Risk Contextualization

Gueorgui Petkov[a]

[a] Kozloduy NPP, Kozloduy, Bulgaria, gipetkov@npp.bg

Abstract: Probabilistic safety assessment and management seeks to reach the standards of theoretical systematicity and empirical accuracy achieved in the models of natural sciences. To this end, a set of standards has been developed and improved in the form of statistically validated measures and probabilistic principles based on deterministic and probabilistic analysis. This set allows systematically derive potentially objective risk assessments and well-defined decisions. But it must also be borne in mind that much of the data and models are subjectively influenced by the uncertainty of the context in which they are obtained and linked. In other words, PSA in its current state contains a large amount of risk-related information, but without context of these models and results may not have really predictive and explanatory power and a common solid basis for comparative decisions. Therefore, thousands of sequences of events and transitions between the complex system states need to be monitored and analyzed by integrated code simulations with specific initial and boundary conditions of actual configurations to understand and predict risk. For the entire multi-unit nuclear power plant site, the cases become even more numerous and complex, as it is necessary to take into account not only the technological conditions, but also the whole context of the NPP site, including human, organizational and environmental factors to model an integrated system linking the facility and activity. A symptom-based context evaluation procedure could be used as a probabilistic tool for dynamic deterministic-probabilistic safety analyses interface in order to contextualize and supplement the existing risk metrics but not to replace them. The paper presents opportunities for the context quantification procedure of the Performance Evaluation of Teamwork method for risk contextualization, assessment and management on the multi-unit NPP site.

1. INTRODUCTION

The probabilistic approach uses a number of realistic assumptions, which include various uncertainties and should be addressed as explicitly as possible [1]. Probabilistic Safety Assessment (PSA) seeks to cover all contributors to risk of facility and activity system (FAS) operation in order to assess and understand its risk profile and to make the right risk-informed decisions. Its results serve to verify the compliance of risk assessments with the existing goals, criteria and safety requirements of the respective regulator [2].

The full-scale PSA model of a FAS, such as a nuclear power plant (NPP), must include all the various possible influences: 1) all internal and external initiating events (IE) and hazards caused by random failures, human actions (HA), natural and man-made phenomena for which an 'exhaustive but limited' list of initiators is drawn up, 2) general or specific reliability data of the equipment, 3) certain operating modes, states and conditions, 4) particular sources of hazards, and 5) distinct configurations of the installations located on the NPP site. All these elements of the model are most often extracted, modeled, evaluated and interpreted in different contexts for quantification with the same risk measures for different risk contributors. These differences in context must be taken into account, if possible unified, in order to understand and predict the risk and the thousands of sequences of events and transitions between complex system states that need to be monitored and analyzed through integrated code simulations with specific boundary conditions. and actual configurations. These sequences of events must be checked, grouped, and restricted to make the task practical for PSA purposes. The detailed

deterministic safety analyses (DSA) should be also reduced to a number of representative event sequences and identified bounding cases that have similar accident progressions to reduce uncertainty.

The stages of selection, modeling and evaluation of the data in the model imply subjectively typed situations and averaging the context of their implementation. But their interpretations for different configurations, reliability models and situations imply heterogeneity of scope, limited details and conservatism of initial and boundary conditions. Assuming an average homogeneous context of events in the process of risk modeling, assessing, aggregating and communicating can distort both the risk profile and risk-informed decision-making process. Increasing the elements for determining risk has its reasons, but it only increases the need to accumulate data, which is ultimately collected again through aggregating, context averaging and subjective expert judgment.
Therefore, the risk needs to be contextualized in order to give a more plausible secondary probabilistic dimension to the different configurations modes, conditions and situations in which the FAS operates due to the different risk contributors. This contextualization, or the study of the context for its homogenization, can be done in different ways. For example, by causal modeling of scenarios in thermo-hydraulic (TH) simulation specifying the significance of results according to given criteria or by quantification of context based on the occurrence and recognition of combinations of typical symptoms of the object in different situations. Symptoms are the deterministic characteristics of the object (FAS) in a given situation perceived by the subject (human) through images in his mind. Their scenario-sensitive combination in their run, simulating a risk contributor, allows for a deterministic-probabilistic modeling of context.

Risk contextualization is a process of combining *contextual factors and conditions* (CFCs or symptoms) to provide a probabilistic description of the FAS state, reduce uncertainty in risk assessment, and specify the exact risk profile for more reliable risk-informed decision-making. Following the dictionary definition of '*contextualization*,' it involves the placing the FAS in a context or in a situation within which they exist or happens. The purpose of this contextualization is to form a more accurate representation of risk, to contextualize and supplement the existing risk metrics but not to replace them. It is supporting risk characterization [3], information, understanding, communication and integrated risk-informed decision making (IRIDM) [4].

Most sources of uncertainty need to be defined in the context in which they are considered. This relationship is most obvious and can be derived from the human reliability assessment (HRA) [5], but it could be also applied to probabilistic modeling of scenarios, phenomena and dependencies [6], data mining [7], living PSA or dynamic risk monitoring (RM) [8], multi-unit PSA, risk aggregation [9], communication and management.

