Intégration des études probabiliste et déterministe de sûreté pour une prise en compte des risques dans la démonstration de sûreté de la conception de futurs réacteurs

Integrating probabilistic and deterministic safety analyses for risk-informed safety demonstration of future reactor design

YU Shizhen
Université libre de Bruxelles
Bruxelles
shizhen.yu@ulb.be

ZHANG Jinzhao
Tractebel ENGIE
Bruxelles
jinzhao.zhang@tractebel.engie.com

LABEAU Pierre-Etienne
Université libre de Bruxelles
Bruxelles
pierre.etienne.labeau@ulb.be

Résumé — Les analyses déterministes et les Études Probabilistes de Sûreté (EPS) sont réalisées pour les centrales nucléaires existantes afin de démontrer leurs marges de sûreté et/ou d'identifier des améliorations en matière de sûreté. Compte tenu de l'émergence de nouvelles et futures conceptions de réacteurs, notamment de Génération III+, de Génération IV et de Petits Réacteurs Modulaires (SMR), des approches innovantes peuvent être proposées pour mieux intégrer les EPS et les analyses déterministes pour la quantification de la marge de sûreté dans les analyses d'accidents de dimensionnement (DBA) et les analyses d'accidents hors dimensionnement (DEC), pour l'objectif d'optimiser la démonstration de sûreté au stade conceptuel. Concernant les analyses DBA, il est proposé d'incorporer les données sur la disponibilité des systèmes issues d'EPS et de s'inspirer des pratiques de fiabilité dynamique pour traiter les incertitudes liées à l'évolution dynamique d'un accident. Dans le cas des analyses DEC, il s'agit de fournir une méthodologie globale, guidée par les données et les résultats d'EPS, et qui couvre l'ensemble du processus d'analyse depuis la définition et la classification des scénarios, en passant par les analyses prenant en compte les incertitudes, jusqu'à la quantification des marges. La quantification et la démonstration des marges de sûreté ont été réalisées pour les deux types d'analyses, révélant également leurs différents objectifs tout au long des processus d'analyse.

Mots-clefs — étude probabiliste de sûreté, accident de dimensionnement, accident hors dimensionnement, meilleure estimation plus incertitude, fiabilité dynamique

Abstract — Deterministic Safety Analyses (DSA) and Probabilistic Safety Assessments (PSA) are performed for existing nuclear power plants to demonstrate safety margins and/or to identify safety improvements. In view of the emergence of new and future reactor designs, including Generation III+, Generation IV and Small Modular Reactors (SMR), innovative approaches can be proposed to better integrate PSA and DSA for safety margin quantification in both Design Basis Accident (DBA) analyses and Design Extension Condition (DEC) analyses, in order to optimize the safety demonstration at the conceptual stage. Regarding DBA analyses, it is proposed to incorporate insights on system availability from PSA, and to inspire from dynamic reliability practices to treat uncertainties related to the dynamic evolution of an accident. Whereas for DEC analyses, it is intended to provide a comprehensive methodology which is guided by PSA data and results, and which covers the entire analysis process from the definition and classification of scenarios, via analyses taking uncertainties into account, to the quantification of margins. The safety margin quantification and demonstration have been achieved for the two types of analyses, revealing as well their different focuses throughout the analysis processes.

Keywords — probabilistic safety assessment, design basis accident, design extension condition, best-estimate plus uncertainty, dynamic reliability

I. INTRODUCTION

Major concerns about climate change and the security of supply have brought nuclear energy back to its position of major contributor to the expected decarbonization of the energy mix. Innovative reactor designs are proposed, and their safety case needs to be made before moving forward towards their construction.

Nuclear safety demonstration, and more precisely safety margin quantification, was initially dominantly supported by Deterministic Safety Analyses (DSA), which consist of physical modeling simulations and analyses of scenarios being well defined a priori. In 1975, a pioneering Probabilistic Safety Assessment (PSA) was performed in (US NRC NUREG-75/014, 1975), and PSA emerged along time to complement DSAs. Consisting of event tree and fault tree analyses, PSA intends to provide an overview of all probable relevant risks in a Nuclear Power Plant (NPP) with a system (and if applicable in certain cases human) reliability mindset. At the DSA side, besides the conservative and Best Estimate Plus Uncertainty (BEPU) approach for the Design Basis Accident (DBA), a realistic approach with best-estimate computer code, realistic assumptions on system availability and initial and boundary conditions has been recently proposed for Design Extension Conditions (DEC) in (International Atomic Energy Agency, 2019). PSA can typically provide insights on system availability. Since the 90s, dynamic PSA has been developed and to a less extent applied, in order to include phenomenological modeling of system evolution together with its stochastic behavior in PSA, to consider possible dependencies between failure events (Aldemir, 2013).

