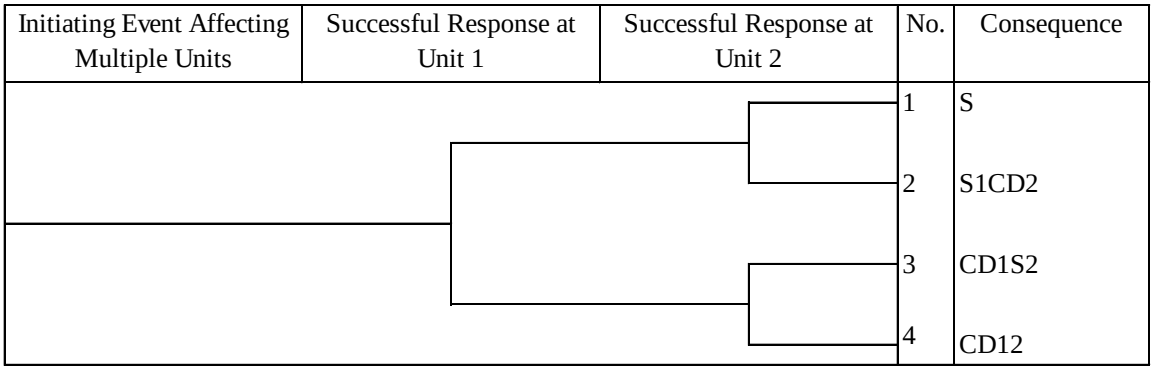

Fig. 3. Simplified Combined Event to Model a Multi-Unit Event Tree Using Fault Tree Conversion of Accident Sequences

Option 2 is conjunction and subsequent Boolean reduction and quantification of unit level minimal cut sets generated for a given end state (core damage or fuel damage) for an initiating event that induces transients at multiple units. This assumes the generation of minimal cut sets for each unit and release source separately, and subsequently combination of those cut sets, rather than developing an integrated model. Quantification of any end state combination is straightforward, and, unlike event tree linking, the method can be relatively easily extended to level 2 PSA too. On the other hand, this approach has some

weaknesses as well. Success branches are not represented in the minimal cut sets, therefore end state combinations that include success sequences cannot be quantified properly. For example, this method can be used to determine the frequency of CD12 but not CD1S2 or S1CD2 of Fig. 2. The precision of the solution is substantially affected by the number of minimal cut sets retained for the analysis, and the goodness of the approximation cannot be assessed correctly.

It must be emphasized that the PSA modeling tasks discussed in Section II.D have to be solved, irrespective of the modeling options used. Thus the combination of the unit level models (either at the level of accident sequences or minimal cut sets) can only yield meaningful results after the models to be combined are prepared for capturing multi-unit effects and phenomena.

III. DEVELOPMENT OF AN INITIAL MULTI-UNIT PSA MODEL

Although the feasibility study confirmed the need for multi-unit PSA to appropriately describe site risk and provided options for solution, the practicability of multi-unit modeling could not be judged merely on the basis of theoretical examples. A small scale pilot study was prepared to experiment with the different modeling options on a real example. Loss of off-site power (initiating event K1_K) was selected for the purpose of the pilot, because it is a multi-unit initiating event itself, and a likely consequence of external events that are important to site risk is this initiating event too. To limit the size of the problem the study was restricted to the reactors of units 1 and 2 operating at full power at the time of the initiating event.

A PSA model for the two-unit analysis was developed by modifying the event tree models of the K1_K initiating event of the two units to accommodate multi-unit effects specific to off-site power and to enable a logically correct analysis by appropriate treatment and designation of shared as well as strictly unit specific systems and other model elements. Most importantly, the electric power supply configurations with the associated power transfer possibilities between the units following a K1_K event were studied and evaluated in cooperation between PSA experts and the operating personnel. Three power transfer modes were modeled, one of them being power transfer from a unit operating in house load to its twin unit via the so-called backup power buses as exemplified in Fig. 4. 11SP denotes the operating turbo-generator at unit 1, 10BL/20BL and 10BM/20BM are the backup buses and X, Y, W are the 6kV safety buses. It is noted that a full scope human reliability analysis was beyond the scope of the study; therefore only rough initial estimates were used to describe the probability of successfully establishing an appropriate power supply configuration in a given power fault scenario.

