Challenges and Opportunities to Implement Advanced Probabilistic Safety Assessment (PSA) Approaches and Applications for Nuclear Power Plants

Brinkman, J. L. [a]; Jeon, H.[b]; Guigueno, Y. [c]; Hortal, J. [d]; Luis Hernandez, J. [e]; Mandelli, D. [f]; McLean R. [g]; Minibaev, R. [h]; Nitoi, M. [i]; Röwekamp, M. [j]; Schneider, R. [k]; Siu, N. [l]

[a] NRG, Arnhem, The Netherlands, brinkman@nrg.eu
[b] Korea Hydro & Nuclear Power, Daejeon, Korea, jeonhojun@khnp.co.kr
[c] IRSN, Fontenay-aux-Roses, France, yves.guigueno@irsn.fr
[d] Consultant, Madrid, Spain, jav.hortal@gmail.com
[e] International Atomic Energy Agency, Vienna, j.luis-hernandez@iaea.org
[f] Idaho National Laboratory, Idaho Falls, ID, USA, diego.mandelli@inl.gov
[g] Bruce Power, Toronto, ON, CANADA, rob.mclean@brucepower.com
[h] International Atomic Energy Agency, Vienna, r.minibaev@iaea.org
[i] RATEN ICN, Mioveni, Romania, mirela.nitoi@nuclear.ro
[j] Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, Germany, Marina.Roewekamp@grs.de
[k] Westinghouse Electric Corporation, Windsor, CT, USA, schneire@westinghouse.com
[l] Consultant, North Potomac, MD, USA, nosiubiz@gmail.com

Abstract: To build on the marked benefits of probabilistic safety assessment (PSA) in support of Integrated Risk-Informed Decision Making (IRIDM), IAEA Member States have been spending considerable efforts to improve PSA approaches and extend applications of existing approaches. In 2018, the IAEA started a project supported by USA extrabudgetary funds aiming to collect current experiences regarding these activities and to develop a related technical document that might support future updates of related IAEA Safety Guides on PSA. The PSA topics considered in the scope of this technical document are dynamic PSA, combination of hazards, use of non-permanent equipment, use of Level 2 PSA in support of the development of Severe Accident Management Guidelines (SAMG), Level 3 PSA, the incorporation of ageing aspects in the PSA model, and software reliability of digital instrumentation and control systems and modelling within PSA. This paper summarizes the challenges and the opportunities identified through the IAEA project. Despite the disparity of topics, a number of general lessons regarding technical, infrastructure, and decision support challenges are highlighted.

1. INTRODUCTION

Probabilistic safety assessment (PSA) has long been recognized as a powerful tool for nuclear power plant (NPP) safety. It has been used in practical applications to identify potential vulnerabilities in design and operation and associated risks. PSA spans over a wide range of areas in its scope of analysis to complement deterministic safety analysis approaches as highlighted by Requirement 15 of IAEA Safety Standards Series No. GSR Part 4 (Rev. 1) [1].

IAEA Safety Guides provide recommendations for the development and application of, respectively, Level 1 PSA [2] and Level 2 PSA [3], based on a consensus among Member States on the best practices related to "classic" or "traditional" PSA approaches (hereafter referred to as traditional PSA approaches). These IAEA Safety Guides are currently going through a review and update process to incorporate recommendations related to the development of PSA models for spent fuel pools, multi-unit NPPs, the use of non-permanent equipment, and hazards (internal and external) and their combinations.

It is well-recognized that PSA is potentially subject to a number of limitations, some methodological and some resource-driven. Ongoing work in several Member States is aimed at addressing these limitations to improve analysis realism, better characterize uncertainties, and better support Integrated

Risk-Informed Decision Making (IRIDM). Recognizing the considerable effort in these activities, and supported by extrabudgetary funds from the USA, the IAEA initiated a project in 2018 to identify challenges and opportunities in advanced PSA approaches and applications. The specific topics addressed by the project are:

- Dynamic PSA;
- Combinations of hazards;
- Modelling of non-permanent equipment;
- Use of Level 2 PSA in support of the development of Severe Accident Management Guidelines (SAMGs);
- Level 3 PSA;
- Software reliability of digital instrumentation and control systems and modelling within PSA;
- Incorporation of ageing aspects in PSA.

It can be seen that this list ranges from advanced approaches that are intended to address fundamental assumptions in traditional PSA but have not yet seen major IRIDM application, to topics that appear to be addressable using (at most) modest extensions of currently available approaches but for which modern IRIDM applications have been limited for various reasons.

The project team is in the process of finalizing a TECDOC, entitled "Advanced Probabilistic Safety Assessment (PSA) Approaches and Applications for Nuclear Power Plants," which will address the current experience of IAEA Member States with regard to the above topics. This paper provides a short description of one key aspect addressed by the TECDOC: the major opportunities and challenges for each of the selected advanced PSA topics.

2. ADVANCED APPROACHES IN PSA

2.1. Dynamic PSA

A formal, widely accepted definition of dynamic PSA does not exist, but the term suggests a combination of PSA and system dynamics methods. Such a combination may encompass significant advantages over the separate use of both types of disciplines for the purpose of safety assessment.