In view of the emergence of new and future reactor designs, including Generation III+, Generation IV and Small Modular Reactors (SMR), innovative approaches can be proposed to better integrate PSA and DSA for safety margin quantification in both DBA analyses and DEC analyses, in order to optimize safety demonstration at the conceptual stage (Zio, 2014). Methodologies for DSA in general, and specifically for DEC analyses have been established with the intention to be risk-informed, and will be discussed in the current paper to reflect the findings and differences in their applications.

II. LITERATURE REVIEW

On the probabilistic side, deterministic analyses are typically used as supporting calculations in static PSA to determine the satisfaction of success criteria (Arkadov et al., 2012). Then as previously mentioned, dynamic PSA integrates phenomenological modeling of system evolution, thus deterministic calculations pending on possible trajectories as determined in dynamic PSA. However, dynamic PSA is much less applied than the static one in the nuclear industry mainly due to its complexity in development and the high computational costs (Aldemir, 2013).

On the deterministic side, the inclusion of probabilistic elements is attempted with the Extended BEPU (EBEPU) approach. EBEPU is an extension of the BEPU approach, which is currently widely applied in the nuclear industry for safety demonstration, and which considers uncertainties related to physical and modelling parameters, while making conservative assumptions on system availabilities (D’Auria, 2019; Martin & Petruzzi, 2021). EBEPU intends to incorporate insights from (static) PSA on possible/probable safety system configurations to DSA (Martorell et al., 2017; Queral et al., 2021).

The term of Integrated Deterministic and Probabilistic Safety Assessment (IDPSA) emerged, with various methodologies proposed to better integrate interactions among physical phenomena, system availabilities, control logics and operator actions, in order to further identify undiscovered vulnerabilities; however, challenges remain regarding computational efficiency and user-friendliness of IDPSA method and code application (Zio, 2014).

III. METHODOLOGY ESTABLISHMENT

A general methodology of IDPSA has been firstly established, which can be applied to any DSA, and typically to DBA analysis. It has been previously reported in (Yu et al., 2024a) in details, and is summarized in Sub-section A. Then it has been further developed to an extended methodology for DEC analysis in order to cover the entire DEC analysis process: scenario definition and categorization, assessment considering relevant uncertainties, margin quantification and improvement identification. This extended methodology has been described in (Yu et al., 2024b), and is summarized in Sub-section B. Both methodologies have the safety margin quantification as primary objective of application. These advanced approaches attempt to optimize safety demonstration of existing NPPs, as well as to demonstrate safety in an integrated fashion for future reactor designs.

A. *General IDPSA methodology*

The general methodology of IDPSA considers:

1) probable configurations of safety systems (based on EBEPU), which are related to aleatory uncertainties (e.g. demand failures, failure times, recovery time of equipment, etc.) in PSA models (Karanki et al., 2017);

2) physical/modelling parameters related uncertainties (based on BEPU), which can be both aleatory (e.g. initial and boundary conditions) and epistemic (e.g. physical model parameters) (Karanki et al., 2017);

3) accident dynamic evolutions related uncertainties, which are generally aleatory uncertainties (Karanki et al., 2017; Rahman et al., 2018);

4) uncertainty treatment in two loops with computing cost optimization, by deploying an inner loop for uncertainties related to accident dynamic evolutions (e.g. timing of operator action, actuation setpoint of safety system), and an outer loop for all other uncertainties. Indeed, rather than handling uncertainties based on their nature (aleatory or epistemic), it is intended to approach them by their impact on the accident evolution, which also helps to optimize the computational cost.

The steps of it are illustrated in Fig. 1. The various uncertainties are identified through Steps 3 to 5. Physical/modeling parameters in Step 3 are generally identified by a Phenomena Identification and Ranking Tables (PIRT) analysis. Safety system availabilities in Step 4 correspond to their configurations informed by PSA results, which are typically the number of available trains of a given system. Step 5 identifies uncertainties related to accident dynamic evolution, which correspond typically to timing of operator action and actuation setpoint of a safety system.

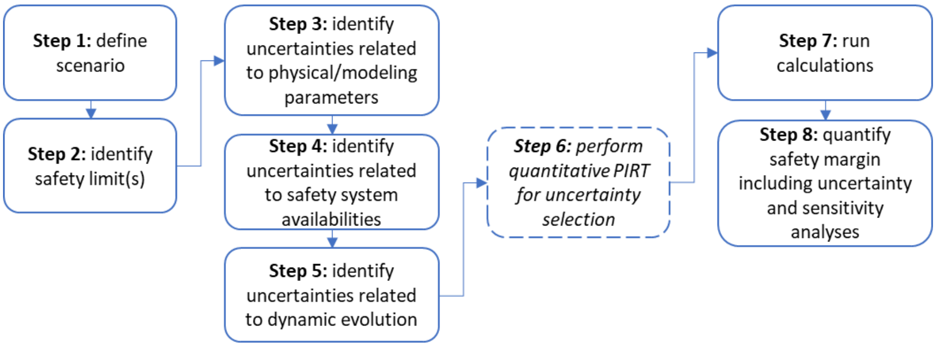

Fig. 1. General methodology of integrated deterministic and probabilistic safety analysis (Yu et al., 2024a)