2. HRA CONTEXT FOR THE NPP SAFETY

2.1. HRA Development

The HRA is an applied hybrid science on the frontier between PSA, reliability and resilience analyses, human factor (HF), DSA, complex system simulation, cognitive systems engineering, psychometrics, psychology, ergonomics, neuroscience… HRA is trying to apply what is known from sciences to reflect interactions and interferences within the FAS, to assess a human error probability (HEP) of a human failure event (HFE), design, construct fault-tolerant, resilient interactions between human, organization, environment and technology. HRA is related to PSA that includes at least two quantities: severity of possible adverse consequence(s), probability of occurrence of each consequence and possibly casual scenario, utility, group of population…

The context is related to perception, understanding, control, safety and management of natural phenomena, processes and systems in which human participates. Therefore, the human resilience and HRA are most directly dependent on the context.

If we want to achieve better results for the NPP safety, we have to understand how work of humans is designed in the NPP context, how this work is imagined, monitored, controlled and done (or expected to be done) in situations of changing object and its image. An object is developed, perceived, inferred and managed by humans as its image (work tool) during the design, construction, commissioning, operation, decommissioning, etc.

The technique for human error-rate prediction (THERP) is a method used in the field of HRA, for the purposes of evaluating the HEP of a HFE occurring throughout the completion of a specific task [10]. THERP method gives the *"thesis"* or the aim of first-generation HRA methods: to obtain a HEP of identified HFE by reasoning and weighting of internal and external holistic performance shaping factors (PSFs). HA may be distinguished in two sequential stages – cognitive (diagnosis) and executive (manual or response). Dougherty comes up with the idea to change the first-generation HRA models such as THERP and human cognitive reliability (HCR) correlation [11] with the second-generation HRA models [12] because of the *"unfinished business related to HRA, which includes identification, specification and fitting of human cognition model to define the error potential and context"* of HA [13]. Hollnagel [14] notes that a detailed knowledge of HA's objective context and its subjective image that exists in the human mind is the basis for understanding HA in "second-by-second" dynamics. However, the temporal approach used in THERP, e.g. Swain's TRC or its 'improved' version called the HCR correlation [11] are *"virtually impervious to context"* [12].

The most of so called second-generation HRA methods made a formalistic substitution of the THERP's PSFs or their modifications with "contextual", "influencing" or "error-forcing" factors. But it did not substantially alter HRA's outcomes, because they also redefine the context by expert judgment (guessing the anchor value) and by multiplying the PSF (guessing the influencing factors). This substitution exemplifies the Dougherty's observation [12] and insight of that *"the influential and contextual approaches may find themselves indistinguishable at the quantification stage because of the paucity of actual data*." The aim of the new generation of HRA methods or *"antithesis"* is to take into account the context with its specificity, severity of consequences, multidimensional dynamics and holistics of FAS states for each individual or group cognitive and executive response.

Some of HRA concepts are indisputable; others are result of inertia in group thinking, misinterpretation, judgment heuristics, biases and business interests. To overcome the above challenges based on subjective identification, quantification, reduction, data-mining and measuring of HFE with expert judgment of PSFs and anchor values, a realistic symptom-based approach to describe of the FAS context was proposed [15].

HRA *"synthesis"* is to obtain a HEP of an identified HFE in the holistic and dynamic FAS context based on its specific symptoms' recognition for any individual and group cognitive or executive response. A symptom's impact is reasoned, measured and weighted by internal and external global and local *("glocal"*) *context factors and conditions* (CFCs) for it.

2.2. Approaches to the FAS Description, Modeling and Management

The following approaches could be identified and used to describe, model and manage the complex systems included facility and activity together:

- Person approach and system approach to modeling and managing HFE

The first approach focuses on *"the contribution of human errors on the system, their own psychological justification, accusations of forgetfulness, inattention, or moral weakness"* [16].

The second approach focuses on the conditions, situations and context in which a person deliberately and conscientiously performs his/her actions to effectively manage the system and limit the consequences of the risk of its operation. An extreme statement is *'human error is never the root cause.'* The system approach is preferable and practical for context-based HRA. It isn't important *"who blundered, but how & why the defences failed."* Human performance needs to be considered as a

variability of a whole system where human interacts with technology, other humans, organizations and environment (HFE ≡ FAS failure event).

- An approach to describing the FAS based on PSFs and an approach to describing the FAS variability of the system based on symptoms (CFCs) – Figure 1.

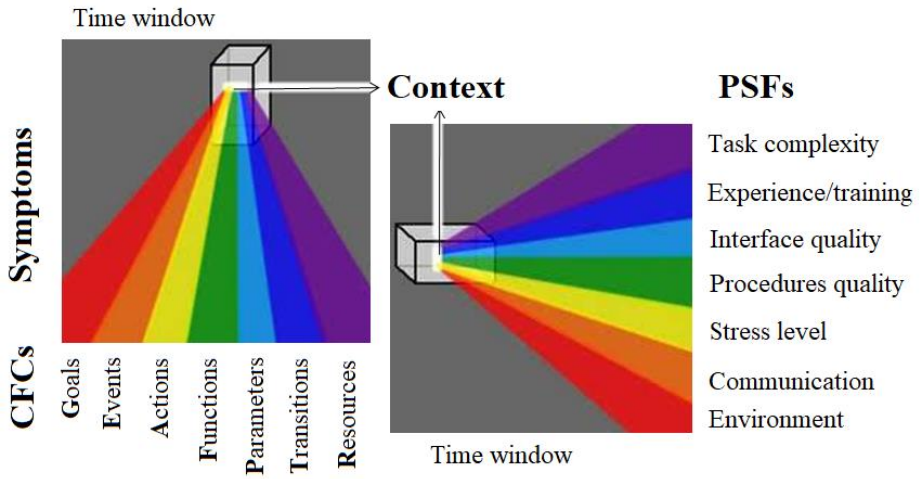

Figure 1: Psychologist's and engineer's points of view for the FAS context

The symptom-based approach is preferable and more practical for a comprehensive, contextual and dynamic description of FAS due to:

