AN APPROACH TO JOINT APPLICATION OF INTEGRATED DETERMINISTIC-PROBABILISTIC SAFETY ANALYSIS AND PSA LEVEL 2 TO SEVERE ACCIDENT ISSUES IN NORDIC BWRS

Sergey Galushin[1], Pavel Krčál[2], Lisa Ranlöf[2], Ola Bäckström[2], Yvonne Adolfsson[2], Pavel Kudinov[1].

[1] *Royal Institute of Technology (KTH), Stockholm, Sweden*
[2] Lloyd's Register Consulting, Stockholm, Sweden

In this paper we outline a conceptual approach for combined use of Probabilistic Safety Assessment (PSA) and Integrated Deterministic-Probabilistic Safety Assessment (IDPSA), considering Nordic Boiling Water Reactor (BWR) severe accident issues (specifically ex-vessel steam explosion and debris bed coolability) for illustration.
We describe a conceptual approach based on post processing of the results generated by IDPSA to update the "static" Boolean structures in the standard PSA representation. The challenge in the evaluation is to retain the failure combinations from the PSA to allow for component importance evaluation, to be able to perform the calculations in a reasonable time frame and to use all relevant information from the IDPSA results.
We discuss the approaches for determination of the event space (for IDPSA analysis) which is consistent with PSA damage states from PSA-L1 and L2. We also discuss application of post processing approach for analysis of huge amount of data generated in the process of uncertainty space exploration, which is difficult to use directly in decision making process including incorporation of such data into PSA framework, to update structures of "static" Boolean structures in standard PSA. Using data post processing approach we can significantly reduce amount of information which represents results from IDPSA analysis.
Keywords: Risk assessment, dynamic reliability, PSA, severe accident.

I. INTRODUCTION

Severe accident progression is driven by combination of time dependent physical phenomena and equipment failures. The outcome of Probabilistic Safety Assessment level 2 (PSA L2) can be significantly affected by time and order of events. In order to address the influence, Integrated Deterministic Probabilistic Safety Assessment (IDPSA) approach was proposed [19]. The aim of IDPSA is to support risk-informed decision making. A set of developed methodologies that combine deterministic model of a nuclear power plant with a method for exploration of the uncertainty space can be generally assigned to IDPSA. For instance, Dynamic PSA belongs to the IDPSA family. IDPSA methodologies explore uncertainty space (using methods for uncertainty space exploration) and search for failure domains in system response parameters (using deterministic models). Failure domain is a domain of uncertain parameters where critical system parameters (e.g. pressure, temperature, etc.) exceed safety thresholds. IDPSA itself is not efficient in resolving stochastic equipment failures which is a large part of safety assessment. Therefore, it is suggested to develop an approach for combined use of PSA and IDPSA as complimentary tools in order to use each method where it fits the best.

The goal of this paper is to outline a conceptual approach for such combined use of PSA and IDPSA, considering Nordic BWR severe accident issues (specifically ex-vessel debris bed coolability and steam explosion) for illustration.

In this approach there are several challenges to overcome. First, it is necessary to design a method for providing relevant data about damage states from PSA for IDPSA analysis of L2 sequences. In this paper we discuss the approaches for determination of the event space (for IDPSA analysis) which is consistent with PSA damage states from PSA-L1 and L2. Second, IDPSA generate huge amount of data in the process of uncertainty space exploration, which is difficult to use directly in decision making process including incorporation of such data into PSA framework. In order to overcome these issues we use scenario grouping and classification methodology for post processing of IDPSA analysis results [18] to update structures of "static" Boolean structures in standard PSA. Using Grouping and Classification approach we can significantly reduce amount of information which represents results from IDPSA analysis. Third, we need to design an approach for incorporation of the (reduced) information of failure domain from IDPSA analysis into PSA.

In this paper we describe a conceptual approach that use data from Grouping and Classification of IDPSA results to update the "static" Boolean structures in the standard PSA representation. The challenge in the evaluation is to retain the failure combinations from the PSA to allow for component importance evaluation, to be able to perform the calculations in a reasonable time frame and to use all relevant information from the IDPSA results.

The paper will discuss the approach on how the sequences shall be made consistent between the techniques and also how the quantification is performed.

II. PROBABILISTIC SAFETY ASSESSMENT, ET/FT APPROACH

Within nuclear industry, classical PSA techniques make use of the conventional ET/FT approach as a tool to investigate different scenarios, which can lead, depending on safety system failures, human errors, either to failure or safety domains.

Complete PSA of a plant includes three levels. PSA L1 focuses on phenomena take place in the reactor cooling system and reliability of the core protection systems. The outcome of the analysis is the estimation of Core Damage Frequency (CDF) and correspondent scenarios that lead to core damage (Plant Damage States, PDSs). In Level 2 PSA, the chronological progression of Plant Damage States, identified in PSA L1, is evaluated, and correspondent probabilities of containment failure modes and magnitudes of the radioactive releases are estimated. Level 3 analysis includes the analysis of the dispersion of the radioactive materials from the release and correspondent impact on the environment and human health [1-3].

In a standard PSA, the output of PSA level 1 is typically core damage (possibly separated in a few sub-categories). These core damage sequences are then divided into a number of sub-categories based on attributes, which shall be representing the important features for the level 2 progression.

There are, normally, around 20-40 plant damage states (PDS) defined in the interface between level 1 and 2. This interface is therefore reasonably crude.

For the plant studied in this paper, there are 27 PDSs for power operation and low power operating modes. The attributes that are considered relevant to characterize the core melt for the continued process are:

- Initiating event (Transient or LOCA)
- Time point of the core melt (early, late)
- Reactor pressure (low, high)
- Containment atmosphere (inert, air)
- Can cooling with containment spray system be taken into account (Failed, Yes)
- Activated containment pressure relief (activated, not activated)
- Activated containment filtered release (activated, not yet activated, failed)
- Bypass of containment (bypass, intact)
- Warm suppression pool (warm if pool cooling fails, else cool)

The events that are represented in a PSA level 2 are the events that change the conditions for retaining of releases within the RPV or within the containment. Hence, if the coolability in the RPV is different in different scenarios – then this is vital information. If the sequences are affecting the phenomena that can occur, then this is also vital information.

For each of the PDS there is a containment event tree. The containment event tree (CET) defines the accident progression as analyzed in the PSA. The sequences in the CET end at the release categories (RC), and there are normally around 15-40 of such. The RCs can be defined in different ways, for example release size or defined by type of sequence. The normal approach is to use "by type of sequence", because then only a limited amount of verifying deterministic calculations are considered required. For the "by type of sequence" approach the characterization is based on for example;

- Type of release (over pressurization of containment, filtered release, non-filtered release)
- Timing of release (early, late)
- Initiator (pipe rupture, non-pipe rupture, bypass)
- Sprinkling established (y/n)

The main purpose of this study is to analyze, in a greater level of detail, the attributes that are of interest for the core relocation – and further on melt through of the reactor pressure vessel, RPV, and the following effects on phenomena.

The type of phenomena that are usually accounted for in a PSA are:

- Hydrogen burn (deflagration and detonation)
- In-vessel steam explosion
- Ex-vessel steam explosion
- Direct containment heating
- Rocket mode
- Melt concrete interaction (basemat penetration)
- Steam generator tube rupture (only for PWR)

The effect of the phenomena can be:

- Containment rupture
- Different type of bypass

- Activation of filter

The consequence most focused is of course containment rupture.