An **optional** *Step 6* is proposed in case a selection among (a large number of) uncertainties is necessary, in order to identify the most sensitive ones for further analysis. It corresponds to a sensitivity analysis. The general computational scheme for Step 7 is illustrated in Fig. 2, with the uncertainties treated in two loops:

- An outer loop consisting of two dimensions:
    - a first dimension for physical/modeling parameters;
    - and a second for safety system availabilities;
- An inner loop for uncertainties linked to accident dynamic evolution.

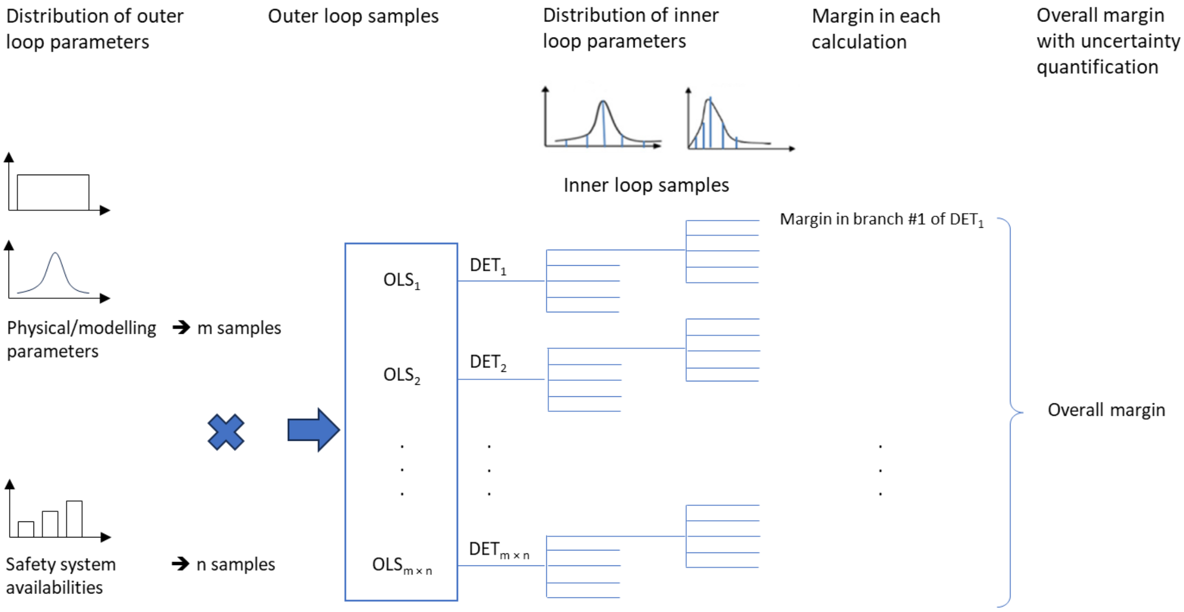

Fig. 2. Illustration of uncertainty treatment in two loops (Yu et al., 2024a)

In Step 8, different dimensions of the safety margin are quantified:

- *Margin of individual calculation* for each of the $N = \sum_{i=1}^{m\times n} B_i$ dynamic sequences (i.e. branches in Fig. 2):

$$m_j = \begin{cases} limit - load_j, & if\ load_j < limit \\ 0, & if\ load_j > limit \end{cases} \tag{1}$$

with $load_j$ the load in calculation j, and *limit* the safety limit.

- *Probabilistic safety margin* of the scenario:

$$p = \sum_{j=1}^{N} p_j\,, \qquad with\ \ p_j = \begin{cases} w_j, & if\ load_j < limit \\ 0, & if\ load_j > limit \end{cases} \tag{2}$$

and w_j being calculated based on the distributions of the various uncertainty parameters.

- *Probability-weighted margin* of no trespassing calculations in the accident scenario:

$$m = \frac{\sum_{j=1}^{N} m_j \times w_j}{p} \tag{3}$$

The *probabilistic safety margin* corresponds to the probability that a safety limit is respected; whereas the *probability-weighted margin* measures the distance of no trespassing calculations from the safety limit, ensuring the absence of cliff-edge effect (i.e. a slight increase in the load leads to a significant increase in the failure probability).

B. *Extended IDPSA methodology for DEC analysis*

The steps of the extended IDPSA methodology are illustrated in Fig. 3. It is a Level 1 PSA sequence-based approach. Each sequence corresponds to a sequence in the event tree of Level 1 PSA. As a consequence, Steps 1-8 (either through Steps 1, 2 and 3-8, or through Steps 1, 2, 3bis and 8) need to be repeated for each “main Core Damage (CD) sequence” in Step 1.1.