- extended application of the symptom-based approach to nuclear accident management

The symptom-based approach is usual in nuclear accident management. The IAEA NS-R-2 [17] establishes the following requirements on accident management: *"The training of operating personnel shall ensure their familiarity with the symptoms of accidents beyond the design basis and with the procedures for accident management."* Later in IAEA SRS No. 48 [18] *"symptom/state-based procedures"* were justified. In IAEA NS-G-2.15 [19] a *'symptom-based approach'* was also recommended: *"2.14. The approach in accident management should be based on directly measurable plant parameters or parameters derived from these by simple calculations."*

- possibility for statistical entropy description of macroscopic FAS in addition to the microscopic causal description

The dynamic interactions of the NPP are manifested by interference of symptoms (*stimuli with meaning for operator*). The FAS context could be presented by them on the macro level. If we want to understand the root causes of human errors, we should search in depth at micro level.

The holistic or macroscopic context qualification and quantification procedure is the first stage of a *Performance Evaluation of Teamwork* (*PET*) method that modeling most valuable FAS features in the accident progression obtained by PSA and DSA interaction [20]. It relies on combinations of recognizable symptoms for statistical description of the variability of FAS performance and gives controllable framework of mental processes as cognition and communication.

Macroscopic statistical description of the FAS context would help to identify the dynamic and holistic nature of the system's behavior. A certain macroscopic state can be found in many microscopic accessible states. The basic idea of the distinction between macro- and microscopic levels is to change the set of microscopic accessible states with equivalent subsets of macroscopic states (bit states). It follows the Shannon theorem [21] regarding the entropy as the measure of information, and was the basis for the used, in the PET method, an analogy of energy and information. The mental process in the FAS is described at each moment by its microstates (quantum states). A specific quantum state represents the most detailed possible FAS description.

- ability to solve theoretical questions about explored and unexplored mental processes [6],
- applicability for extending the definitions of images, errors, violations, holistics and dynamics of context [6],
- the PET procedure for evaluation of context, cognition, communication and decision-making error probabilities consists of eight steps and its iterative and recursive character in the spiral evaluation steps are also presented in [6].

2.3. Description of the Scenario Context Qualification and Quantification Process

Insufficient exchange of information between designers, safety analysts and technologists can lead to violated or unexpected context and inadequate risk assessment. If important symptoms of the description are omitted, then distortions in the context and risk assessment occur.

The timeline description and analysis of the accident scenario and tasks needs to be detailed and chronologized in order to improve the qualification and quantification process of the context probability (CP), error probability (EP), communication context probability (CCP) and HEP as shown on Figure 2 [5].