From the initial sequences in the PSA level 1, all events that are leading to a certain PDS is then treated in the same manner in the continued sequence (however, dependencies are treated logically correct if the failure should affect systems in PSA level 2). It is however obvious that it will be different scenarios from a deterministic stand point if there is an initial loss of offsite power and no start of the diesels, compared to a scenario where the diesels would stop after some hours.

The purpose with the improved integrated link between the PSA is hence to be able to judge if, for example, these scenarios need to be treated differently in the PSA context.

The approach chosen was to identify some sequences from the PSA level 1 and to use the DPSA methodology to evaluate the progress of these sequences. It will involve in-depth studying of the mechanisms for core relocation, since this is an important factor for the continued sequence. By identifying the mechanisms that contribute to the core relocation, the analysis is also expected to provide information on efficient measures, non-efficient measure or contra-productive measures to avoid core relocation. Eventually, it is expected that the IDPSA integration will give a clearer answers to:

- Can the core melt process/relocation be stopped and how?
- Are there actions that must not be taken during a sequence?
- How will the conditions for phenomena be affected, and thereby give guidance on how to treat these in the PSA?

Based on the above information, refined requirements on definition of plant damage states can be fed back.

III. INTEGRATED DETERMINISTIC PROBABILISTIC SAFETY ASSESSMENT

Integrated deterministic and probabilistic safety assessment (IDPSA) is a set of methodologies that aim to support risk-informed decision making. IDPSA includes both stochastic disturbances and deterministic response of the plant, and their mutual interactions into consideration in safety assessment.

The main motivation for development of the IDPSA methods was early realization that static logic models applied in PSA has inherent limitations in resolving mutual interactions between (i) stochastic disturbances (e.g. failures of the equipment), (ii) deterministic response of the plant (i.e. transients), (iii) control logic and (iv) operator actions [14]. Passive safety systems, severe accident and containment phenomena are the examples of the cases where such dependencies of the accident progression on timing and order of events are especially important.

During the last decade significant progress has been achieved in the development and application of new tools which combine probabilistic and deterministic approaches in order to address issues when timing of the events defines accident progression [6-10].

A common feature of these methodologies is that the possible sequencing of events in scenario evolution is not predetermined by the analyst (as it is the case with the traditional PSA), but rather by a dynamic system model (usually a computer code) as the system evolves in time based on a user specified partitioning of the uncertainty space.

A survey of IDPSA methodologies applied for safety assessment of nuclear power plants can be found in [11].

III.A. IDPSA Methodology and Decision Making Process

It was mentioned, previously, [19] that the readiness of a tool is difficult to determine if there are no clear criteria for success or goal for the analyses. In terms of decision making, quantification of consequences into figures of merit is necessary (i.e. to establish safety goals and success criteria).

IDPSA methods are capable of quantifying aleatory uncertainties in time dependent scenarios. It was emphasized (during the IDPSA meeting 2012 [19]) that this mostly had an effect within the context of academia whereas it did not do much for deployment into the industry. Therefore, the focus must be directed towards what the decision makers need and what they regard as important.

Credibility, uncertainty quantification (robustness of decision), comprehensiveness (risk profile instead of one number) and understanding were outlined as important factors in terms of what kind of data to be provided for the decision makers. Consistency was also emphasized as important since different kinds of decisions (e.g. for industry or regulators) put different requirements on the data provided.

III.B. Risk Oriented Accident Analysis Methodology

The Risk Oriented Accident Analysis Methodology (ROAAM) [20,21] can be considered as an example of a decision support method. The ROAAM marries probabilistic and deterministic approaches. This methodology developed by Professor Theofanous [21] has been applied to successfully resolve different severe accident issues in LWR plants, and severe accident treatments in LWR designs e.g., [23].

When applied to the Nordic BWR plants, the tight coupling between severe accident threats (steam explosion and basemat melt-through due to debris un-coolability) and high sensitivity of the Severe Accident Management (SAM) effectiveness to timing of event (e.g., vessel failure) and characteristics (e.g., melt release conditions) present new challenges in decomposition, analysis and integration (see Figure 1).

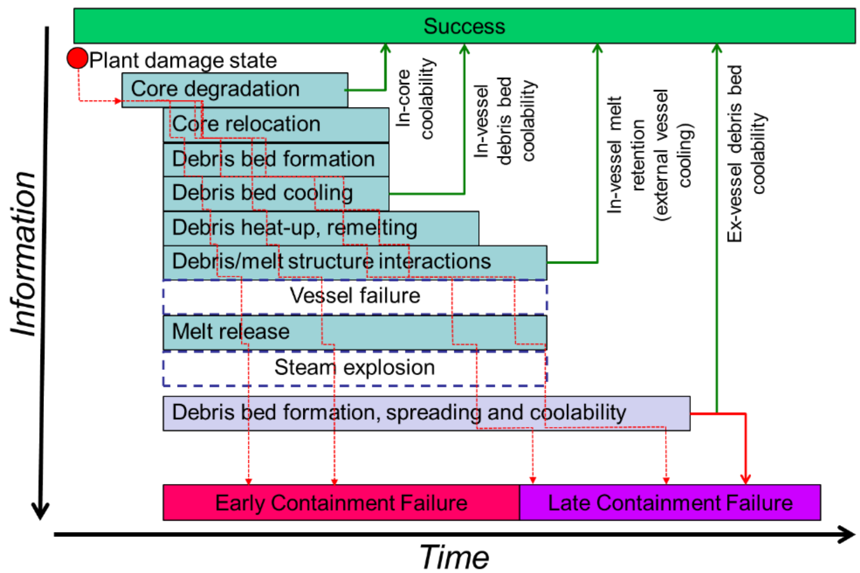

Figure 1. Severe accident progression in Nordic BWR [22].

ROAAM+ framework for Nordic BWR [22] represent a set of coupled modular frameworks (see Figure 2), it is developed connecting initial plant damage states with respective containment failure modes. Deterministic processes are treated using surrogate models based on the data obtained from the fine-resolution models.

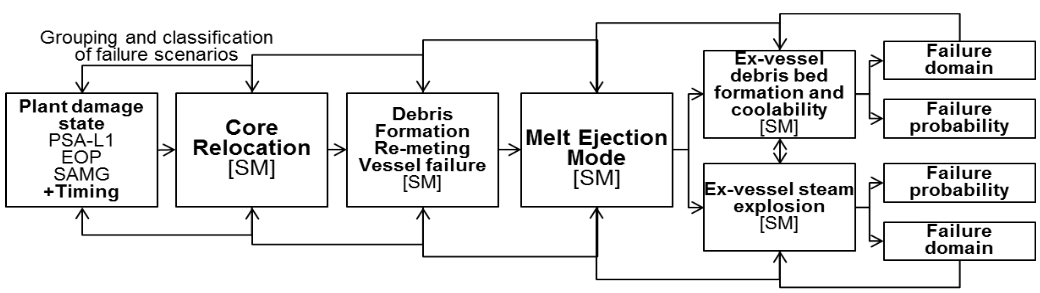

Figure 2. ROAAM+ framework for Nordic BWR [22].