Current PSA methods are based on classical Boolean logic structures such as Event-Trees (ETs) and Fault-Trees (FTs). Although extremely useful, one potential drawback of traditional ET/FT based methods is that physical, temporal and spatial dependencies are only loosely considered. This becomes particularly relevant when dealing with complex accident sequences coupled with recovery actions and external events.

The key characteristic of dynamic PSA methods is the aim to explicit model system dynamics, i.e., the temporal evolution of the system elements (including components, subsystems, humans) and their interactions, all in the course of accident scenarios. One of the possible advantages of dynamic PSA is, that some dependencies among failure events that are not captured by traditional PSA can now be taken into account.

Not all traditional PSA methods or applications that address time considerations and dependencies in some fashion can be labelled as dynamic PSA. In general, the relevant timescale for interactions in dynamic PSA methods is that of the evolution of an accident, i.e. a time scale where characteristic time intervals can range from seconds to tens of hours. Consequently, a traditional PSA model that evolves in time, e.g. a risk monitor, is not considered a dynamic PSA.

Likewise, using deterministic system simulations as a support for the development of a traditional PSA model is not considered to be dynamic PSA. Contrary to the case of dynamic PSA, supporting simulations and probabilistic quantification are not performed simultaneously in traditional PSA.

Conclusions from supporting simulations in traditional PSA are mostly generic while interactions simulated in dynamic PSA are sequence specific and dependencies between dynamic and probabilistic aspects are modelled at the sequence level.

Practical PSAs often make some effort to incorporate analyst-recognized dynamic interactions in some fashion. However, the ET/FT approach is in fact a static Boolean logical structure and its capability to incorporate timing information is very limited. Definition of basic events can include specific time information (e.g. power recovery actions before x hours) or success criteria related to performance requirements on available time, but the basic difficulty to address system interactions in the timescale of the accident remains. Other situations, such as changes in the ordering of the events of a sequence or the repetition of a particular event (e.g. a safety valve cycling), may be even more difficult to address with ET/FT models and may lead to complex solutions that could easily become unpractical.

Dynamic approaches to PSA are intended to help to overcome these and other limitations of traditional methods, thereby providing increased realism of the analysis. They are also able to produce a significantly greater amount of potentially useful output information, including a better characterization of failure conditions that is not restricted to the PSA minimal cut sets. Additionally, each particular dynamic PSA methodology may provide specific results not available from traditional analyses. There are many other areas where dynamic approaches to PSA may provide additional advantages but, depending on the scope of the analysis, their usefulness may be higher or lower.

A non-exhaustive list of potential applications for dynamic PSA includes: (i) verification of model parameters and assumptions of traditional PSA, (ii) analysis of safety margins with regard to safety criteria upon significant plant changes, (iii) precursor analysis of actual events, (iv) assessment of Technical Specifications requirements not derived from deterministic analysis, such as surveillance requirements or completion times, and (v) technical support for emergency management.

Despite the benefits that dynamic PSA approaches might provide, there are still aspects where margin for improvement exists. One of the main challenges that dynamic methodologies has to face is efficiency, especially for full-scale applications. However, experience shows that while dynamic PSA methods have not been widely applied so far for industry applications, there have been a number of demonstrations of their capability to address specific issues where dynamic interactions play an essential role.

It is often said that dynamic PSA involves a high degree of complexity and indeed, conducting a dynamic PSA for all sequences on a full scope PSA model can be computationally unmanageable. However, as with any engineering analyses, carefully considered modelling simplifications to focus analysis resources on key issues can simplify the problem. Moreover, IRIDM applications can be of very different types and a dynamic analysis need not always be complex. Depending on the type of application, dynamic PSA analyses could be quite simple while maintaining important advantages of the dynamic approach.

An important challenge to the application of dynamic PSA in IRIDM is the lack of standards defining the required capabilities, tools, and acceptable analysis environments and scopes of dynamic PSA methods. There is a need to develop and implement adequate standards related to dynamic PSA methodologies but, at the same time, it is a difficult challenge due to the many aspects to be considered and the lack of experience in practical applications.

Another challenge involves the availability of data that is not required for traditional applications. At the same time, the potentially high amount of information that can be generated by a detailed dynamic PSA needs to be adequately managed in order to extract useful conclusions. Finding or generating new data sources and developing suitable data handling tools are important challenges for widespread application of dynamic PSA methods.

An additional challenge derived from the use of large simulation resources for detailed dynamic PSA is that most legacy system simulators can be susceptible to simulation crash or various numerical issues leading to long simulation times. Appropriate analysis needs to be performed to identify the causes of these problems. Careful employment of surrogate models can help address this challenge.

As a final remark, it can be said that although dynamic PSA is not so much an alternative to replace traditional PSA approaches, it is being increasingly viewed, in the authors' appreciation, as a complementary tool that can be used either to improve the quality of traditional PSA event trees and fault trees or to address specific types of problems for which traditional methods are not especially suited.