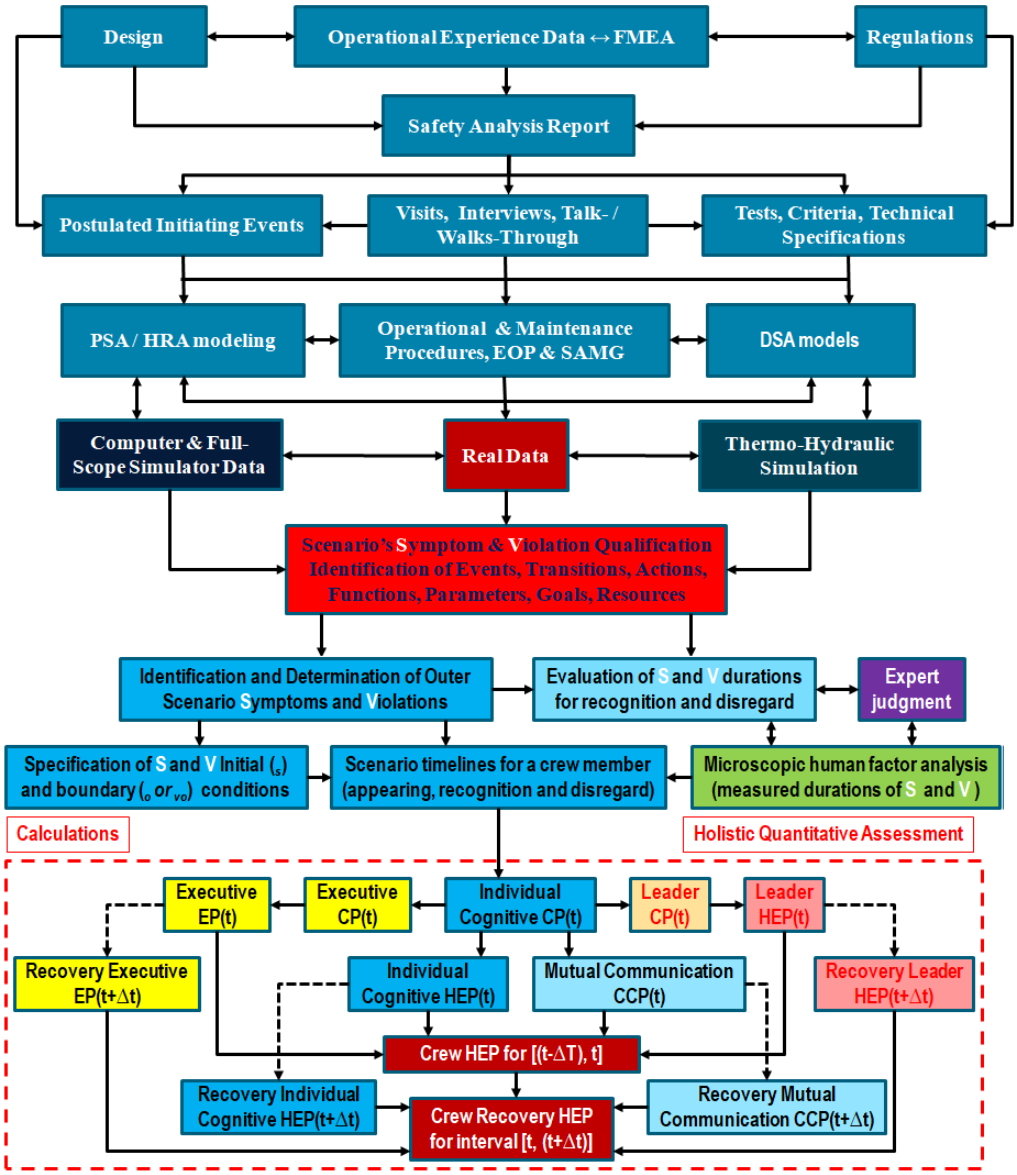

Figure 2: Scenario's timeline description for qualification and quantification of holistic dynamic context and human error probabilities

3. MULTI UNIT PSA CONTEXTUALIZATION AND RISK AGGREGATION

3.1. Multi-Unit PSA and Risk Aggregation Metrics

Single-unit and hazard PSA (SUPSA) for complex FAS as NPP is usually based on static logical structures event and fault tree (ET-FT) models of single reactor without or with its Spent Fuel Pools (SFPs). The DSA set of a NPP site most often includes modeling and simulation of the TH behaviors of single reactors and associated to them SFPs, and the operator responses to the accident scenario of internal and external events.

Following the Fukushima Daiichi disaster, special attention has been paid to multi-unit NPP sites, where a set of units, potential *"hazards, and combinations thereof"'*, impacts of inter-unit dependencies, shared systems and common resources on-site safety need to be addressed in PSA and DSA. This multi-unit PSA (MUPSA) considers the extended accident progression outside of the single reactor unit and requires explicit aggregation of risks of all potential on-site risk contributors.

The following expanded metrics of site risk are defined for a MUPSA with a frequency basis of events per site-year in [22] in frequency per site-year of an accident involving core damage frequency (CDF) or large early release frequency (LERF) on one or more reactors:

- Site CDF (SCDF) and Site LERF (SLERF)
- Multi-Unit CDF (MUCDF) and LERF (MULERF).

It should be borne in mind that the risk metrics must be scanned and selected without total optimism or total conservatism and to correspond to the occurrence of real severe accidents. The various outcomes can be depicted on a Venn diagram presented in Figure 3. It shows a comparative scope of SCDF for a Kozloduy NPP (KNPP, Bulgaria) site with two units (U) and two SFP. For the KNPP site with 4 sources, 2^4-1=15 disjunctive events need to be considered if all possible combinations need to be explicitly determined for calculating a site risk measure [22]. However, as shown in [9] for the three known major nuclear accidents (Three Mile Island, Chernobyl and Fukushima Daiichi), the IE outcomes depend on scenario context. The over- or underestimation of the multi-source risk profile in risk aggregation could be avoided not only by moderately complicating of the integrated PSA model [22], but also by taking into account probabilistic measure of IE scenario context, i.e., the contextualization of risk is a necessary.

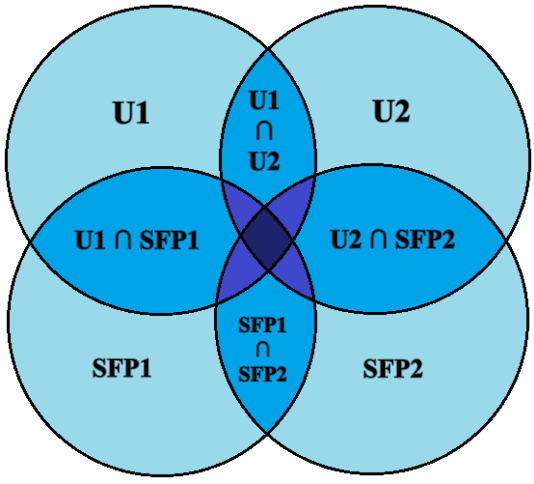

Figure 3: Venn diagram depicting accidents for Unit 5, Unit 6, SFP5 and SFP6 of KNPP

3.2. Contextual Challenges for Multi-Unit PSA and Risk Aggregation

All risk assessment tools look for dangerous relapses in the FAS dynamic holistic context. The main objective of the contextualization for MUPSA and risk aggregation on the NPP site is to take into

account all explicit and implicit dependencies between all units and hazards in order to minimize failures and risks, to increase the effectiveness of management and the practice to reduce the decision-making uncertainties. These uncertainties and dependencies are determined in a situation for which an explicit probabilistic description of risk, based on static SUPSA of any single-unit and hazard exists. This means that the MUPSA model should take into account the scenario's context and explicit aggregation of risks of as many facilities and hazards as possible at the NPP site: shared equipment, conditions, and organization; inadequate emergency procedures and guidelines (Emergency Operating Procedures – EOP; severe accident management guideline - SAMG); hazard-induced and common cause failures (CCFs), and HFEs during the scenario's progression.