Indeed, Level 1 PSA CD sequences are the starting point of the analysis process. Main CD sequences are those with a significant frequency. For each of them, main Minimum Cut Sets (MCSs) are identified in Step 1.2, being either bounding regarding the consequences, or representative regarding the percentage of the sequence frequency the MCS covers. Thus one scenario equals to one MCS with its initiating event, initial and boundary conditions and available systems according to the PSA model, plus operator actions from procedures. Thus for each main CD sequence, one or a few scenarios (i.e. MCSs) are identified, and will be further analyzed.

Steps 2-5 and 6-7 are identical as Steps 2-5 and 7-8 respectively of the general methodology illustrated in Fig. 1. Step 3bis is introduced to simplify the process with only one bounding calculation per scenario in case a sufficient margin is deemed available based on engineering judgment a priori.

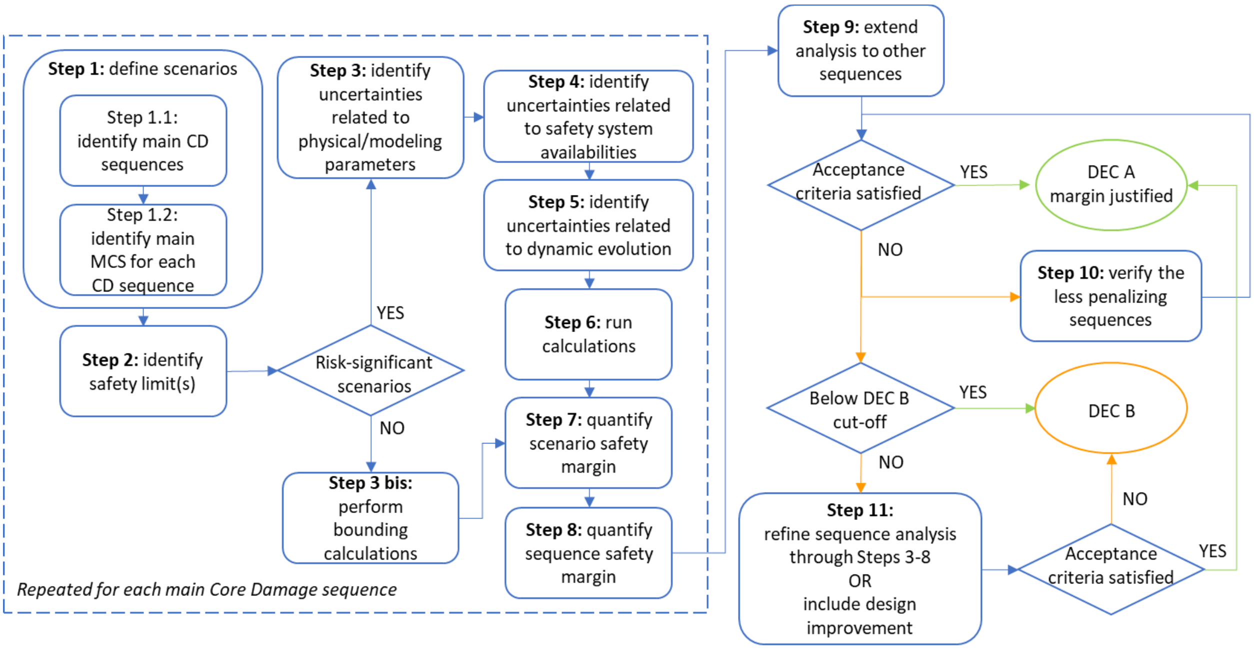

Fig. 3. Extended methodology of integrated deterministic and probabilistic safety analysis for DEC analysis (Yu et al., 2024b)

Step 8 intends to integrate scenario margins into sequence margins:

- *Probabilistic safety margin* of the sequence:

$$p_{sequence} = \sum_k p_k \times w_k \tag{4}$$

with w_k the probability weight of scenario k, calculated based on the proportion of the sequence covered by the MCS.

- *Probability-weighted margin* of the sequence:

$$m_{sequence} = \sum_k m_k \times w_k \tag{5}$$

Remark that the probabilistic safety margin p and the probability-weighted margin m of a given scenario described in Equations (2) and (3) are noted as p_k and m_k respectively in the extended IDPSA methodology for DEC analysis; as in one DEC sequence analysis, several scenarios are involved.

Step 9 allows to apply insights from main CD sequence analyses to other sequences with the same initiating event based on engineering judgment. The remaining steps of the methodology allow to categorize the sequences as DEC A (with limited core degradation) or DEC B sequences (with core melting).