The surrogate models are computationally efficient and preserve the importance of scenario and timing. Systematic statistical analysis carried out with the complete frameworks helps to identify risk significant and unimportant regimes and scenarios, as well as ranges of the uncertain parameters where fine-resolution data is missing. This information is used in the next iteration of analysis with fine-resolution models, and then refinement of (i) overall structure of the frameworks, (ii) surrogate models, and (iii) their interconnections. Such iterative approach helps identify areas where additional data may significantly reduce uncertainty in the fine- and coarse-resolution methods, and increase confidence and transparency in the risk assessment results. The overall modular structure of the frameworks and the refinement process are discussed in the paper [22] in detail.

III.B.1. Scenario Grouping and Classification Methodology for Post processing of Data Generated by Integrated Deterministic-Probabilistic Safety Analysis

One of the common features of IDPSA analysis is a huge amount of the data generated by the deterministic codes. Therefore, one of the main challenges for application of IDPSA methods is data post-processing and communication of the analysis results. Extracted information should be suitable for decision making and risk-informed characterization and eventually improvement of safety and performance of the system. Scenario grouping and classification approach with application of decision trees [18] has been developed for post-processing and visualization of the results generated by IDPSA tools.

III.B.2. Scenario Grouping and Classification Methodology for Post processing of Data Generated by Integrated Deterministic-Probabilistic Safety Analysis

A decision tree is a classification and data-mining tool for extraction of useful information contained in large data sets. An instance is classified by starting at the root node of the tree, testing the attribute specified by this node, then moving down the tree branch corresponding to the value of the attribute in the given example. This process is then repeated recursively for the sub-tree rooted at the new nodes until no further branching in the tree can be made, or some stopping pre-set conditions are met [26]. A flow-chart like structure is generated in which internal nodes represent test on an attribute, each branch represents outcome of test and each leaf node represents class label (decision taken after computing all attributes). Decision trees can be used as a powerful visual and analytical decision support tool, especially in case of multidimensional data, since visualization of results in the original space is non-trivial. Decision tree can be constructed using different data impurity measures (e.g. Gini impurity measure, information gain measure) to select the best split among the candidate attributes at each step while growing the tree [12]. Decision trees also can be used as a predictive model which maps observations about an item to conclusions about the item's target value.

From the PSA and decision support perspective, decision tree in its structure represent success and failure paths that can be interpreted in ET/FT methodology. Indeed, classification of the instances in the data set, performed by decision tree approach, can be interpreted as success and failure paths as it shown in Figure 3. The leaf nodes that correspond to failure domain and correspondent decision rules that lead to these nodes will form failure paths, e.g. in Figure 3, the conditions that lead to failure are (top-to-bottom Y<2, X<3), and, on the other hand, the instances outside the failure domain will be represented by success paths (Y<2, X>3 and Y>2).

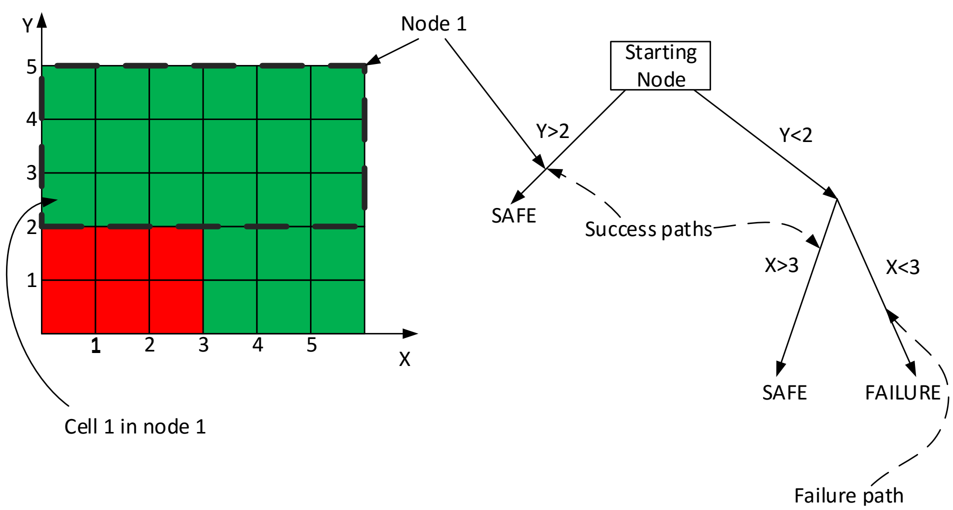

Figure 3. Example of decision tree representation of the failure domain.

The probability (failure/success) for each node can be obtained as follows:

$$P_{(node)} = \sum_{i=1}^{k_j} p_i \quad \xi_i \qquad (1)$$

where p_i - is probability of cell i in node j, ξ_i - probability of cell (scenario) i in node j, k_j - total amount of cells in node j.

IV. APPLICATION EXAMPLE

Decision tree approach can be used for characterization of the failure domains and visualization of the results in the way that can support decision making process.

In this section we illustrate how proposed methodology can be applied in presentation of ROAAM+ framework results.

IV.A. Characterization of the Failure Domain for Debris Bed Coolability

To illustrate failure domain characterization using decision tree approach for debris bed coolability we considered the following case:

- Debris bed coolability (DECO, see Figure 4) model [27,] with no spreading within ROAAM+ framework for Nordic BWR [22].
- Properties of relocated debris are predicted by MEM (Melt Ejection Mode) which include:
  - Vessel Failure Mode analysis [30,31].
  - In-vessel debris coolability [32].
  - Analysis of core degradation and relocation to lower plenum [33].
- Uniform distribution of debris bed angle between 0 and 30 degrees.
- Uniform distribution of particle size between 1 and 3.5mm.

Note, that the results of failure domain analysis with ROAAM+ for debris bed coolability, presented in this paper (see Figure 5), are preliminary and can be considered only for illustrative purposes.

In this paper we consider PDS where the core damage is caused by the loss of effective coolant inventory makeup initiated by station blackout (SBO) with the additional loss of backup diesel generators. The recovery time of the power supply and active safety systems recovery is varied between 1000 and 7200 seconds (2h). In the analysis of the effect of timing on the effectiveness of SAM the following safety systems were considered:

- System 314: Pressure control and relief system (ADS) has several functionalities and is able to operate with only battery backups. Opening of SRV's (system 314TA function) provides instant depressurization of the primary system to a designed operation pressure. The depressurization function (system 314TB function includes VX105 Motor operated valves) is initiated on low water level L6 (1m below the core top) discharging steam to wet well (WW) to a level sufficient for the low pressure injection sources (ECCS) to be activated.
- 314 TA Function. The spring-operated part of the overpressure protection system is still operating to specifications and will open valves stepwise, starting at slightly above 70 bar and opening completely at 75 bar, to discharge steam to the containment and protect the Reactor Pressure Vessel (RPV) from explosive failure.
- System 323: The low pressure coolant injection (LPCI) is part of the emergency core cooling system (ECCS), which provides water injection into the down comer to facilitate reflooding in the bottom of the core. System is activated on L3 level signal (+2m), however water injection starts when pressure difference between wet well (WW) and down comer (DC) is below 12.5bar. Maximum injection capacity of ECCS is reached at 2 bar difference between WW and DC and equals 4x366kg/s.
  - Function will be recovered after a user-imposed time delay, with mass flow of 100% of designed capacity that corresponds to 4 injection trains.