In order to correctly interface deterministic models (DMs) with probabilistic models (PMs), and to use them jointly for contextual MUPSA and HRA there are three main challenges:

- How to convert the dynamic outputs of complex and time-consuming DM codes into PM input?
- How and by what software tools to represent the stochastic input in dynamic PSA or in contextual SUPSA or MUPSA models?
- How to take into account dependencies and reduce the transmitted and aggregated uncertainty from the DMs and PMs to the risk-informed outcomes and measures?

3.3. Suboptimal Safety Information Transfer

The DM codes give the best physical description of the NPP processes and they are the preferred tool for the PM input preparation. Unfortunately, the combinations and variations of the input parameters and the obtained results are too many and this makes DMs impractical to cover all possible conditions and situations (contexts). Therefore, ways are sought to summarize and reduce the inputs and outputs of DM for converting them to PM input for PSA by typing and grouping scenarios, simplifying models to reduce time and effort for modeling and calculation. An alternative option to such efforts is the probabilistic description and interpretation of the dynamic symptom-based context identifying the NPP events and processes for operators. This raises questions about how to optimize the interface and transfer of information between DSA and PSA in order to rationally use their capacity.

i) *DSA capacity* (C_{DSA}) includes:
   1. TH simulations of groups of postulated IEs (PIEs)
   2. Detailed dynamic TH models
   3. Basis for full-scope simulators with multi-step procedures
   4. FAS context can be modeled and defined much better than by expert judgment.

(ii) *PSA capacity* (C_{PSA}) includes:
   1. Limited set/list of PIEs
   2. Detailed static ET-FT models
   3. Powerful software tools
   4. Expertly judged HEPs for HFEs of the critical operator's actions or tasks.

DSA capacity for PSA ($C_{DSA\text{-}PSA}$) is used only to formulate the ET-FT success criteria where lists of PIEs and HFEs are used as the base set for TH analysis. The individual cognition, mutual communication and group decision-making processes of designers, experts and operators are not modeled in the DSA-PSA interface and consequently, the transfer *rate from DSA to PSA* ($R_{DSA\text{-}PSA}$) is small. Vast amount of DSA information about the FAS responses remains a side-product due to suboptimal transfer between DSA and PSA ($C_{DSA\text{-}PSA} >> R_{DSA\text{-}PSA}$). The optimal interface for an information transfer nearly without error requires $C_{DSA\text{-}PSA} \rightarrow R_{DSA\text{-}PSA}$.

3.4. Features of Dynamic MUPSA Options

The two options of summarizing and reducing DM inputs and outputs for turning them into PM inputs for PSA have their advantages and disadvantages.

In the first option, the *Risk Informed Safety Margin Characterization* (RISMC) is to produce *Reduced Order Models* (ROMs) of the TH codes (RELAP5-3D, MELCOR) [23]. ROMs need to replace TH simulations completely in order to reduce high computational costs (time and number of runs), and their results should be interfaced to the used tools for stochastic or probabilistic modeling and selected codes for system analysis (RAVEN) instead of classical Boolean structures such as ETs-FTs.

The second option is to quantify the dynamic CP(t), for operators, crews in main control rooms (MCRs), emergency or technical support centers, local zones of single units, hazards and site by the PET method [6]. CPs are used in parallel with the tree models for dynamic modulating of the PSA outcomes. The PET context quantification procedure relies on the change in time of the system macroscopic state and the counting of possible FAS accessible states.

This option for dynamic contextual MUPSA explicitly considers timing and sequencing of symptoms appearing for all units simultaneously in a PSA-HRA framework. There are no limits for operator's responses, outputs, technological or logical interface between DMs and PMs. Explicitness of this option give a clear idea of the possible decisions, prioritizations and accident mitigation measures to be taken.

The PET approach employs both DM and PM in a single analysis framework for HRA, PSA and accident analysis. In the DM set are included:

A. TH behavior of the NPP (reports, TH code or full-scope simulations),
B. External event study (such as flooding, tsunami, earthquake etc.) and
C. Operator responses to the accident based on operational manuals

DM of the NPP (A, B, C) is performed by using TH codes which simulate the FAS behavior evolution. Scenario's timeline could be traced by the counting of appearing, reported, recognized and disregarded symptoms and violations in time. Such symptom-based tracing of the holistic dynamic context (including physical, psychological, organizational, environmental factors) of FAS agents (individual operators and crews) on the NPP site. It is applied for qualification and quantification of their "situation awareness" in time and serves as a basis for dynamic contextual MUPSA, HRA and accident analysis.

The CP(t) could be evaluated as a potential for erroneous action, wrong decision-making, failed or unsuccessful FAS behavior. It is based on operational recognized concepts (symptoms) for control obtained from TH or full-scope simulations in the accident progression. A dynamic symptom-based context quantification procedure could be used as a tool for DSA-PSA interface. This procedure is a part of the PET method for HRA and accident management [20, 25].

Figure 4 shows the main features of the PET context vs. RISMC safety margin option.