2.2. Combinations of Hazards

The recommendation in IAEA Safety Guides to consider individual hazards as well as combinations of hazards in the design, operation and safety assessment of NPPs is not new. They reflect the fact that combinations of hazards (so-called combined hazards) might have a stronger impact on plant safety than each single hazard on its own. Therefore, proper consideration of the risk resulting from combined hazards is important. The recommendation to ensure completeness of the list of site and plant specific hazards considered in traditional PSA also applies to the different types of hazard combinations (see [2] and [3]). Thus, the identification of hazards implies identifying all single and combined hazards that may be risk significant. The key question the PSA developer faces is the assessment and justification of scenarios based on combinations of hazards. In addition to the frequency uncertainty, there is also an uncertainty in the magnitude of the multi-dimensional impact (e.g. wind speed, duration of extreme heat, amount of snowfall, etc.). Combined as well as single hazards might cause impacts on NPP items important to safety that exceed the hazard recovery times or the resilience capacity of the plant with respect to water make-up, diesel fuel or human resources.

Event combinations of hazards to be assessed should include combinations of consequent (subsequent), correlated, and unrelated (independent) hazards (see Appendix I of IAEA Safety Standards Series No. SSG-64 [4]). The systematic consideration of combinations of hazards in traditional PSA implies proper identification of the combinations to be analysed, evaluation of their potential impact on the plant, assessment of their frequencies and incorporation in the traditional PSA model. To accomplish a comprehensive and systematic identification and screening of combined hazards, the entire single hazards list (natural and human induced external hazards as well as internal hazards representing a total of more than 120 single hazards) needs to undergo a systematic and well-founded hazard combination identification and screening process for the given site and plant under investigation. To obtain a consistent and efficient combined hazard analysis involves the use of the completed impact analysis (including the traditional PSA model) for single hazards or, at a minimum, of the results of the qualitative assessment of single hazards. The list of single hazards not screened out forms the basis for the identification and screening of hazard combinations. Observing current trends and developments in IAEA Member States, this process comprises the following typical tasks related to the identification of applicable single hazards: development of screening criteria; screening of single hazards; identification of potentially significant combined hazards; screening of combined hazards; and incorporation in the traditional PSA. More detailed information will be provided in the TECDOC that is being developed.

Given the relatively new development of combined hazard assessment there are several challenges and open issues in this area. One major challenge is to ensure that analysis resources are appropriately focused, e.g. to ensure that not too much time is spent in identifying and dismissing unimportant combinations. Another challenge is related to the national legislative framework, i.e. to what extent it is required to assess hazard combinations. The scope of assessment can vary significantly, depending on the methodological approach applied. A systematic and comprehensive screening approach with robust, well-defined criteria is key to ensuring an accurate representation of the risk from single as well as combined hazards, and a manageable and workable scope of the assessment. Methods need to be applicable to any NPP site in the world, for any set of potential hazards (including all hazards known so far) and for any reactor design. Where screening determines that a hazard is low risk, it needs to be

ensured that the cumulative screening of events does not mask significant removal of hazards from the risk profile. Quantitative screening criteria should be sufficiently low to ensure this.

Consideration of single as well as combined hazards requires oversight to ensure that multiple challenges to the internals of a plant are adequately modelled. The traditional PSA practice of only assuming one initiating event per event sequence is challenged here. It needs to be clarified if and how multiple occurrences of the same type of hazard are considered in the analysis. A typical example for such an event combination is a storm surge from a hurricane creating potential paths in a barrier island shielding an NPP, which is followed by a storm surge from a second hurricane that strikes the plant, which in this situation is less protected.

Due to the fact, that external hazards in general and combinations of external hazards in particular are rare events that can be practically excluded for several sites because of their climatic, topographic or geological conditions, the database regarding impacts from single or combined hazards is small. Moreover, the documentation for various natural hazards observed more than 200 years ago is insufficient.

2.3. Modelling of Non-Permanent Equipment

The Fukushima Daiichi NPP accident in 2011, caused by a sequence of natural hazards and consequent failures of safety functions, demonstrated the possible vulnerabilities of existing and planned NPPs. The location of some mitigating systems within the NPP itself resulted in their failure being caused by the natural hazards that challenged the plant. A strategy of providing non-permanent equipment geographically separate from the plant has been widely adopted as a means of mitigating this vulnerability.

The emergency mitigating strategies and equipment have been designed for initiating events and accident conditions, which typically include station blackout (SBO), the loss of the ultimate heat sink (LUHS) and severe external hazards, such as external flooding and major seismic events. Even so, the procedural guidance that was developed for using those strategies and equipment does not necessarily limit their use in other accident conditions. Therefore, depending on the feasibility of using those strategies and equipment, they can be modelled for mitigation of other initiating events and challenges.

The use of non-permanent equipment is an additional measure to ensure fuel integrity, in particular to protect fuel stored in the spent fuel pool (SFP) from melting and to mitigate severe accident progression in the reactor core. The effectiveness of these measures can be demonstrated by traditional PSA methods. Realistic modelling of such strategies and equipment improves understanding of the actual risk profile of the plant. Not only does it enable more accurate estimates of the as-built and as-operated risk metrics, it also improves the identification of potentially important scenarios. This is consistent with the concept of design extension conditions (DEC) introduced in IAEA Safety Standards Series No. SSR-2/1 (Rev. 1) [5].