IV. APPLICATION AND RESULTS

A. *General IDPSA methodology application on DBA analysis*

The general methodology has been applied to a DBA analysis case for a Gen-II Pressurized Water Reactor (PWR), concerning a 3 to 8" Small-Break Loss Of Coolant Accident (SBLOCA) (Yu et al., 2024a). A single failure of the Emergency Core Cooling System (ECCS) is assumed, meaning that 1 train of the safety injection system is lost for injecting into an intact loop. The Peak Cladding Temperature (PCT) of 1200°C has been chosen as safety limit.

A large number of physical/modeling parameters have been considered including the break size. Only the safety injection system availability (#47 in Fig. 5) has been selected as system uncertainty, with 3 probable configurations: 2 High Pressure Safety Injection (HPSI) trains available, 1 HPSI train available, and 2 Low Pressure Safety Injection (LPSI) trains available. Finally regarding dynamic evolution uncertainties, “RCP trip delay” and “AFW delay” (respectively #48 and 49 in Fig. 5) have been chosen based on a quantitative PIRT process.

Results in the existing conference paper (Yu et al., 2024a) are not all repeated here, only some main results illustrating the various margins described in Section III-A are given in Fig. 4 and TABLE I. Fig. 4 provides the probability and the maximum PCT calculated for each calculation, based on which the margin of individual calculation and the probability-weighted margin can be computed. The probabilistic safety margin equals to 1 as the safety limited is never exceeded in the performed calculations. Then TABLE I. provides the probability and the probability-weighted margin for each safety system configuration, and also the overall probability-weighted margin of all calculations.

Additionally, sensitivity analysis results of the final computations are provided in Fig. 5. Pearson and Spearman coefficients have been deployed, which measure sensitivity regarding respectively linearity and monotony.

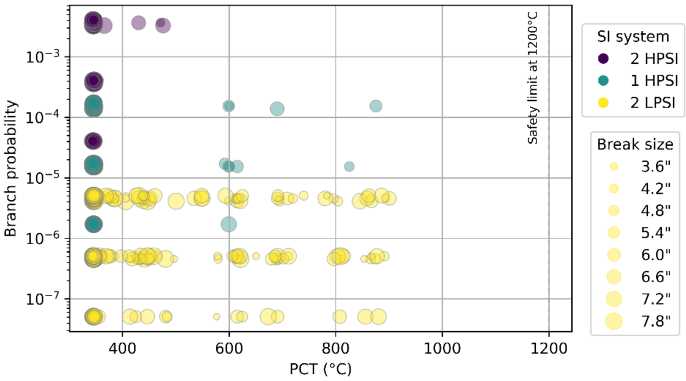

Fig. 4. Application of general IDPSA methodology on DBA – branch probability vs PCT

TABLE I. APPLICATION OF GENERAL IDPSA METHODOLOGY ON DBA – PROBABILITY-WEIGHTED MARGIN

Configuration	**Probability**	**Probability-weighted margin [K]**
2 HPSI	95.84%	853.0
1 HPSI	4.04%	848.6
2 LPSI	0.12%	800.5
All calculations	**100%**	**852.8**