4. CONTEXTUAL SITE PSA

4.1. Risk Metrics for Contextual Site PSA

The purpose of dynamic contextual MUPSA is to supplement, extend and modulate the existing risk metrics and not to replace them as [9]. The PET option uses standard SUPSA risk metrics (CDF& LERF). $CP_{ijk}(t)$ is calculated for each accident sequence (k), group of PIEs (j) and single reactor/hazard (i). It takes into account dependencies, uncertainty and ambiguity of statuses of units, hazards and teams. It would not lead to overestimating multi-unit risk metrics and excluding any damage that was not underestimated originally, e.g., context-free or average SUPSA outcomes. Eq. (1), can be used for a relationship between CDF (for SUPSA, upper S index) and SCDF (Site CDF, upper Site index) in MUPSA on NPP site:

$$SCDF(t) = \sum_{i=1}^{I} \sum_{j_i=1}^{J_i} \sum_{k_{ji}=1}^{K_{ji}} \int_{t_{ijk}}^{T_{ijk}} \frac{CP^{Site}(t) * CDF_{ijk}^{S}}{CP_{ijk}^{S}(t)} \quad (1)$$

where

Feature	RISMC	PET
System analysis	RAVEN	ET-FT
Event timing	Implicitly	Explicitly
Event sequencing	Implicitly	Explicitly
FAS responses	Limits	No limits
$C_{DSA\text{-}PSA} \geq R_{DSA\text{-}PSA}$	Reduced	Not reduced

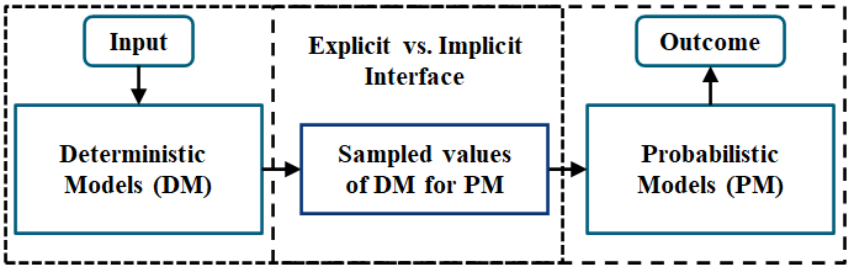

Figure 4: Advantages of contextual vs. safety margin option

- i is a number of single unit or hazard on the NPP site; I is total number of units/hazards;
- j_i is a number of PIE for i single unit or hazard; $j_i = 1...J_i$, J_i is total number of PIEs;
- k_{ji} is a number of sequence (scenario) of j PIE for i single unit/hazard; $k_{ji}=1...K_{ji}$; K_{ji} is total number of sequences for j PIE_i;
- t_{ijk} is initial time of the k_{ji} scenario; T_{ijk} is final time (steady state) of the k_{ji} scenario after core/fuel melt;
- $CP^{Site}(t)$ / $CP_{ijk}^{S}(t)$ is $CP(t)$ for the site and for k-scenario, j-PIE of the i-unit in Site PSA or SUPSA accordingly;
- CDF_{ijk}^{S} is a CDF for k-scenario, j-PIE of the i-unit in SUPSA;

The CDF evaluation by internal initiators is usually based on the analysis of $\approx 2 \times 10^1$ PIE groups and $\approx 10^3$ sequences leading to fuel damage. As a result of the quantification, about 10^4 minimal cut sets for CDF could be received. In emergencies, the 'sure choices' over 'choices that contain ambiguity' alternatives to specific sequences must be compared in risk analysis. This includes not just accounting for failures of the structures systems and components (SSC) but also needs to monitor the holistic context and take into account its impact on risk and "twofold inference" perception. The contextual Site PSA can be oriented both to a specific emergency sequence and general risk.

4.2. Example for a Contextual Site PSA

In a contextual Site PSA example below, the deterministic data for PM are extracted out of the State-of-the-Art Reactor Consequence Analyses (SOARCA) project of the US NRC (2013) where a TH model with MELCOR1.8.6 is used for simulation of the long-term station blackout (LTSBO) of the two-unit NPP "Surry" with Pressurized Water Reactor (PWR). The 'unmitigated' unit 1 (U1) and 'mitigated' unit 2 (U2) LTSBO timelines are based on the results of TH and accident analyses as described in [25].

A digraph decision-making model for two-unit NPP "Surry" site is shown in [9]. But only simple sub-graph (7 nodes) of this model is used for calculation of the $CP^{Site}(t)$ of the Emergency Operation Facility (EOF) team by $CP_i^{S}(t)$ of the MCR1 and MCR2 crews.

On the basis of Eq. (1), the following Eq. (2) for calculating the $SCDF(t)$ on the NPP site in time for contextual MUPSA of LTSBO sequences:

$$SCDF(t) = \sum_{i=1}^{I} \int_{t_i}^{T_i} \frac{CP^{Site}(t) * CDF_i^S(t)}{CP_i^S(t)} \quad (2)$$

Dynamic assessments of CP_i^S and CP^{Site} during the LTSBO for U1, U2 and NPP site are presented on Figure 5, for 24h (1440min). Figure 6 shows a comparison between dynamic curves of the relations between *SCDF(t)* and $SCDF_{static}$ (≈2x10^{-6}1/y) for 1440min (24h), obtained by the standard PSA level 1 model of the NPP "Surry" site, where: 'Digraph,' 'Av' and 'Site_U1_U2' are for a context with an 'mitigated' and a 'unmitigated' scenarios; 'U1_U1' and 'U2_U2' are for a context with two 'unmitigated' or 'mitigated' LTSBO scenarios accordingly.