The intended use of non-permanent equipment is expected to be documented, e.g. the connection points, procedures and sequence of connection. This enables analysis of non-permanent equipment using traditional PSA methods. However, there are several considerations to be made. Among the most notable issues identified by Member States:

(a) Lack of reliability data. Non-permanent equipment usually has its own reliability characteristics and classification as well as testing and maintenance intervals. Operating experience for non-permanent equipment is also not widely disseminated. The storage conditions of non-permanent equipment or related parts (e.g. flexible hoses) that are not considered in traditional PSA models, might affect their reliability or function. This issue can be resolved as plants gather specific experience and reliability data. Testing and maintenance programmes also have to be developed and properly reflected in PSA models.

(b) Human reliability analysis (HRA). In general, the HRA needs to identify and quantify human failure events that are not included in the original (before non-permanent equipment) PSA. These events may arise in a wide variety of scenarios with different plant and staff conditions, different time windows, different paces of events and levels of stress, etc. The analysis needs to consider the operating guidelines for the non-permanent equipment, the characteristics of the equipment and its deployment, and the possibility of insufficient procedures and training programmes as well as the effects of potential extreme environments on human performance. In addition to adjusting performance shaping factors (PSFs), the HRA likely needs to include a qualitative analysis defining subtasks for actions not addressed in the original PSA.
(c) Assessing the availability of non-permanent equipment against external hazards during deployment. Considering the relevant operating guidelines, the models needed to assess relevant site conditions, and the potential loss of function (possibly caused by damage to the site or damage to the equipment itself during deployment).

Previous considerations related to the modelling in PSA of the implementation of non-permanent equipment under external hazard conditions require a good understanding of the uncertainties associated with assumptions.

2.4. Use of Level 2 PSA in support of the development of SAMGs

Consideration of measures for the prevention and mitigation of severe accident phenomena started in the 1990's. These considerations addressed both the design for new NPPs and modifications for existing NPPs designed in accordance with earlier standards. Severe Accident Management Guidelines (SAMGs) were developed to provide guidance to operating personnel in mitigating and controlling any radioactive releases produced as a consequence of an accident.

Level 2 PSAs can be used to support the development of SAMGs, even if they do not provide the sole basis. As a systematic approach, Level 2 PSAs can (in principle) identify potentially important scenarios of severe accidents that might otherwise be missed. Ensuring the quality, scope and level of detail of Level 2 PSA can be seen as a crucial challenge for the use of Level 2 PSA for severe accident management assessment. Some technical features of a Level 2 PSA can be identified as a prerequisite for their use for SAMG assessment and may also be challenging, such as:

(a) Modelling of severe accident phenomena. In the development of a Level 2 PSA, the different phenomena associated with severe accident progression are identified and studied, including their uncertainties and the relation among the different phenomena.
(b) Modelling of severe accident management provisions and assessment of their impact (positive and negative) on the progression of the accident.
(c) Level of detail and accuracy of system modelling. In particular, for the instrumentation and control and safety features needed to cope with severe accidents, equipment survivability under severe accident environmental conditions (e.g. pressure, temperature, radiation) and the duration of such conditions and mission times have to be considered. To quantify the probability of systems failure, the correct mission time, depending on the accident sequence, is needed for mitigating systems, particularly for those which may need to be in operation for a long period of time.
(d) Human reliability analysis. A detailed treatment of human and organizational factors in Level 2 PSA is needed for the development of improved PSA-informed SAMGs. In particular, the treatment of decision making and execution under extremely difficult circumstances (e.g. plant damage, harsh environmental conditions, loss of permanent equipment, use of non-permanent equipment).
(e) Modelling of the containment function. In particular the identification of all scenarios leading to containment isolation failures, and the effects of pressure and thermal loadings on the containment performance (e.g. maximum allowable pressure and temperatures before the leak rate increase).
(f) Modelling of radioactive releases. To compare advantages and disadvantages of various options of SAMGs, it is important to characterize associated source terms and to assess radioactive releases

with adequate risk metrics that allow to take into account both short and long terms effects. From this point of view, traditional Level 2 PSA risk metrics (e.g. large (early) release frequency) might be insufficient, and identification of additional risk metrics or use of Level 3 PSA would be useful.

2.5. Level 3 PSA

Compared to the information from Level 1 PSA and Level 2 PSAs, the information obtained from Level 3 PSA allows for a better and far more complete assessment and characterisation of the off-site (public) risks attributable to a spectrum of possible accident scenarios involving an NPP. This is because Level 3 PSA directly assesses these risks, whereas Level 1 PSA and Level 2 PSA assess surrogates of the risk. However, unlike Level 1 and Level 2 PSA, which are widely developed and applied in many Member States, the development and use of Level 3 PSA is currently limited to a relatively small number of Member States due to several reasons, as described in Ref. [6]. Several of these reasons can be seen as challenges and open issues in the (necessary) development of Level 3 PSA to obtain a wider acceptance:

(a) Risk metrics for Level 3 PSA (health effects and economic). The choice of a suitable risk metric is in some cases driven by legal requirements or regulatory expectations. Also, non-radiological related risks, for instance fatalities or injuries caused by evacuation, could be considered. Exchanging experiences with organizations responsible for regulating other hazardous industries to gather information on the risk metrics used in those industries could give valuable insights. Connection could be sought with the recent IAEA initiative on 'methodology for aggregation of various risk contributors for nuclear facilities'[1].