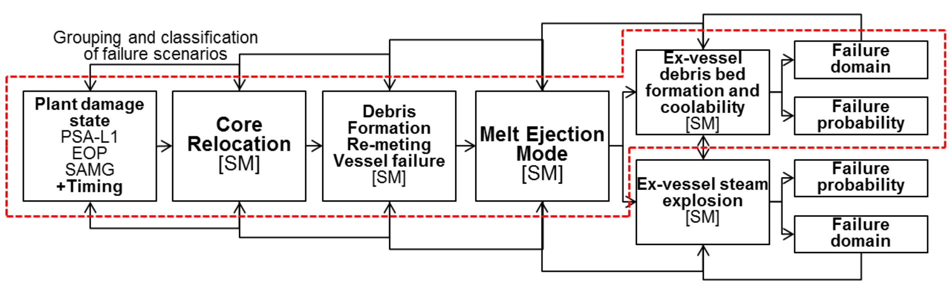

Figure 4. ROAAM+ Framework Nordic BWR (Ex-vessel debris bed coolability)

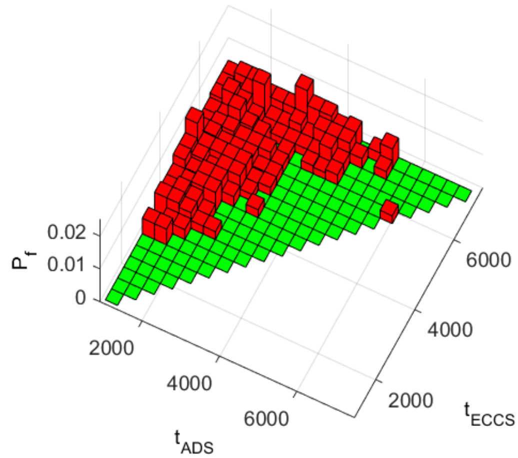

Figure 5. DECO failure domain in terms of input space parameters (ADS,ECCS recovery time (sec)). screening probability 0.001.

ROAAM+ framework analysis gives the following failure domain as a function of input parameters (see Figure 5): ADS (system 314) time delay, ECCS (system 323) time delay – which form accident scenario space.
Failure domain in Figure 5 can be represented in form of decision tree as a set of final nodes and decision rules that lead to these nodes.
Each final node in decision tree (see Figure 6) represents some specific area of scenario space and it is characterized by a set of decision rules that lead to this space. For example in Figure 7 – node j = 1 represent the area of input space where ADS and ECCS activation time is below 2890 seconds (which represents the first decision rule (cut) in the decision tree "ECCS<2890"), the scenarios located in this area represent 10% of the total scenario space for selected PDS.

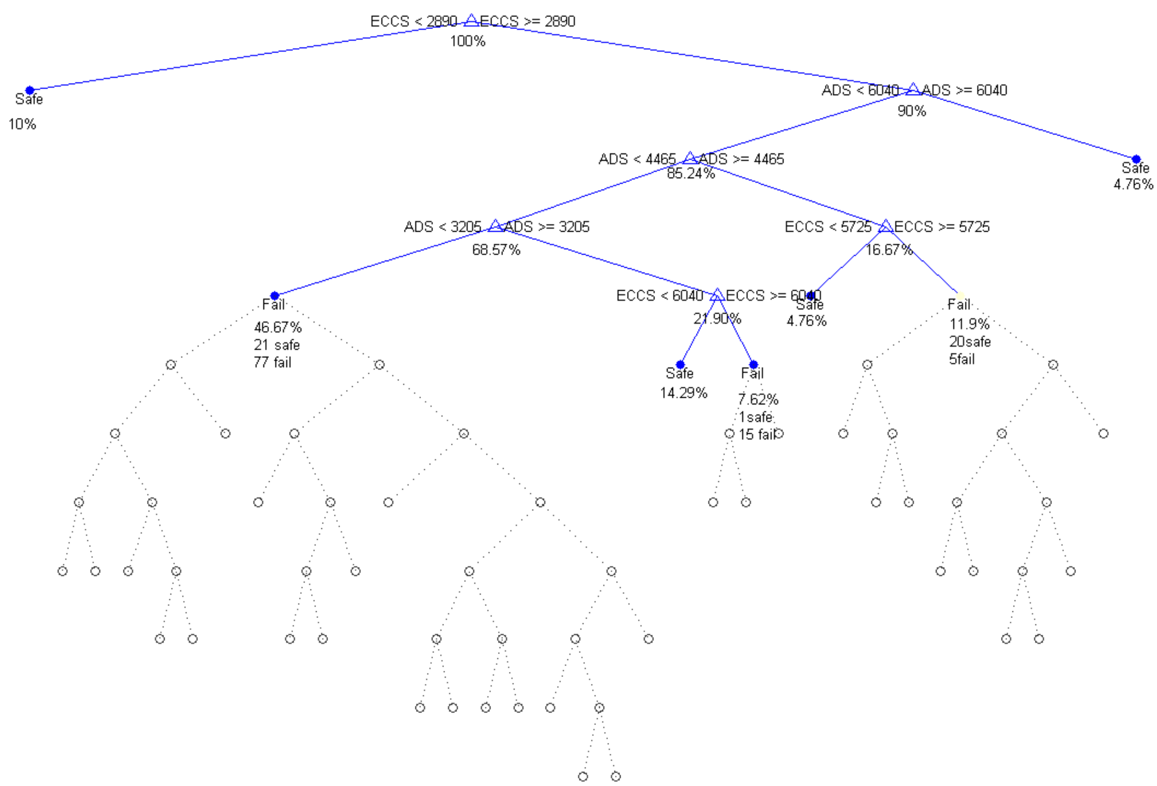

Figure 6. DECO failure domain in terms of input space parameters (ADS, ECCS recovery time (sec)). Decision Tree representation.

The conditional containment failure probability due to DECO (i.e. non-coolable debris configuration in LDW) for each node can be obtained as follows

$$P_{f(node)} = \sum_{i=1}^{k_j} p_{f_i}\,\xi_i \tag{2}$$

where p_{f_i} - is probability of failure of cell i in node j, ξ_i - probability of cell (scenario) i in node j, k_j - total amount of cells in node j.