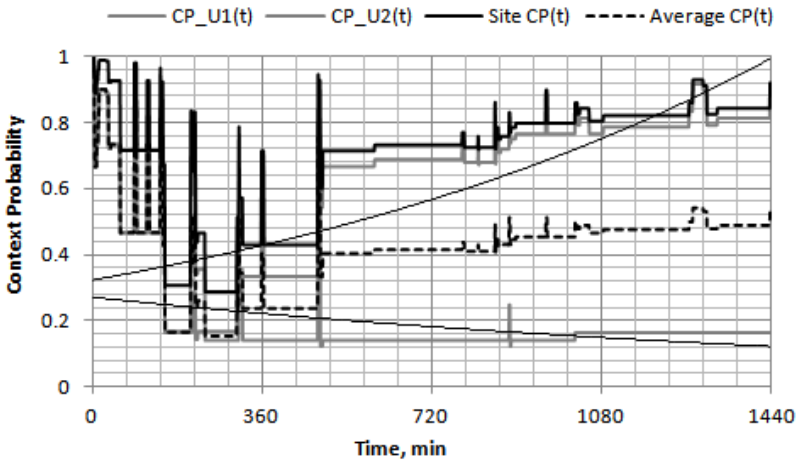

Figure 5: NPP 'Surry' LTSBO $CP_i(t)$ for U1, U2, average and site.

It can be seen from the Figure 6 that the difference between 'Digraph' and 'Site_U1_U2' models results is negligible. It means that there is no need to use the full PET model to calculate the cognitive error probability (CEP) of MCR crews and the CCPs for mutual communication between teams. It can be replaced by a simple reliability formula ($CP^{Site}=CP_1+CP_2-CP_1*CP_2$) to derive the approximate context of the NPP site (Site CP) from the aggregated contexts for the MCR_1 (CP_U1) and MCR2 (CP_U2). However, this is not advisable when there are detailed contexts for other local operators and teams [9], and as have been shown in the Fukushima Daiichi accident analysis or for the HRA using the PET method [25].

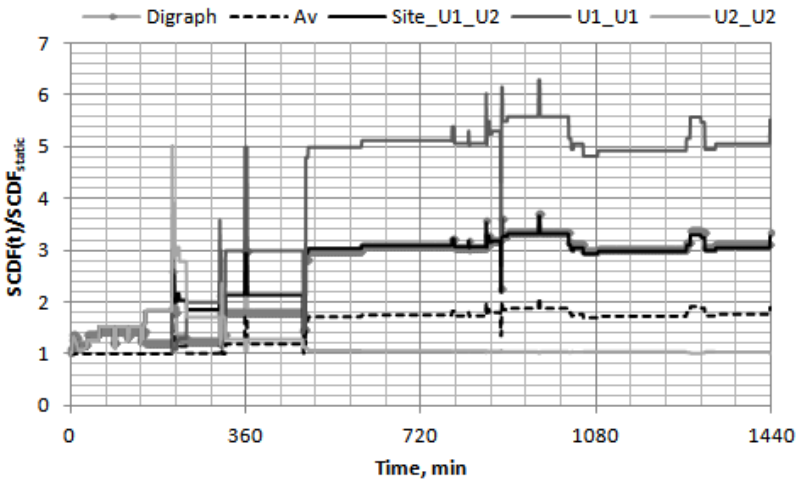

Figure 6: Contextual risk assessment for two-unit site NPP during PWR LTSBO

The use of dynamic context assessment with the PET method is useful not only for dynamic contextual Site PSA and weighing the severity of accident sequences, comparing and evaluating conservativeness of the PSA models, see [9], but also for reducing the uncertainty and ambiguity of outcomes for dynamic and static risks. For example, on the Figure 7 is shown the approximation of CDF(t) based on the LTSBO example without taking into account the standard risk monitoring inputs (SSC statuses, changes of alignments, configurations, modes and POSs).

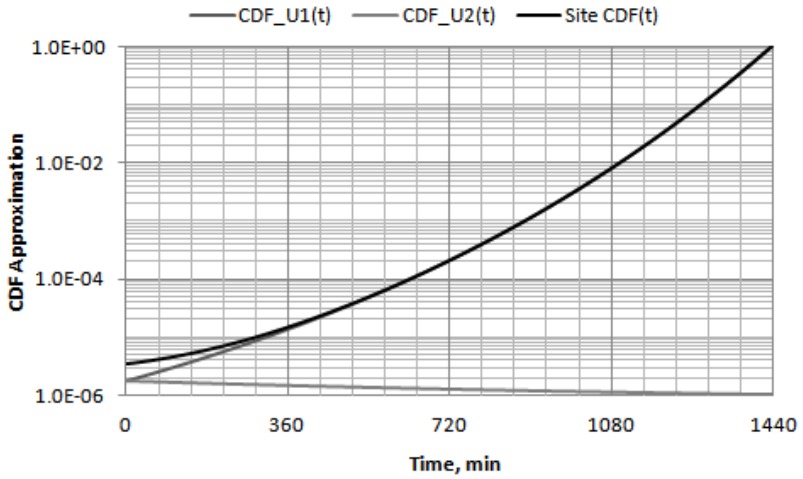

Figure 7: Contextual CDF approximation for the NPP with an 'unmitigated' and 'mitigated' unit during PWR LTSBO

4. CONCLUSION

Contextual Site PSA should be carried out in an integrated manner by including DSA and PSA aspects and taking into account the whole dynamic FAS context in accident progression.