(b) Uncertainties. The perceived large uncertainty of Level 3 PSA results seems to be an important factor in preventing its use. Reduction (or at least better characterization) of the uncertainties in the results of such analyses could be a way to overcome this. Sources of uncertainty/opportunities for improved realism are:
   (i) The present consequence assessment codes do not evaluate aquatic dispersion. This dispersion route cannot generally be neglected, especially when evaluating economic or environmental metrics. Developing tools (or borrowing tools from other disciplines) for modelling the dispersion in water (surface water, groundwater) would be worthwhile, as well as modelling and assessing the source term, resulting from severe accidents, which could be released to water sources.
   (ii) Correlation between the weather conditions used in the dispersion calculation and the initiating events leading to the source term. This would necessitate a coupling between the Level 2 and Level 3 PSA results (directly or via pre-processing). A further correlation could be explored between the initiating event and/or the weather conditions on, for instance, evacuation possibilities, e.g. external hazards that damaged the plant can also damage the necessary infrastructure outside the plant.
   (iii) Treatment of concurrent and time shifted radiological releases from multiple radiological sources located at the same site.
   (iv) Selection of atmospheric transport and dispersion (ATD) model considering the impact of temporal and spatial variability.
   (v) The set of radionuclides used to characterize the off-site consequences.

(c) Low dose issues. All computer codes use a dose response model based on the linear no-threshold (LNT) hypothesis. Dose response models have been primarily developed to support the system of radiation protection, in which the precautionary principle leads to the use of LNT. However, it is not considered appropriate to use the LNT hypothesis to estimate numbers of radiation-induced health effects within a population exposed to low doses (i.e. to multiply low doses by large numbers of individuals) [8]. One possible way forward in terms of the application of Level 3 PSA would be to evaluate the impact of different assumptions about the health effects associated with exposures to low doses.

[1] https://www.iaea.org/topics/design-safety-nuclear-power-plants/risk-contributors-methodology

(d) Health effects caused by psychological stress created by the accident are presently not treated in Level 3 PSA but can in principle be included. For low doses the psychological effects may dominate over the radiological effects. Qualitatively, a sufficient conservative dose–effect relationship for low doses could cover this. However, there is little numerical data, and no consensus on how to address this quantitatively.
(e) Level 3 PSA communication. Communication of PSA results is a challenge for PSA as a whole and is not limited to Level 3 alone. It is to a large extent caused by the (public) perception of probability and risk. The public tries to understand radiation as it relates to their everyday life. Technical experts rely on formal risk tools. This leads to a mismatch between how specific authorities and the general public approach risk, which in turn can lead to many misunderstandings.

Regarding the potential benefits, the use of more detailed models in Level 3 PSA contributes to:

(a) Justifiable treatment of features (topography, unusual weather conditions) that challenge Gaussian plumes;
(b) Non-averaging treatment of situations involving threshold effects (e.g. early fatalities, mitigation in accordance with protective action guidelines);
(c) Consistency with state-of-the-art science (improves PSA user confidence).

2.6. Software reliability of digital instrumentation and control systems

Digital instrumentation and control (DI&C) systems, e.g. computer-based I&C systems are important for NPP safety. The reliability of such systems is determined by the reliability of two main components of the system: hardware and software. IAEA Safety Standards Series No. SSG-3 [2] recommends that in PSA the reliability of "both hardware and software components" be considered. Nevertheless, this separation is already a simplification, which is justified by the complexity of analysing the reliability of digital systems. The real reliability of a digital system is the totality of the reliability of software that runs on specific hardware. Although there is no consensus on the quantification of software reliability, there is consensus on several philosophical aspects of software failures and the general appropriateness of the use of probabilistic models in modelling those failures. At a high level, the areas of consensus are that software can fail and the occurrence of software failures can be treated stochastically. Thus, software failure rates and probabilities may be included in the reliability model of the digital system.

Despite the complexity of digital systems analysis, the results that can be obtained can improve the understanding of the safety/risk impacts of digital control systems. The main advantage, despite the possible simplifications in modelling, is a more realistic risk profile that displays the weakest or most sensitive places in the structure of the digital system, supporting an improved understanding of the safety of the NPP as a whole.

In comparison to the reliability of hardware, which can be assessed by traditional PSA methods, the treatment of software reliability needs other approaches to perform a quantitative assessment. There are a large number of methods (including combinations of methods) for assessing the reliability of software and the reliability of a digital system as a whole. The TECDOC being developed provides a description of the following four major categories of quantitative software reliability methods: software reliability growth methods (SRGMs); Bayesian belief network (BBN) methods; test-based methods; and other methods, such as correlation approach methods, metrics-based methods and context-based software risk model (CSRM) methods.