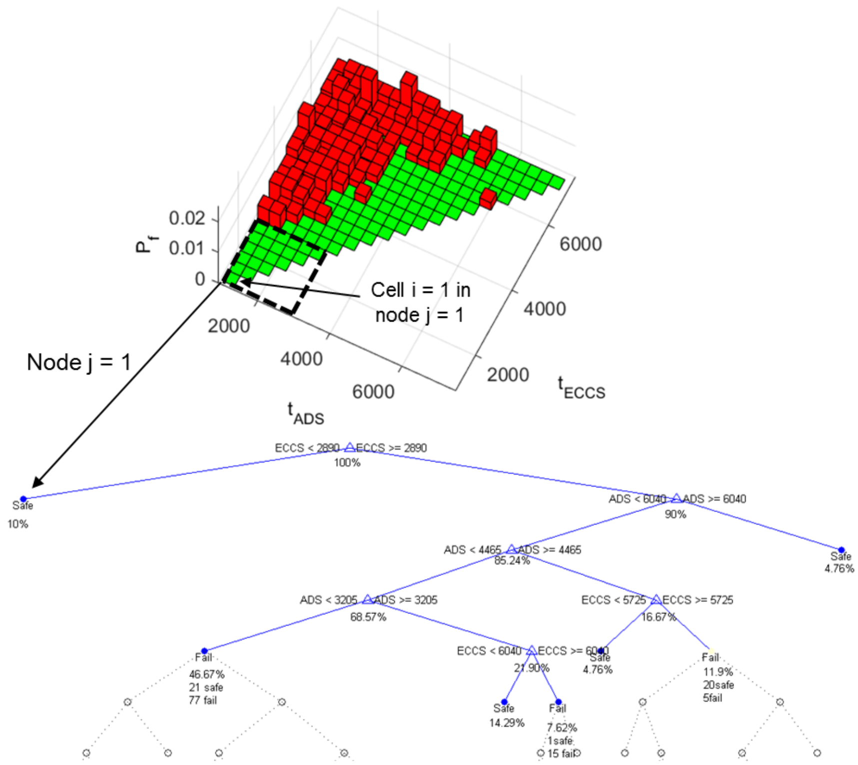

Figure 7. DECO failure domain in terms of input space parameters (ADS, ECCS recovery time (sec)). Decision Tree representation.

If we assume the uniform probability distribution for scenarios in our scenario domain, it is possible to obtain conditional containment failure probability for each node in the decision tree (Table 1). The results presented in the Table 1 indicate that the total conditional containment failure probability due to debris bed coolability for selected PDS, assuming uniform distribution of scenarios in scenario space (i.e. recovery time of ADS and ECCS is uniformly distributed between 0 – 7300 sec) equals $P_f = 2.277264e-3$. Different ranges in safety systems activation times lead to different consequences in terms of debris bed coolability. These results can be considered as accident progression bins (APB) for selected PDS and used as an input for source term evaluation. We can also observe, in the results, that the highest contribution to conditional containment failure probability is given by scenarios with early ADS activation and late ECCS water injection. Table 1 can be represented in form of block diagram (see Figure 8) to provide better understanding of the results.

Table 1: DECO Failure domain characterization

ADS(sec)	ECCS(sec)	Fraction of data explained	$P_{f(node)}$	FLAG
[0,2890]	[0,2890]	0.1	0	safe
[0,1945]	[2890,3520]	0.028571	7.3852e-5	fail
[1945,3205]	[2890,3520]	0.038095	0	safe
[0,3205]	[3520,7300]	0.4	1.80471e-3	fail
[3205,4465]	[2890,6040]	0.142857	0	safe
[3205,4465]	[6040,7300]	0.07619	3.19099e-4	fail
[4465,6040]	[2890,5725]	0.047619	0	safe

[4465,5725]	[5725,6670]	0.057143	0	safe
[5725,6040]	[5725,6670]	0.014286	1.1521e-5	fail
[4465,5410]	[6670,7300]	0.028571	6.8072e-5	fail
[5410,6040]	[6670,7300]	0.019048	0	safe
[6040,7300]	[6040,7300]	0.047619	0	safe
TOTAL			2.277264e-3	

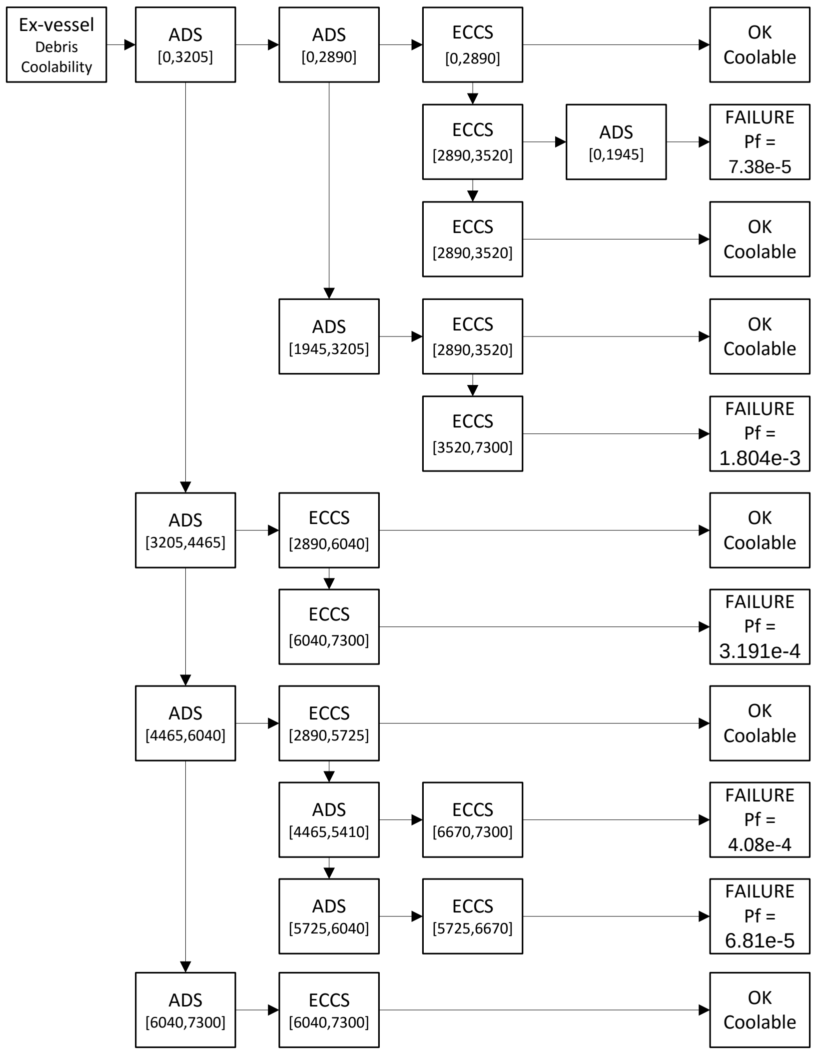

Figure 8. DECO failure domain in terms of input space parameters (ADS, ECCS recovery time (sec)). Block-Diagram representation.

V. DISCUSSION

The results from the study are very interesting from a methodological point of view. It has been shown that a decision tree is a viable way of presenting the output of the DSA analysis. The question is; how can this data be used in a PSA context?

The gains in the PSA using the information from the IDPSA are at least:

- Improved sequence definitions when phenomena can be relevant (improved PDS definitions and the sequences in the containment event tree).
- Estimation of probabilities for phenomena.

V.A. Improved Sequence Definitions

The binning of accident sequences from PSA level 1 into plant damage states as well as the modelling of accident progression scenarios in PSA level 2 are based on factors such as type of initiating event, time from initiating event and pressure in the reactor. These factors, attributes, are normally based on a finite amount of analyses, where engineering judgements are necessary. An IDPSA approach can provide valuable information regarding these factors and influence the definition of sequences in PSA, since the IDPSA approach is informed by significantly more calculations. Several key elements in the level 2 sequences and phenomena handling and their boundaries can be analyzed at each stage of the modelling of accident progression via, for example, a reverse analysis in the ROAAM+.