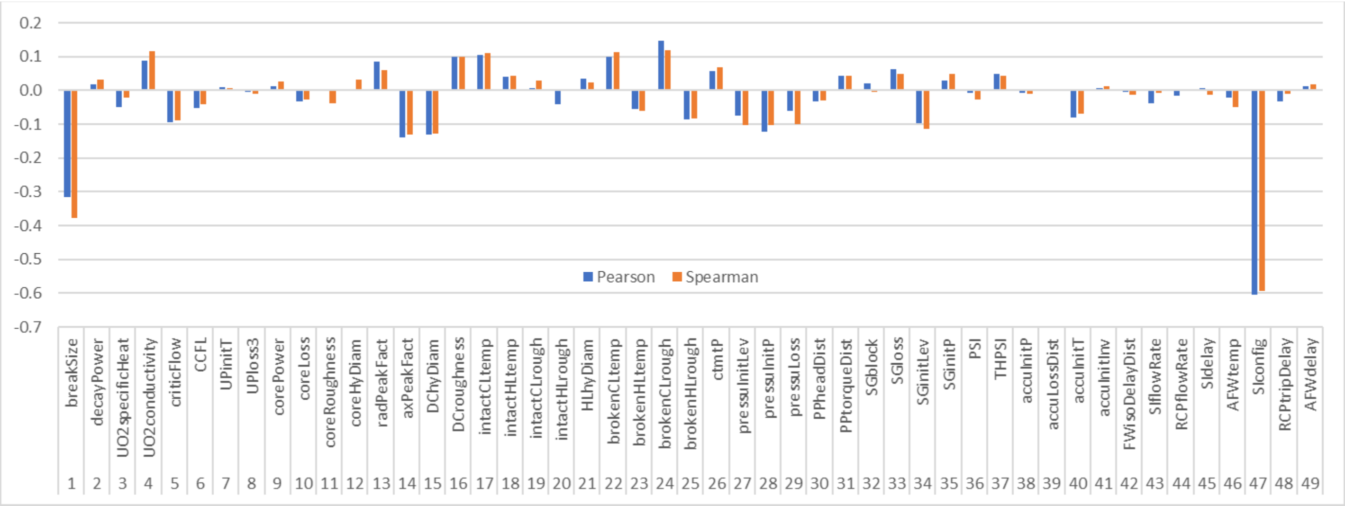

Fig. 5. Application of general IDPSA methodology on DBA – sensitivity analysis

B. *Extended IDPSA methodology application on DEC analysis*

The extended IDPSA methodology has been applied to a DEC analysis case for a Gen-II PWR, focusing on a SBLOCA CD sequence with failed safety injection system (noted as %AL1A-R:0028) (Yu et al., 2024b). Two scenarios being identified as main MCSs have been analyzed: MCS#1 with a break being a stuck-open Pressurizer Safety Valve (PSV), with an additional failure of all accumulators; and MCS#4 with a break ranging from 3/8 to 3”, also with a failure of all accumulators. Again, the PCT of 1200°C has been considered as safety limit.

A number of physical/modeling parameters have been taken into account. Regarding system availability, only the second level injection system (i.e. back-up safety injection system, noted as EA) has been considered (i.e. #40 in Fig. 7). Two complex operator actions have been treated as dynamic evolution uncertainties: the second level injection and the cool-down to shutdown operation by Steam Generators (SGs) (respectively #41 and 42 in Fig. 7). Indeed, the time needed to achieve these two actions are quite long (best-estimate values of 10 and 3 minutes respectively), and with higher uncertainties comparing to other actions considered in the scenarios.

Again, results in the existing paper (Yu et al., 2024b) are not all repeated here, only some main results illustrating the various margins described in Section III-B are given in Fig. 6 and TABLE I. Fig. 6 provides the probability and the maximum PCT calculated for each calculation, and for each scenario (or MCS). The probabilistic safety margin and the probability-weighted margin are then computed per scenario, and at the end for the sequence %AL1A-R:0028, as provided in TABLE I.

Additionally, sensitivity analysis results of the final computations are provided in Fig. 7, with Pearson and Spearman coefficients as measurements.

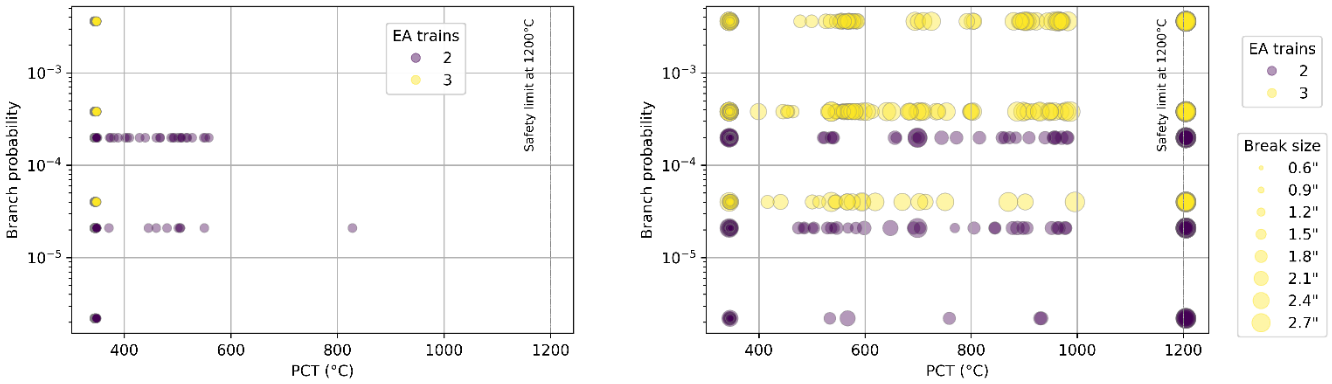

Fig. 6. Application of general IDPSA methodology on DBA – branch probability vs PCT (MCS#1 at left, MCS#4 at right)

TABLE II. MARGIN ASSESSMENT OF SEQUENCE %AL1A-R:0028

	Probabilistic safety margin	**Probability-weighted margin [K]**	**of %AL1A-R:0028**
MCS#1: PSV stuck open	0.9991	854	97%
MCS#4: break of 3/8-3"	0.7477	734	3%
Sequence %AL1A-R:0028	**0.9924**	**851**	**100%**