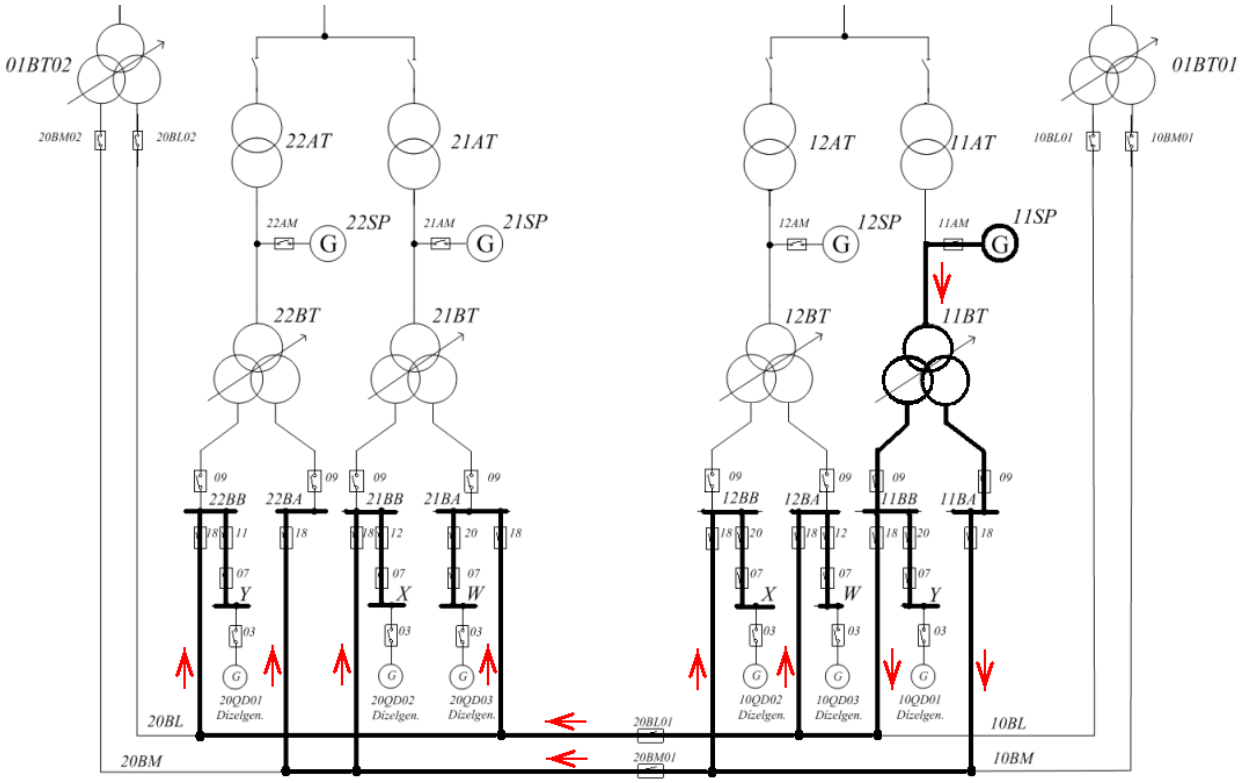

Fig. 4. Power Transfer between Two Twin Units via Backup Buses

IV. RISK QUANTIFICATION

The two-unit PSA model was prepared to enable risk quantification by the use of both options envisaged in the feasibility study.