One example that have been studied with reverse analysis in the ROAAM+ approach is recovery of emergency cooling system (ECCS) and ADS. These safety systems have, for some reason, failed during PSA level 1 and a possibility of system recovery to avoid more severe consequences is modelled in PSA level 2. A successful recovery early in the sequence would allow the core to be arrested in the reactor pressure vessel (RPV) and hence provide the best possibility to limit the releases.

To arrest the core in the RPV based on the assumption that coolability is possible given successful recovery of the ECCS and ADS. Low pressure scenarios with activated re-flooding can for example be considered successful if it is activated within three hours after core melt. This modelling is supported by a few MAAP analyses.

The human reliability analysis regarding recovery actions is based on the available time for the operator action. It can be noted that the dominating sequences for loss of feed water from PSA level 1 are due to loss of external power supply and failure of back-up power systems. The time for possibility of manual recovery of back-up power systems and the time for possibility of return of off-site power are therefore very important for the quantitative results.

The result of the reverse analysis using the ROAAM+ approach is graphically shown in the decision tree, it indicates the “safe” timespans, i.e. recovery of ECCS and ADS leads to coolability of the debris, and “failed” timespans, i.e. even with recovery there is a possibility that the debris may not be coolable. The reverse analysis using the ROAAM+ approach indicates that the current assumptions regarding available time for recovery needs to be updated, since the successful states in the IDPSA indicates that the systems needs to be activated earlier to ensure a successful cooling.

It can be noticed that the “safe” state in the decision tree is given based on a threshold. Safe means, in the ROAAM+ approach, that the conditional failure probability for debris coolability is lower than 1E-3, which indicates in the arbitrary scale of probability a “physically unreasonable” level of likelihood [14].

When likelihoods used in ROAAM+ are translated into PSA probabilities, the arbitrary scale of probability should be applied in reverse in order to achieve the same meaning between “physically unreasonable” level in ROAAM and screening frequency in PSA. For instance, it should be evaluated in a continued study if 1E-3 probability threshold in ROAAM+ should be translated into PSA as 1E-4 of conditional frequency. The reason is that a threshold should preferably be set so that the conditional probability would be insignificant with regard to the target value (frequency of <1E-7 for releases).

The target value for PSA Level 1 is often set as 1E-5. A conditional failure probability for level 2 less than 1E-4 would hence fulfil the condition to be insignificant (two orders of magnitude below the acceptable threshold). This means that all “safe” scenarios can be disregarded in the PSA if 1E-4 is used as a threshold value in the analysis. This is identified as a future update and development of the connection between reverse analysis in ROAAM+ and PSA.

The studied example provides a possibility to identify how timing of the recoveries affects the possibility to obtain ex-vessel debris coolability. The results can be used to improve sequence definition in several ways:

- Give more accurate and refined definition of available times for different operating actions and thus provide a better basis material for the HRA.
- Identify the sequences where the debris may not be coolable after re-flooding.
- Provide failure probabilities for the identified sequences. Coolability may need to be modelled with a failure probability that is dependent on the timing of the sequence. Time dependent failure probabilities can be considered since the plant damage states are binned with time after initiating event as one factor. The binning of the plant damage states may therefore be updated with regards to the findings from the deterministic analysis.

The reverse ROAAM+ analysis has, in addition to the coolability, also provided very interesting preliminary results for the treatment of phenomena in the sequence following melt through. To make full use of the results, more understanding is needed on the factors that is causing the situations that are described by the reverse analysis, for example: What type of sequences (from start) are causing a melt through above a certain size? This is an area where further work is needed.

V.B. Estimation of Probabilities of Phenomena and Consequences

In addition to a better understanding of the sequences and their causes, it has to be recognized that we will neither have full understanding nor the possibility to represent all possible realistic situations in a risk analysis. Hence it will also be of vital importance that, in addition to a better representation of the sequences, we improve our ability to estimate the probability that a certain phenomenon with risk significant consequences can occur.

The analysis of physical phenomena requires extensive understanding of complex interactions and feedbacks between scenarios of accident progression and phenomenological processes. Physical phenomena are of high importance for the PSA level 2 results since they influence the severity of the consequences.

The analysis includes identification of relevant phenomena, identification of relevant sequences where phenomena can occur as well as estimating the probability of the phenomena. The available data for phenomena is often based on scarce data, which typically leads to conservative assumptions. Better support and basis material for the analysis of probabilities for phenomena, given conditions of scenario, would therefore increase the level of accuracy and credibility substantially.

The reverse analysis with ROAAM+ provides insights regarding under what conditions each phenomenon is relevant. The backward analysis regarding steam explosion, for instance, provides information regarding at what conditions a steam explosion can give consequences of risk significance. This may be used as one input to the quantification of probabilities of phenomena with certain consequences since the ratio of "failed" sequences may be used.

The estimation of other level 2 related failure probabilities such as recovery actions can also be refined by the results of the reverse analysis.

V.C. Feasibility Study on Connection Between Conventional PSA, DSA and DPSA Methods in Addressing Severe Accident Issues of Nordic BWRs.

Currently, based on the ongoing work the results from the IDPSA analysis show that there are some thresholds that change the conditions for the sequence. Therefore, it is very likely that these thresholds will be interesting for the PSA. The decision tree approach has also proved that it can refine the information, and there are some very interesting results that will require further evaluation.

The results from the ongoing work are also very interesting from a methodological point of view. It has been shown that a decision tree is a viable way of presenting the output of the IDPSA analysis. The question is; how can this data be used in a PSA context to integrate the models mathematically?

From the PSA, cut set lists are produced (or rather minimal cut set lists). In most PSA tools, like RiskSpectrum PSA, the same approach is used also for PSA level 2. There are other methods to perform the PSA level 2 calculations. The discussion in this paper is focusing on the Minimum Cut Sett Approach (thereafter MCS approach), as used in RiskSpectrum PSA, and how this can be improved by including information from the decision trees developed within the DSA.

Let us assume that we have an MCS list. This list will include basic events representing phenomena (as well as component failures and human actions – but these are not of interest in this context). These phenomena are treated as individual events – and there is no information on timing. Now, let us assume that we have the decision tree as presented in Figure 7.

The MCS list and the information in the decision tree could be merged. Figure 9 is on an overarching level presenting this.

This would mean that each individual combination of failure events, leading to a particular release, could be quantified for the possible alternatives of combinations in the decision tree.

Why is the approach with a decision tree interesting, compared to the alternatives?

There are several possible methods for including timing and correlation between phenomena into a risk calculation. There are mainly two methods:

- Integrated PSA L1 and L2, but probabilities for phenomena is determined outside the PSA tool.
- Integrated PSA L1 and L2, but conditional release probabilities for the different PDSs are calculated outside the PSA tool.

Integrated PSA level 1 and level 2 projects is the most common method for the interface between PSA level 1 and level 2 (the first bullet) is the most common approach for performing a PSA level 2. The advantage with the method is that there will be an automatic treatment of dependencies between level 1 and level 2, failures that are considered will fail both systems in level 1 and level 2. The amount of plant damage states may due to this be limited. The disadvantage with the approach is that a strict probabilistic approach does not include time as a parameter and there is not an easy way to represent other type of dependencies between phenomena.