The methods mentioned above are separately developed techniques that use non-probabilistic approaches for analysis, but the results can be integrated into PSA. However, several international organizations have been pursuing activities to review and improve methodologies for estimating software failure rates for digital systems for use in PSA e.g. the OECD/NEA/CSNI WGRISK DIGREL project [9], the NKS MODIG project [10], and the Euratom HARMONICS programme [11]. The DIGREL project investigated software reliability quantification building upon taxonomy concepts

identified in Ref. [9]. The taxonomy is based on a failure propagation model and a five-level hierarchical abstraction of the DI&C system: system level, division level, I&C unit level, I&C unit module, and basic component level. The overall objective of DIGREL was to provide guidelines to analyse and model digital systems in a PSA context, using traditional reliability analysis methods (failure mode and effects analysis, fault tree analysis).

Considerable advancements have been made in establishing a taxonomy and a process for evaluating DI&C systems within the structure of PSA for NPPs. While the framework is becoming firmer, there remain issues to resolve and a need to continue collecting reliable data for quantifying software failure rates and appropriate common cause coupling factors for the various DI&C systems used in NPPs. The current challenges that have been identified are the following:

(a) The lack of availability of quality data on failure counts and detailed failure characteristics limits the ability to better define the digital I&C model. The ability to quantify software failures depends on the number of observed failures and the operating time. As a result of verification and validation requirements placed on safety critical software, recent experience with the reactor protection system and the TELEPERM® XS (TXS) platform developed at AREVA indicate that software failures are rare [12]. Furthermore, common cause software failures are difficult to identify and quantify.
Latent software faults will not change over time unless explicitly fixed. The reliability of software generally improves as these errors/faults are identified and removed. However, software upgrades might unintentionally introduce new failure modes. At this point, it is not clear how software fixes are integrated into demand failure probability estimates. In particular, if a system is put in service after an upgrade and a failure occurs shortly after, is that failure attributed to the unit failure or an implementation failure during the break-in period[2]? No mechanism for collecting and recording this failure data in a consistent and comprehensive manner currently exists.
The common cause failure potential is important, as common cause failures might lead to complete system failure. Without observation of such failures for NPP systems (or in other applications outside nuclear industry) and knowing they are rare, software quantification is based largely on models that use limited data and engineering judgement based on the quality processes used to develop and implement the software.
Improvements to data collection and clear data reporting may help better resolve these issues in the future. For demand systems that traditionally get few demands, such as the reactor protection system and the actuation systems for engineered safety features, there may be a benefit in testing a parallel system in a laboratory for an extended period of time. The tests need to consider a wide spectrum of simulated demand signals with randomly injected conditions including random introduction of noise (based on potential instrument behaviours) and varying coincident intervals on a near continual basis until sufficient, approximately 1 million to 10 million, demands are generated. The injected signal could vary based on magnitude, duration (with reasonable limits) and temporal relationship. The goal would be to cover the operational space with a ‘noisy’ signal. For certain systems it is important to understand operability challenges to environmental conditions prior to installation. It is necessary to understand how and when systems would behave/fail when subjected to excessive temperatures, humidity, smoke, vibration etc.

(b) Human machine interface (HMI). DI&C systems generally require interaction with operating personnel, especially during extreme off-normal situations. PSA modelling of such situations needs to consider which type of human actions might occur and model those actions accordingly. In broad terms, this analysis is amenable to existing PSA approaches, considering both software and human reliability. However, incorrect HMI operation (including indication failure) can lead to operator error as well as an overall increase in staff stress levels. When performing an analysis, the lack of data, detailed methods for evaluation, and associated standards might pose a major challenge. Note that for DI&C systems, the human actions requiring analysis might also include recovery and repair actions. Currently, there is no uniform treatment for assessing these actions (including the time required for these actions).

[2] Period allowing the gradual conditioning of new equipment to the operating conditions.

(c) Modelling of dynamic processes. The need for detailed time dependent models to track data arrival/congestion has not been fully resolved [13]. Models consistent with PSA fault tree analysis techniques have been demonstrated, but these models do not explicitly treat temporally-induced system failures [14]. Thus, some potentially important failure might not be correctly represented in a fault tree model. The use of fault tree models can be better supported with comparisons to focused example calculations using Markov-like processes for realistic systems. However, the main issue underlying the resolution of this challenge might be the limitation in detailed data. Simulator models can provide valuable data to assess system/component performances for a large combination of failure modes. Dynamic PSA methods (see above) can model system dynamics and digital I&C failures; a challenge here is how the results can be integrated into traditional PSA studies.

(d) Other open issues. As discussed, there is not a single unified approach to view a digital I&C system and, as a consequence, there are multiple ways to formulate the modelling of digital I&C systems. In addition, data collection and the integration of such data into traditional PSA models remains an open field of research.