The event tree linking approach was applied to combine the prepared K1_K event tree of unit 1 (denoted by 1_00_K1_K in the model, with the first character '1' identifying unit 1 an '00' indicating full power) and the same kind of event tree for unit 2 (denoted by 2_00_K1_K in the model) according to the structure shown in Fig. 2. In addition to directly interconnecting all the sequences of the 1_00_K1_K and the 2_00_K1_K event trees to create a large combined event tree, all the core damage sequences of both the 1_00_K1_K and the 2_00_K1_K event trees were converted into fault trees, and the resulting large fault tree for 1_00_K1_K was linked to the first header, while the fault tree for 2_00_K1_K was linked to the second header of the combined event tree in agreement with the model structure depicted in Fig. 3. To be logically correct, success branches of the core damage sequences were modelled in the converted fault trees, not the failed operations. The third method, i.e. the use of continuing event trees was not experimented in the pilot because it could have been actually the same model as the combined large event tree but split into a set of continuing event trees with identical end states.

Minimal cut set conjunction was applied by generating the minimal cut sets for the core damage sequences of the 1_00_K1_K and 2_00_K1_K event trees and subsequently 'multiplying' these cut sets. The minimal cut sets for the individual event trees and accident sequences were produced by the use of the RiskSpectrum PSA code. Dedicated software was developed and applied to perform Boolean reduction and quantification of the combined cut sets.

V. RESULTS

Both of the modelling and quantification options outlined in the feasibility study were successfully applied to determine the constituents of core damage risk: CDF_1, CDF_2, CDF_{12} and *SCDF*, although, as expected, the minimal cut set conjunction method was found much sensitive to the number of minimal cut sets retained for the analysis. The values of CDF_1, CDF_2 were found much comparable to the core damage frequency determined by the original unit specific PSA models for units 1 and 2. These figures are in the order of 10^{-8}/year, closer to 10^{-7}/year than to 10^{-8}/year. CDF_{12} is just a few percent of CDF_1 and CDF_2. Thus the calculated value of the overall core damage risk *SCDF* does not differ significantly from the simple summation of the original, unit specific core damage frequencies for the two units. However, one must not draw serious conclusions from the figures obtained for the core damage risk, since the purpose of this small scale analysis was to examine the practicability of model development and quantification, rather than deriving credible estimates on multi-unit risk.

In addition to determining point estimates of risk, numerical uncertainty as well as sensitivity analyses were also experimented with the two-unit PSA model (using the event tree linking method only), and this attempt was also successful. This paper does not aim at discussing the associated quantitative results but to witness only the feasibility of the analysis.

VI. FOLLOW-ON ACTIONS

The feasibility study resulted in the specification of the major technical tasks in a site risk analysis. A small scale pilot analysis on the loss of off-site power initiating event led to the development and quantification of an initial two-unit level 1 PSA model for the Paks plant. Based on the findings of this two-stage study, recommendations were made and presented to responsible plant personnel to move forward with the analysis and evaluation of site risk using multi-unit and multi-source PSA modeling for a wide range of initiating events and plant operational states. Follow-on analysis is now in preparation to perform a full scope multi-unit level 1 PSA for the four units of the Paks NPP to the extent reasonably practicable. The ultimate goals of the follow-on analysis are to

- Quantify and evaluate level 1 PSA measures (core damage and fuel damage risk) for the whole site
- Identify analysis areas and associated technical issues in need of improvement or refinement to yield credible risk estimates
- Examine how the level 1 PSA for the site can be developed into a level 2 PSA.

VII. CONCLUSIONS

Site level risk assessment was found necessary to enable an improved characterization of risk and a better understanding of plant vulnerabilities. The assessment is considered achievable, but the need was identified for substantial further analysis and developmental work. Consequence modeling for external events and human reliability analysis for multi-unit accidents have to be highlighted in this respect. The pilot study led to a refined proposal for the practical steps to be followed during site risk assessment. The initial multi-unit PSA model developed for the Paks NPP in the study is considered a good starting

point for a full scope analysis. A full scope level 1 PSA for the Paks site is in preparation by making use of the achievements of the preparatory analyses performed so far.

REFERENCES

1. "Technical Approach to Multi-Unit Site Probabilistic Safety Assessment (MUPSA)", Draft Safety Report, International Atomic Energy Agency, Vienna, Austria (2013)
2. Summary Report of the "International Workshop on Multi-Unit Probabilistic Safety Assessment", Ottawa, Ontario, Canada, November 17–20, 2014 (2014).
3. http://asampsa.eu/