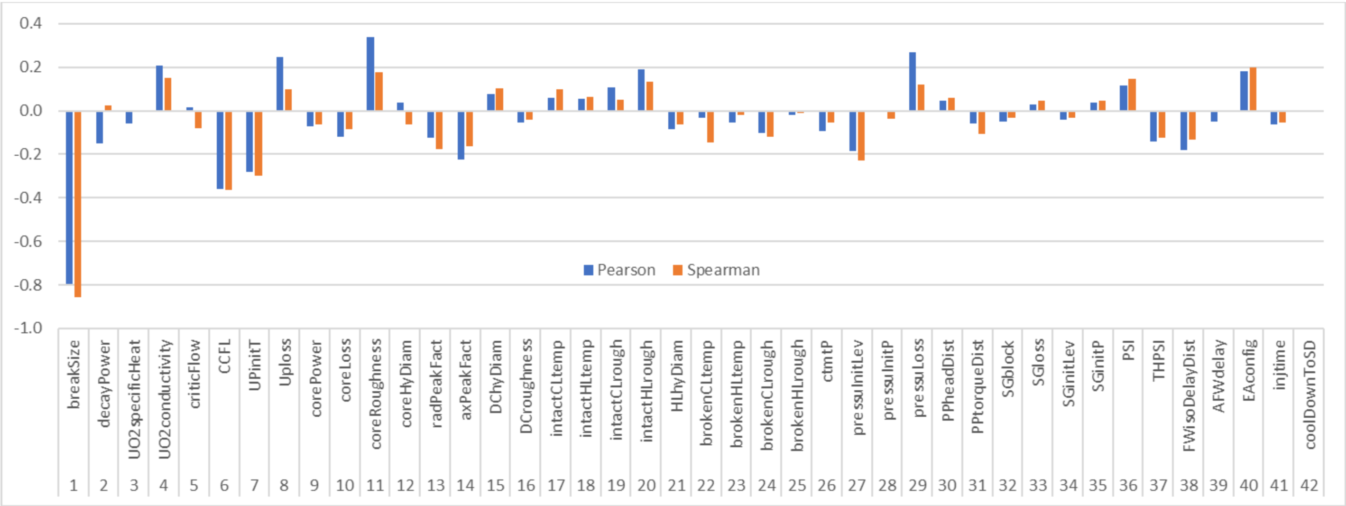

Fig. 7. Application of extended IDPSA methodology on DEC – sensitivity analysis for MCS#4

V. DISCUSSION AND PERSPECTIVES

Regarding the general methodology which can be applied to DBA analyses typically, besides the consideration of physical/modeling parameter uncertainties based on BEPU approach, it is proposed to incorporate insights on system availability from PSA, and to inspire from dynamic reliability practices to treat uncertainties related to the dynamic evolution of an accident. Whereas for the extended methodology for DEC analyses, it is intended to provide a comprehensive methodology which is guided by PSA data and results, and which covers the entire analysis process from the definition and classification of scenarios, via analyses taking uncertainties into account, to the quantification of margins.

Thus it can be understood that the backbone of the general IDPSA methodology is the deterministic approach (and more precisely the BEPU approach), and PSA inputs attempt to bring improvements to make the methodology more realistic regarding system availability and accident dynamics. As the primary objective of DSA, or more precisely DBA analysis, is to demonstrate safety by confirming significant margins, what is important is to consider a wide range of impacting uncertainties, to raise the confidence in the results. From the example provided in Section IV-A, it can be observed that safety system availability can be of significant sensitivity. However, as operator actions and system actuations are often well defined in DBA, with rather limited uncertainty, uncertainties related to dynamic evolution may not be of high importance.

Concerning the extended IDPSA methodology for DEC analysis, as previously mentioned, PSA inputs guide almost the entire process in its application. CD sequences are at the beginning of the process for scenario definition, frequencies are involved in scenario categorization, system availability and dynamic evolution are considered in analyses, and probabilities are deployed in margin quantification. It should be reminded that in DEC analysis, it is important to target risk-significant scenarios, and to propose improvements regarding nuclear safety. Best-estimate calculations are tolerated. Thus priority is given to uncertainties which are deemed as most impacting on results, which are typically those related to system availability, dynamic evolution (for instance operator actions with high uncertainty on the performances, system actuation and component failure that can change the course of the accident), and a few (i.e. a less number of, comparing to DBA analysis for instance) sensitive physical/modeling parameters. In the example provided in Section IV-0, the main intervening system which is the second level injection system is proved of significant sensitivity; and it was necessary to evaluate the operator actions related to the second level injection and the cool-down to shutdown operation by SG because of the uncertainties in the required time to perform them.

Finally regarding safety margin quantification, instead of a single conservative margin value in traditional DSAs, or a distribution of the load comparing to the safety limit typically in BEPU analyses, *probabilistic safety margin* and *probability-weighted margin* (of no trespassing calculations) have been further proposed. The combination of these two margin measurements allows to understand, in case the safety limit is exceeded in a number of simulations, the probability of respecting the safety limit (by the *probabilistic safety margin*), and the degree to which the no trespassing calculations conform to the safety limit (by the *probability-weighted margin*). These insights are especially relevant for situations in which the safety limit is exceeded only in a small proportion of the simulations, while significant margins are still present in no trespassing simulations. Additionally, the degree of safety limit exceedance can also be obtained for simulations not respecting the safety limit, which can be insightful if the safety limit is only limitedly exceeded.