The second alternative means that the results are computed from PSA level 1, and transferred to PSA level 2 as frequencies for each PDS. This means that the treatment of dependencies will have to be established by defining more plant damage states (then also including system states). It is obvious that the full set of dependencies cannot be represented. This method, on the other hand, is very powerful because an equation system can be defined for the different events that can happen, and time is a possible parameter.

The idea behind the merge of the decision tree and the MCS list would be to capture the good features of the MCS approach, but also to in a condensed way utilize all the relevant information from the deterministic calculations – including timing. An obvious strength of the concept would be to not simplify the very complicated scenarios by equations, but instead use the thresholds that are of interest.

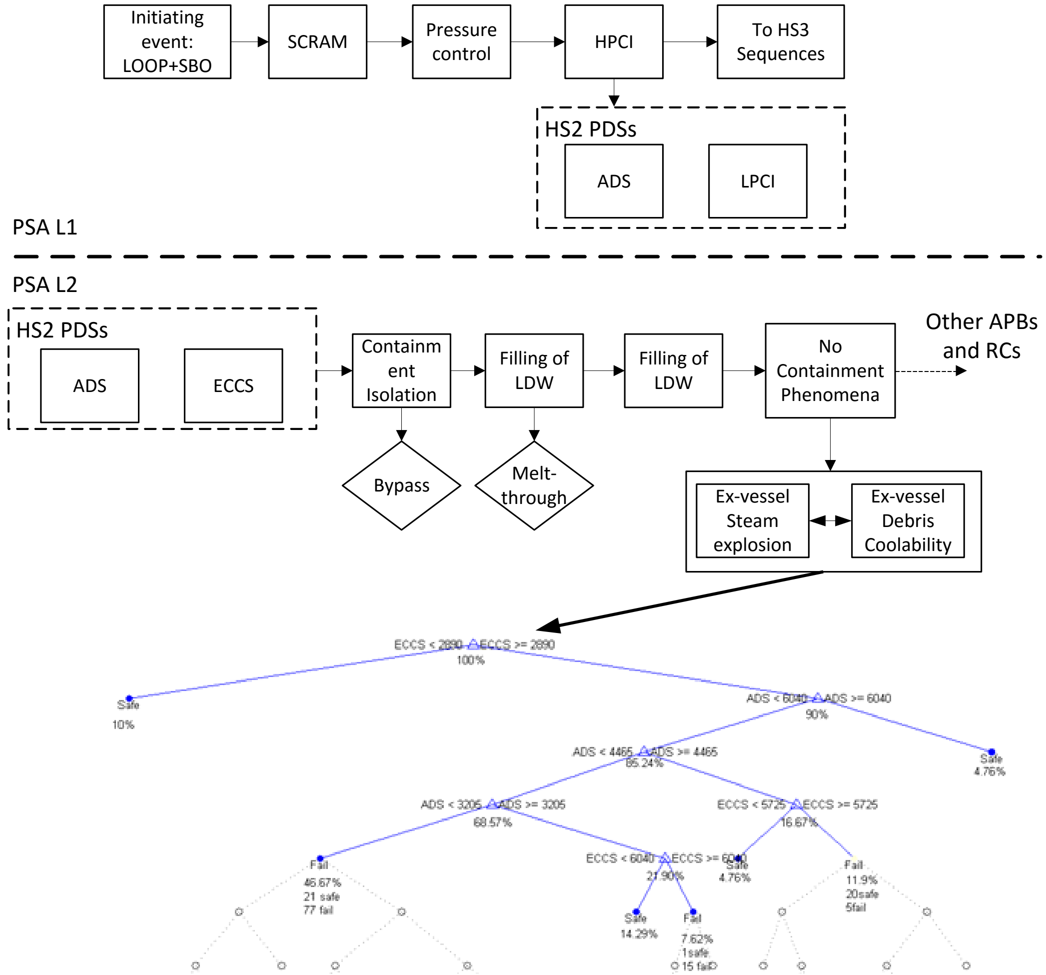

Figure 9. Joint application of PSA and IDPSA

The approach to run a lot of calculations to define the relevant scenarios could be compared to CFD calculations that are performed for example for explosion risk analysis within the oil and gas industry. Initially they performed a limited amount of deterministic explosion calculations and used that information to make judgements on all scenarios, but today the trend is surely towards using a very massive amount of CFD calculations.

V.C.1. Quantification and representation

Given that the information in the MCS list is available, and given that we have a decision tree capturing all relevant information, the quantification will not be a trivial task since there will need to be additional information required. Timing is a very important part, and also if one event in the MCS could be obsolete in some scenarios. Obsolete events should preferably, from PSA stand point, be represented separately in the PSA logic – and thereby be represented by separate MCSs.

To some extent the timing information could be considered being already part of the basic events, through the reliability model "mission time". This reliability model is represented by following formula:

$$Q(t) = q + (1 - q)\left(1 - e^{-\lambda Tm}\right) = 1 - (1 - q)e^{-\lambda Tm} \qquad (3)$$

Where:

- Q(t) is the failure probability of the component.
- q is mission time independent failure probability of the component.

- λ is failure rate, mission time dependent failure probability.
- Tm is the mission time.

This reliability model is used for most components in the PSA model, which has a mission time. However, this mission time is not referring to a specific time point, but rather specifying the time the component is required to operate. There is no way, in the PSA tool today, to specify an origo, for example, at the time core melt begins. In many cases the same events are used in the sequences prior to core damage, and hence they cannot be set zero in the PSA level 2. This issue needs to be resolved, for example by assuming that the mission time in PSA level 2 is in addition to the specified mission time (which would then be for PSA level 1).

Other type of events that could be affected by different timing is for example phenomena and operator actions that could be dependent on available response time. The type of data for the operator response would need to have some time dependent model, like THERP [28], or to have some other method for inclusion of such data. It could also be a very simple reliability model, in which you specify the failure probability for some time points. Example is given in the graph below.

Regarding phenomena and their likelihood; the idea would be to identify the type of scenarios that could result in a specific type of phenomena, and scenarios where the phenomena could be ruled out. Therefore, a first hypothesis could be to have a few probabilities for phenomena – and select the most representative on for each scenario.

A challenging part will be to identify which events that should be referred to as affected. The decision tree will be on a high level – but the results for the MCS are on a very detailed level. It should be reasonably easy to, for example, allocate basic events to systems. But, there are support systems that affect more than one front line system, for example diesels, and it will be a challenge to define the appropriate timing for these events.

Assuming that these data are available and that we have been able to connect all basic event with its relevant node in the decision tree so we could calculate the MCS conditional the decision tree, then it is likely that there may be several combinations of timing that may cause the MCS to occur. Some sort of convolution approach will then be needed to encompass all scenarios.

It should also be mentioned that how the quantification of the MCS list shall actually be performed is also a subject for research. Some possible methods could be:

- BBN (Bayesian belief networks [12]) - to be able to quantify events depending on other events.
- Automata [29], to be able to include states and time into the analysis.

ACKNOWLEDGMENTS

The work is supported by the Swedish Nuclear Radiation Protection Authority (SSM), Swedish Power Companies, Nordic Nuclear Safety Research (NKS), and Swiss Federal Nuclear Safety Inspectorate (ENSI) under the APRI-MSWI program at the Royal Institute of Technology (KTH), Stockholm, Sweden.