2.7. Incorporation of ageing aspects in PSA

Nuclear power plants need to ensure an adequate safety level throughout their lifetime and consequently an assessment of the effects of ageing phenomena on plant safety margins can be very useful for IRIDM, particularly for the Periodic Safety Reviews (PSRs) for reactor units for which there are plans to extend their lifetime. The assumption of high reliability for passive structures, systems and components (SSCs) could be questionable when NPPs are operating near the end of their designed lifetime, or during the lifetime extension period. Ageing-related effects, and the effects of test and maintenance activities in controlling degradations, can be treated using available ageing PSA (i.e. a PSA that incorporates ageing effects (APSA)) approaches, thereby better reflecting the existing and projected plant situations, including the time-dependent risk profile of the plant.

Ageing PSA (APSA) can be used to predict a plant's changing risk profile over time see **Fehler! Verweisquelle konnte nicht gefunden werden.**. This can help to identify the time at which ageing SSCs should be replaced to maintain the plant risk within desired limits, and thereby to provide a basis for relicensing. By identifying and ranking important contributors to the predicted deterioration of plant safety margins and associated corrective measures, the APSA results can also rank SSCs for ageing management as well as for long-term operation activities [16].

In contrast with a traditional PSA, APSA can explicitly model the mitigation of ageing effects by maintenance, addressing such matters as the effectiveness of maintenance activities (e.g. "as good as new" or "as good as old"). This can enable the evaluation of component-specific programmes (equipment qualification, in-service inspection, maintenance) as well as ageing management programmes intended to detect, in a timely manner, the ageing degradation of a specific SSC before actual failure. By identifying critical issues related to ageing, APSA results can provide a timely warning about the potential deterioration of plant performance.

It is acknowledged that developing a full-scope APSA is quite challenging in terms of resources and efforts, but fortunately, even more limited scope ageing studies that consider only some aspects of ageing impact can provide useful guidance in focusing the resources on those SSCs for which ageing impacts are important and therefore for which the implementation of ageing mitigation measures is likely to be effective.

The main challenges for the treatment of ageing effects using APSA are related to the following:

(a) The need for multiple and complex resources. Experience has shown that developing a full-scope APSA is demanding, since it requires even more resources than developing a full-scope PSA. Due to the complexity involved, it is not easy to investigate all the effects that ageing could have on an NPP (considering both active and passive components), and it might be even more difficult to

include them adequately within PSA, in order to estimate their impact at the component, system and plant levels.

(b) Appropriate data. A realistic APSA requires more information than a traditional PSA model, and data need to be available, sufficient, and of good quality.

(c) Finding a suitable reliability model that would reasonably predict the behaviour of key SSCs over time. Data sources are not always sufficient to statistically validate an assumed model for ageing behaviour. Choosing a reasonable model from the possible alternatives is not easy, and this contributes to significant uncertainties in predicting failure rates and their variation over time. Any statistical findings need to be interpreted carefully. Sometimes the lack of strong evidence for ageing (which might be viewed as supporting a constant failure rate model) does not prove that ageing has not occurred; there just could be insufficient data to draw firm conclusions about it.

(d) Modelling ageing of passive SSCs. Past studies have shown that passive SSCs can be important risk contributors for an ageing facility but modelling their ageing faces challenges similar to those described above. Moreover, further effort is required to integrate these models into an APSA, since some of these passive SSCs cannot be modelled within a traditional PSA.

(e) Ageing impact on the results of Level 2 PSA. Similar to Level 1 PSA, the mitigation systems used in Level 2 PSA are also subject to ageing effects, and the analysis of such effects is subject to the same challenges described above, but perhaps to an even greater degree. It should be noted that containment performance plays an important role in determining the level of consequences of severe accidents in nuclear facilities and investigating the ageing effects on the containment behaviour over time could provide interesting insights. Ageing of the reactor vessel is a very challenging issue that might have a notable impact on most of the Level 2 PSA accident sequences.

(f) Uncertainties. As with other PSA studies, the results of a full-scope APSA are subject to significant uncertainties, and these are even higher for longer prediction periods. In addition to the typical uncertainties generated during the classic data analysis, there is a need to address other uncertainties associated with the choice of reliability trend models and their parameter values, uncertainties related to the data collected (e.g. non-destructive inspection results on the passive components), assumptions made, or related to the effectiveness of ageing management activities, etc. Moreover, there may be considerable uncertainty involved in mapping the ageing-induced failures of passive SSCs (previously not represented in the PSA model) to the failures of plant systems and functions.

For some PSA applications, such as extending the ageing management programme to some additional SSCs, a complete uncertainty analysis might not be needed. However, in order to facilitate the use of ageing results and to extend the number of potential applications of APSA studies, all potentially significant uncertainties need to be identified and incorporated in the prediction models to appropriately support IRIDM.

(g) Demonstration of value. Although APSA methods and models have long been available, recent applications have been limited to research studies and demonstration analyses. A challenge for the increased use and development of APSA is the demonstration of value that offsets the resource requirements mentioned earlier. Case studies beyond those performed to date might prove useful in such a demonstration.

4. CONCLUDING REMARKS

The IAEA project discussed in this paper covers a wide variety of advanced PSA approaches and applications. Some of the associated topics (particularly combined hazards, non-permanent equipment, and software reliability) are of strong interest to many Member States. Others are, at least currently, mainly being pursued by small technical communities with the possibility of wider interest with changing circumstances and, in some cases, accepted demonstrations of value.