Most hardware dependencies and technological interactions could be covered in the PSA model explicitly or by conditional probabilities and consequences. However, the crucial dependencies are not only related to the multi-facility site, they are also related to multi-activity structures and interactions between design, operation, regulation and organization, non-diversified design deficiencies, common infrastructure, emergency centers, etc.

The PET context quantification procedure for explicit and implicit modeling of dependencies and reducing uncertainty could be used as a valuable addition to the contextual Site PSA.

The need for detailed and dynamic determination of operator's performance context leads to the need of continuous monitoring and diagnostics. Development of a comprehensive system for risk monitoring, quantitative evaluation and management of operators' reliability based on their behavior and performance during full-scope simulator training is also one of the "hottest" areas in safety investigation of industrial accidents and incidents [20]. It forces a need to automatically data mining on the MCRs or simulators and helps reduce the use of experts to make judgments on the context effect.

References

[1] IAEA, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), IAEA, Vienna (2016).
[2] IAEA, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3, IAEA, Vienna (2010).
[3] NRC, Understanding Risk: Informing Decisions in a Democratic Society, Paul C. Stern and Harvey V. Fineberg, Editors; Committee on Risk Characterization, Washington, DC (1996).

[4] IAEA, Considerations on Performing Integrated Risk Informed Decision Making, IAEA-TECDOC-1909, IAEA, Vienna (2020).
[5] G. Petkov, Symptom-based Approach for Dynamic Human Reliability Assessment and Risk Management through Holistic Context Evaluation, IAEA-J4-TM-55244, Vienna, Austria, (2017).
[6] G. Petkov, *Symptom-based context quantification for dynamic accident analysis*, Safety Science Journal, https://doi.org/10.1016/j.ssci.2018.02.027, (2018).
[7] G. Petkov, PET generative data models for HRA data mining, Proc. of the ESREL 2019 Conference, Hannover, Germany**,** 22-26 September (2019).
[8] G. I. Petkov, Dynamic Contextual Risk Monitoring on the KNPP Site for Optimization of the Safety Systems Operation, Maintenance and Repair, IAEA-EVT1904091, Vienna (2020).
[9] G. Petkov, Dynamic contextual multi-unit HRA and PSA, IAEA-EVT1804903, Vienna (2019).
[10] A.D. Swain and H.E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, USNRC, (1983).
[11] G. W. Hannaman, A.J. Spurgin and Y.D. Lukic. *Human cognitive reliability model for PRA analysis*, NUS-4531, Electric Power Research Institute, Palo Alto, (1984).
[12] Ed Dougherty. *Human Reliability Analysis – Where Shoulds Thou Turn?* Reliability Engineering and System Safety, 29, 283-299, (1990).
[13] Ed Dougherty. *Context and Human Reliability Analysis*, Reliability Engineering and System Safety, 41, pp. 25-47, (1993).
[14] E. Hollnagel, *Human Reliability Analysis: Context and Control*, Academic press, London, 336p., (1993).
[15] G. Petkov and K. Furuta, *Application of PN-Based Method for Identification and Classification of Human Actions in NPP TLRS*, Proceedings of PSAM-IV, Springer London Ltd., Vol.2, pp.1136-1141, (1998).
[16] J. Reason, *Human error: models and management*. BMJ (Clinical research ed.) **320:**768–770, 2000.
[17] IAEA NS-R-2, *Safety of NPPs: Operation*, IAEA Safety Standards Series No. NS-R-2, IAEA, Vienna, (2000).
[18] IAEA Safety Reports Series No. 48. *Development and Review of Plant Specific Emergency Operating Procedures*, IAEA, Vienna, (2006).
[19] IAEA NS-G-2.15. *Severe Accident Management Programs for Nuclear Power Plants*, IAEA Safety Standards Series No. NS-G-2.15, IAEA, Vienna, (2009).
[20] G. Petkov, V. Todorov, V., Takov, T., Petrov, V., Vladimirov, V., Stoychev, K. and Chukov, I., , Safety Investigation of Team Performance in Accidents, *Journal of Hazardous Materials*, 111, 97-104, 2004.
[21] C. Shannon, *A mathematical theory of communication*. The Bell System Technical Journal 27, 379–423, 623–656, (1948).
[22] IAEA, Risk Aggregation for Nuclear Installations, IAEA-TECDOC-1983, IAEA, Vienna (2021).
[23] D. Mandelli, C. Parisi, A. Alfonsi, D. Maljovec, R. Boring, S. Ewing, S. Germain, C. Smith, C. Rabiti, and M. Rasmussen, *Multi-unit dynamic PRA*, Reliability Engineering and System Safety, 185, 303-317, (2019).
[24] G. Petkov, Symptom-Based Context Evaluation of Human Performance and Convergence of HEAP into Its HPLV. *Proceedings of the 25th ESREL Conference*, pp. 3083-3091. Taylor & Francis Group, London, UK, 2015.
[25] G. Petkov, and I. Petkov, Dynamic human performance context comparison for severe accident management during long term station blackout in light water reactors, *Proceedings of the ESREL2017 Conference*, Portoroz, June 18-22, 2017.