VI. CONCLUSIONS

A general IDPSA methodology has been proposed, which can be applied to DSA, and typically to DBA analysis. Furthermore, an extended IDPSA methodology has been established for DEC analysis. *Probabilistic safety margin* and *probability-weighted margin* have been proposed as additional margin measurements. The way DSA and PSA are integrated differs in the development of these two methods: the general IDPSA methodology is DSA based, and incorporates PSA inputs to be more realistic regarding system availability and accident dynamics; whereas the extended IDPSA methodology for DEC analysis is guided throughout the entire process by PSA data. Nevertheless, both methodologies intends to be risk-informed, meaning that probabilistic insights are taken into account when assessing consequences in magnitude.

Regarding uncertainty consideration for different applications, it is observed that for DBA analysis, uncertainties related to physical/modeling parameters and system availabilities are of more importance; while for DEC analysis, focus should be firstly put on system availability and dynamic evolution related uncertainties.

ACKNOWLEDGMENT

The authors would like to acknowledge the following people for their support that allowed the realization of this work: Christophe Schneidesch, Michèle Auglaire, Simon Verdebout, Niels Palmans, Arnaud Blondeau and Robert Bouchier from Tractebel ENGIE, Younian Yu and Xinghan Lou.

REFERENCES

Aldemir, T. (2013). A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants. Annals of Nuclear Energy, 52, 113–124. https://doi.org/10.1016/j.anucene.2012.08.001

Arkadov, G. V., Getman, A. F., & Rodionov, A. N. (2012). Probabilistic Safety Assessment for Optimum Nuclear Power Plant Life Management (PLiM): Theory and Application of Reliability Analysis Methods for Major Power Plant Components. Woodhead.

D'Auria, F. (2019). Best Estimate Plus Uncertainty (BEPU): Status and perspectives. Nuclear Engineering and Design, 352, 110190. https://doi.org/10.1016/j.nucengdes.2019.110190

International Atomic Energy Agency. (2019). Deterministic Safety analysis for Nuclear Power Plants, Specific Safety Guide No. SSG-2 (Rev. 1). Specific Safety Guide No. SSG-2 (Rev. 1).

Karanki, D. R., Rahman, S., Dang, V. N., & Zerkak, O. (2017). Epistemic and aleatory uncertainties in integrated deterministic and probabilistic safety assessment: Tradeoff between accuracy and accident simulations. Reliability Engineering & System Safety, 162, 91–102. https://doi.org/10.1016/j.ress.2017.01.015

Martin, R. P., & Petruzzi, A. (2021). Progress in international best estimate plus uncertainty analysis methodologies. Nuclear Engineering and Design, 374, 111033. https://doi.org/10.1016/j.nucengdes.2020.111033

Martorell, S., Sánchez-Sáez, F., Villanueva, J. F., & Carlos, S. (2017). An extended BEPU approach integrating probabilistic assumptions on the availability of safety systems in deterministic safety analyses. Reliability Engineering & System Safety, 167, 474–483. https://doi.org/10.1016/j.ress.2017.06.020

Queral, C., Fernández-Cosials, K., Zugazagoitia, E., Paris, C., Magan, J., Mendizabal, R., & Posada, J. (2021). Application of Expanded Event Trees combined with uncertainty analysis methodologies. Reliability Engineering & System Safety, 205, 107246. https://doi.org/10.1016/j.ress.2020.107246

Rahman, S., Karanki, D. R., Epiney, A., Wicaksono, D., Zerkak, O., & Dang, V. N. (2018). Deterministic sampling for propagating epistemic and aleatory uncertainty in dynamic event tree analysis. Reliability Engineering & System Safety, 175, 62–78. https://doi.org/10.1016/j.ress.2018.03.009

US NRC NUREG-75/014. (1975). WASH-1400: Reactor safety study.

Yu, S., Zhang, J., & Labeau, P.-E. (2024a). Advanced Best-Estimate Plus Uncertainty Approach by Integrating Probabilistic and Deterministic Safety Assessments. Conference BEPU-2024, Lucca, Italy; paper 334.

Yu, S., Zhang, J., & Labeau, P.-E. (2024b). Safety Margin Quantification by Integrating Probabilistic and Deterministic Safety Assessments—Application to Design Extension Conditions. Nuclear Engineering and Design, submitted for publication, 113121.

Zio, E. (2014). Integrated deterministic and probabilistic safety assessment: Concepts, challenges, research directions. Nuclear Engineering and Design, 280, 413–419. https://doi.org/10.1016/j.nucengdes.2014.09.004