REFERENCES

1. International Atomic Enerfy Agency, *Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants*. 2010, Viena. (2010)
2. International Atomic Enerfy Agency, *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants*. 2010, Vienna. (2010)
3. *Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants*. IAEA Safety Standards Series No. SSG-4, STI/PUB/1443 (2010), ISBN 978–92–0–102210–3. (2010)
4. *Defining initiating events for purposes of probabilistic safety assessment*. 1993, IAEA, IAEA-TECDOC-719: Vienna, Austria. (1993)
5. *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*. 1990, U.S. Nuclear Regulatory Commission: Washington, DC 20555. (1990)
6. Kloos, M. and J. Peschke, *MCDET Approach for Considering Epistemic and Aleatory Uncertainties in Accident Simulations*, in *The 9th International Topical Meeting on Nuclear Thermal-Hydraulics, Operation and Safety (NUTHOS-9)*. 2012: Kaohsiung, Taiwan. (2012)
7. Chang, Y.H. and A. Mosleh, *Dynamic PRA using ADS with RELAP5 code as its thermal hydraulic module.* PSAM 4. Springer-Verlag, New York, 1998: p. pp. 2468–2473. (1998)
8. Guarro, S., A. Milici, and R. Mulvehill, *Extending the Dynamic Flowgraph Methodology (DFM) to Model Human Performance and Team Effects NUREGCR/6710*. 2001, US Nuclear Regulatory Commission, Washington, DC. (2001)
9. A. Hakobyan, et al., *Dynamic generation of accident progression event trees.* Nuclear Engineering and Design, 2008. 238(12): p. 3457–3467. (2008)

10. Izquierdo, J.M., et al., *Automatic generation of dynamic event trees: a tool for integrated safety assessment.* Reliability and Safety Assessment of Dynamic Process Systems, NATO ASI Series F, vol. 120. Springer-Verlag, Heidelberg, pp. 135–150., 1994. (1994)
11. Aldemir, T., *A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants.* Annals of Nuclear Energy, 2013. 52: p. 113-124. (2013)
12. Mitchell, T.M., *Machine Learning*. McGraw-Hill series in computer science. 1997, New York: McGraw-Hill. xvii, 414 p. (1997)
13. Y. Vorobyov and T.N. Dinh. *A Genetic Algorithm-Based Approach to Dynamic PRA Simulation*. in *ANS PSA 2008 Topical Meeting - Challenges to PSA during the nuclear renaissance*. 2008. Knoxville, Tennessee: American Nuclear Society, LaGrange Park, IL. (2008)
14. Fletcher, C.D. and R.R. Schultz, *RELAP5/MOD3 User Guidelines. NUREG/CR-5535*. 1992, US Nuclear Regulatory Commission, Washington, DC. (1992)
15. Gauntt, R.O., et al., *MELCOR Computer Code Manuals. NUREG/CR-6119/SAND 2005-5713*. 2005, US Nuclear Regulatory Commission, Washington, DC. (2005)
16. Tuffery, S.P., *Data mining and statistics for decision making*. Wiley series in computational statistics. 2011, Chichester, West Sussex ; Hoboken, NJ.: Wiley. xxiv, 689 p. (2011)
17. Ilango and V. Mohan, *A Survey of Grid Based Clustering Algorithms.* International Journal of Engineering Science and Technology, 2010. Vol. 2(8). (2010)
18. Sergey Galushin and Pavel Kudinov, “Scenario Grouping and Classification Methodology for Postprocessing of Data Generated by Integrated Deterministic-Probabilistic Safety Analysis” Science and Technology of Nuclear Installations Volume 2015 (2015)
19. VTT Research Report VTT-R-08589-12 Proceedings of the IDPSA-2012 Integrated Deterministic-Probabilistic Safety Analysis Workshop. November 2012. (2012)
20. T.G. Theofanous, “On Proper Formulation of Safety Goals and Assessment of Safety Margins for Rare and High-Consequence Hazards,” Reliability Engineering and System Safety, 54, pp.243-257, (1996)
21. T.G. Theofanous and T.-N. Dinh, “Integration of multiphase Science and Technology with Risk management In Nuclear Power reactors: Application of the Risk-Oriented Accident Analysis Methodology to the Economic, Simplified Boiling Water Reactor Design,” Multiphase Science and Technology, V20(2), pp.81-211, (2008)
22. P. Kudinov, S. Galushin, W. Villanueva, S. Yakush, D. Grishenko, Development of Risk Oriented Approach for Assessment of Severe Accident Management Effectiveness in Nordic BWR, PSAM12, June 2014, Hawaii, USA. (2014)
23. T.G. Theofanous and T.-N. Dinh, “Integration of multiphase Science and Technology with Risk management In Nuclear Power reactors: Application of the Risk-Oriented Accident Analysis Methodology to the Economic, Simplified Boiling Water Reactor Design,” Multiphase Science and Technology, V20(2), pp.81-211, (2008)
24. Apostolakis G., Cunningham M., Lui C., Pangburn G., Reckley W., “A Proposed Risk Management Regulatory Framework,” U.S. Nuclear Regulatory Commission, NUREG-2150, Washington, DC, April 2012. (2012)
25. Jolliffe I. T., Principal Component Analysis. 2nd ed. (2002), New York, NY, USA: Springer (2002)
26. Maimon, O.Z. and L. Rokach, Data mining and knowledge discovery handbook. (2005), New York, Springer. (2005).
27. Yakush S. E., Konovalenko A., Basso S., Kudinov P. “Effect of Particle Spreading on Coolability of Ex-Vessel Debris Bed,” 16th International Topical Meeting on Nuclear Reactor Thermal Hydraulics (NURETH-16), Chicago, USA, August 30-September 4, 2015, paper NURETH-16-14112, 13p, (2015).
28. Swain, A.D. & Guttmann, H.E., Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. 1983, NUREG/CR-1278, USNRC. (1983)
29. Hopcroft J.E., Motwani R., Ullman J.D., Introduction to Automata Theory, Languages, and Computation, 3rd edition. Addison-Wesley (2006)
30. Goronovski A., Villanueva W., Kudinov P., Tran C.-T. “Effect of Corium Non-Homogeneity on Nordic BWR Vessel Failure Mode and Timing,” Proceedings of ICAPP 2015, May 03-06, Nice, France, Paper 15160, 2015. (2015)
31. Goronovski, A., Villanueva, W., Tran, C.-T., and Kudinov, P., “The Effect of Internal Pressure and Debris Bed Thermal Properties on BWR Vessel Lower Head Failure and Timing,” 15th International Topical Meeting on Nuclear Reactor Thermal Hydraulics, NURETH 15, May 12 to 17, 2013, Pisa, Italy, Paper 500. (2013)
32. Yakush, S. E., Kudinov, P., Villanueva, W., and Basso, S., “In-Vessel Debris Bed Coolability and its Influence on the Vessel Failure,” 15th International Topical Meeting on Nuclear Reactor Thermal Hydraulics, NURETH 15, May 12 to 17, 2013, Pisa, Italy, Paper 464. (2013)
33. S. Galushin, P. Kudinov, “Core Degradation and Relocation Scenarios in a Nordic-type BWR” – Submitted to the Journal of Nuclear Engineering and Design. (2016).