Despite the disparity in subject matter and technical maturity level across the topics, some broad general statements can be made.

Regarding opportunities:

(a) For all topics, improvements (to a lesser or greater extent) are likely to provide improved realism, improved characterization of uncertainties, and improved support for practical IRIDM.
(b) For the topics of combined hazards and non-permanent equipment, the improvements and associated benefits are likely to be realized in the near term. For the other topics, due to a variety of challenges (summarized below), the improvements and benefits are likely to be longer term, presuming of course that efforts continue.

Regarding challenges:
(a) The technical challenges include: the sparseness or complete lack of empirical data (all topics); the need for accepted models for new scenarios and phenomena (e.g. HRA for scenarios involving non-permanent equipment, aquatic dispersion for Level 3 PSA, software failures); and the need for analysis efficiency (e.g. when tailoring a dynamic PSA approach to an IRIDM problem, when analysing hazard combinations).
(b) For some topics, there are also challenges regarding their use in IRIDM. These include how to best communicate and use the newly generated information (which, for some topics, can be voluminous and in unfamiliar form), and how to deal with user perceptions (since past results developed using older approaches or even assumptions can affect the perception of new results and even the need for new developments).
(c) For a number of topics, there are also PSA infrastructure challenges. These include a lack of consensus on PSA methods and standards (e.g. in the cases of dynamic PSA, non-permanent equipment, and software reliability); and the need to maintain and adapt supporting legacy tools (e.g. in the case of dynamic PSA).

These opportunities and challenges are further discussed in the TECDOC currently being finalized for publication in 2023.

Acknowledgements

The authors acknowledge the outstanding support provided by various experts from IAEA Member States involved in drafting a TECDOC on "Advanced Probabilistic Safety Assessment (PSA) Approaches and Applications for Nuclear Power Plants."

References

[1] International Atomic Energy Agency (IAEA). "*Safety Assessment for Facilities and Activities*", IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), Vienna, Austria, (2016).
[2] International Atomic Energy Agency (IAEA). *"Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants*", IAEA Safety Standards Series No. SSG-3, Vienna (2010).
[3] International Atomic Energy Agency (IAEA). "*Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants*", IAEA Safety Standards Series No. SSG-4, IAEA, Vienna, Austria, (2010).
[4] International Atomic Energy Agency (IAEA). "*Protection against Internal Hazards in the Design of Nuclear Power Plants*", IAEA Safety Standards Series No. SSG-64, Vienna, Austria, (2021).
[5] International Atomic Energy Agency (IAEA). "*Safety of Nuclear Power Plants: Design*", IAEA Safety Standards Series No. SSR 2/1 (Rev. 1), IAEA, Vienna, Austria, (2016).
[6] OECD Nuclear <Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI). "*Status of Practice for Level 3 Probabilistic Safety Assessment*", NEA/CSNI/R(2018)1, Paris; France, (2018).
[7] European Commission (EC). "ASAMPSA_E Risk Metrics and Measures for an Extended PSA", Technical report ASAMPSA_E/WP30/D30.7/2017-31 volume 3, Petten, The Netherlands, (2017), http://asampsa.eu.
[8] United Nations (UN) Scientific Committee on the Effects of Atomic Radiation. "Sources, Effects and Risks of Ionizing Radiation", UNSCEAR 2012 Report to the General Assembly with Scientific Annexes, United Nations, New York, NY, USA, (2015).

[9] OECD Nuclear <Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI). "*Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis*", NEA/CSNI/R(2014)16, OECD/NEA/, Paris, France, (2015).
[10] O. Bäckström, et al. "*Software reliability analysis for PSA: failure mode and data analysis*", NKS-341, Nordic nuclear safety research (NKS), Roskilde, Sweden, (July 2015).
[11] J. Hämäläinen, et al. "*HARMONICS*", Final Public Report, European Commission (EC), Brussels, Belgium, (November 2015).
[12] O. Bäckström, et al. "*Software reliability analysis for PSA*", NKS report NKS-304, Roskilde, Sweden, (2014).
[13] T. Aldemir, et al. "*Probabilistic risk assessment modeling of digital instrumentation and control systems using two dynamic methodologies*", Reliability Engineering and System Safety, vol. 95, no. 10, pp. 1011-1039, (2010).
[14] U.S. Nuclear Regulatory Commissionn(NRC), "Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods", NUREG/CR-6997, Washington, DC, USA, (2009).
[15] E. Stefanov, and G. Petkov. "*A Case Study on Incorporation of Ageing Effects into the PSA Model of NPP with WWER-1000*", EC Workshop on Investigation of Ageing Effects using the Probabilistic Safety Assessment, Kernkraftwerk Gösgen-Däniken, Switzerland, (2010).
[16] M. Nitoi. "Investigation of Ageing Effects Using Probabilistic Safety Assessment", Proceedings of the European Workshop on Probabilistic Safety Assessment, EUR 25102 EN, ISBN: 978-92-79-22322-8, doi:10.2790/39416, ISSN: 1831-9424, Luxembourg: Publications Office of the European Union, Luxemburg, (2011).